Beyond risk scores : context-aware adaptive authentication

Anne Bumiller

COLLEGE MATHS, TELECOMS
DOCTORAL INFORMATIQUE, SIGNAL
BRETAGNE SYSTEMES, ELECTRONIQUE

Université de Rennes

THÈSE DE DOCTORAT DE

L'UNIVERSITÉ DE RENNES

ÉCOLE DOCTORALE N° 601
Mathématiques, Télécommunications, Informatique, Signal, Systèmes, Électronique
Spécialité : *Informatique et Architectures numériques*

Par
Anne Bumiller

Beyond Risk Scores : Context-Aware Adaptive Authentication

Thèse présentée et soutenue à IRISA, Université de Rennes, le 9 novembre 2023
Unité de recherche : IRISA, CNRS, UMR 6074

Rapporteurs avant soutenance :

Prof. Dr. Romain ROUVOY, Professeur, Université de Lille
Prof. Dr. Alexander PRETSCHNER, Professeur, Technische Universität München

Composition du Jury :

Attention, en cas d'absence d'un des membres du Jury le jour de la soutenance, la composition du jury doit être revue pour s'assurer qu'elle est conforme et devra être répercutée sur la couverture de thèse

Président :	Prof. Dr. Francois TAIANI	Professeur, Université de Rennes
Examinateurs :	Dr. Elisavet KOZYRI	Maitre de conférence, UiT The Arctic University of Norway
	Dr. Gerson SUNYÉ	Maitre de conférence, Université de Nantes
Dir. de thèse :	Prof. Dr. Olivier BARAIS	Professeur, Université de Rennes
Co-dir. de thèse :	Prof. Dr. Benoit COMBEMALE	Professeur, Université de Rennes
Co-Encadrants :	Dr. Stéphanie CHALLITA	Maitre de conférence, Université de Rennes
	Nicolas AILLERY	Research Engineer, Orange

"In the social jungle of human existence, there is no feeling of being alive without a sense of identity."
–Erik Erikson

Acknowledgments

Completing a PhD is a deeply personal and professional experience, and therefore, this manuscript would not be complete without adequate thanks to those who supported and accompanied me during these three intense years. First, I would like to thank Pr. Alexander Pretschner and Pr. Romain Rouvoy, the reviewers of this thesis, for the time they dedicated to it and their constructive feedback. I also thank Elisavet Kozyri, Gerson Sunyé and Francois Taiani for agreeing to be part of my jury. I would like to thank Nicolas Aillery, and Gaël Le Lan, my supervisors at Orange, for being by my side, for their advice and remarks, and for the motivation and ideas they brought to me. I thank Olivier Barais, my thesis director, for the stimulating exchanges we had, for the opportunities he offered me with this thesis, and the regular time he spent with me. Foremost, I am truly grateful to my co-supervisors, Stéphanie Challita and Benoit Combemale. Thank you for your guidance, support, and encouragement throughout my PhD journey. Your knowledge, expertise, and encouragement have been instrumental in shaping my research. I would also like to thank Stéphanie Challita for her friendship, and personal support. I would like to express my gratitude to Erwan Diverez, Benoit Herard, Arnault Nagle, and Simon Bécot, for the good work environment they created and maintained at Orange. I would also like to extend my heartfelt thanks to Lucas, his unwavering support and encouragement have been a constant source of strength and inspiration throughout my PhD journey. I would also like to express my gratitude to all the members of the DiverSE team at Inria, and the IDIS team at Orange for their support and assistance. It was a pleasure meeting many wonderful people, everyone was friendly and open for discussion, which made me feel very welcome. A big thank you also to Elisavet Kozyri, and Havard Dagenborg for welcoming me so warmly in Tromsoe and to make such an interesting stay abroad possible for me during this PhD. Thank you to my friends in Rennes for making these years in Rennes so dynamic and enjoyable. Thanks also to all the stuff members of the IForme Fitness Center in Rennes. The uncountable hours of boxing and other classes for stress reduction in such a warm environment were really helpful to getting me back behind the computer. Finally, a last thank you to my family: to my parents who supported me and were always there for me, to my grandmother who were always interested, and to my brother and sister, who were able to push me forward thanks to their constant motivation and energy. Once again, thank you all for your support, guidance, and encouragement throughout this journey. I could not have done it without you.

Abstract

Adaptive Authentication (AA) allows a system to **dynamically select the appropriate method(s)** for a user depending on contextual information, such as location, IP address, and other attributes. However, reasoning about the appropriateness of authentication method(s) (*e.g.,* for security and usability) according to the contextual information is challenging. In recent years, there have been many academic initiatives to replace passwords, and to leverage context information to adjust the authentication method(s) to request. These initiatives focus on using context information to calculate risk scores. Additional authentication method(s) are then required if a certain risk level is detected. However, given the diversity of concerns (*e.g.,* security, usability, deployability, privacy), risk scores used as proxies of the appropriateness of authentication methods are too simple. Reasoning about the appropriateness of authentication methods requires a fine-grained understanding of the contextual situation (*e.g.,* type of risk faced, usability constraints in specific environments). Motivated by the need to improve the design, deployment, and evaluation of *Adaptive Authentication* (AA) systems, my research aims to leverage context information beyond the calculation of risk scores to provide a more fine-grained reasoning about the appropriateness of authentication method(s).

In this dissertation, I provide four major contributions. First, I propose a **structured review of the literature to date on Context Modeling for Adaptive Authentication systems (CM4AA)**. This review helps to understand the representation of context information with appropriate and well-designed models. I analyze how context modeling for AA systems is performed and determine desired properties of the context information model for AA systems. I demonstrate the ability to capture a common set of contextual features relevant to AA systems independently from the application domain, and I emphasize that despite the possibility of a unified framework, no standard for CM4AA exists.

Second, I present a tool-supported **Context-driven Modeling Framework for dynamic Authentication decisions (CoFrA)**, where the context information specifies the appropriateness of authentication method(s) beyond the calculation of risk scores while considering the security, usability, privacy, and deployability properties. CoFrA is a precise, reusable, and extensible metamodel that characterizes the domain of AA and provides a language to determine the appropriate authentication method(s) in a given context.

Third, I propose an **explainability model based on Shapley values** that can be used to explain risk scores that are estimated with score-based approaches to support the transition from score-based approaches to a more fine-grained AA approach. I show that the risks can be explained differently and specifically for each user login attempt. Hence, this explainability model can effectively improve our understanding of risks. The explanations generated can be used to reason on the appropriateness of authentication methods for each user login attempt while considering more information than just the risk

score. More specifically, these explanations can be used within my CoFrA framework to reason on the appropriateness of authentication methods using efficiently this information.

Fourth, I present a **tooled approach for the definition of the most well-suited authentication models**. CoFrA provides a language to determine AA models. For an application, there may be several valid models, and the difficulty is to choose the one that fits the application according to multiple quality criteria. This contribution supports this choice. The evaluation approach that I propose guides authentication practitioners and researchers in the process of evaluating and comparing CoFrA models to define the most well-suited model for specific applications.

All the four contributions of this thesis have been validated rigorously through case studies and extensive exchanges with authentication and modeling experts.

In summary, this dissertation addresses the shortcomings of exclusively using risk scores to determine the appropriateness of authentication methods. The contributions of this thesis aim to improve the design, deployment and evaluation of AA systems by handling a fine-grained reasoning about the appropriateness of authentication methods, beyond the calculation of risk scores. The results of this thesis further enable developers, administrators, and researchers to create efficient AA solutions and support a widespread adoption in practice.

Keywords: Adaptive Authentication, Context, Risk Score, Risk-Based Authentication, Models, Passwords, User

Résumé

Mon doctorat est un **doctorat industriel**. La fondation CIFRE (Convention Industrielle de Formation par la Recherche) est un programme doctoral français qui vise à offrir aux étudiants la possibilité d'obtenir un doctorat dans le cadre d'un projet de recherche industriel. Le programme est soutenu conjointement par le ministère français de l'enseignement supérieur et de la recherche et par des partenaires industriels. L'objectif de CIFRE est de promouvoir la collaboration entre les universités et les entreprises afin de partager les connaissances et l'expertise entre le monde universitaire et l'industrie. Le programme apporte un soutien financier aux doctorants qui réalisent leurs projets de recherche dans une entreprise, sous la supervision d'un encadrant universitaire et d'un encadrant d'entreprise. La fondation CIFRE pour le doctorat permet aux étudiants d'obtenir un doctorat tout en acquérant une expérience industrielle précieuse. Ma thèse est donc soutenue à la fois par l'Université de Rennes (l'équipe DiverSE) et par Orange™. Orange™, en tant qu'entreprise multinationale de télécommunications, s'intéresse aux sujets liés à la gestion de l'identité et à la sécurité et promeut ma thèse pour répondre au manque de moyens permettant d'exploiter les informations contextuelles pour l'AA. DiverSE (anciennement Triskell) est une équipe de recherche de l'IRISA (unité mixte de recherche regroupant le CNRS, l'Université de Rennes, l'INRIA INSA Rennes à Rennes /

Bretagne / France) et travaille sur la. Le programme de recherche de DiverSE porte sur le génie logiciel. Dans ce domaine, l'équipe développe des modèles, des méthodologies et des théories pour relever les défis posés par l'émergence de plusieurs formes de diversité dans la conception, le déploiement et l'évolution des systèmes.

L'***Authentification Adaptative (AA)*** permet à un système de **sélectionner dynamiquement la ou les méthodes les plus appropriées** pour authentifier un utilisateur en fonction d'informations contextuelles, telles que la localisation, et l'adresse IP.

Toutefois, il est difficile de raisonner sur la pertinence de la ou des méthodes d'authentification en fonction des informations contextuelles, lorsque le choix porte sur multiples dimensions telles que la sécurité et l'expérience utilisateur. De nombreuses initiatives universitaires ont été lancées pour remplacer les mots de passe et exploiter les informations contextuelles afin d'adapter la ou les méthodes d'authentification demandées à l'utilisateur et au contexte. Ces initiatives se concentrent sur l'utilisation des informations contextuelles pour calculer des scores de risque. Des méthodes d'authentification supplémentaires sont alors requises si un certain niveau de risque est détecté. Compte tenu de la diversité des impacts en terme de sécurité, expérience de l'utilisateur, déployabilité, et respect de la vie privée, les scores de risque sont des indicateurs trop simples de l'adéquation des méthodes d'authentification. Le raisonnement sur la pertinence des méthodes d'authentification nécessite une compréhension fine de la situation contextuelle (par exemple type de risque encouru, contraintes d'utilisation dans des environnements spécifiques).

Ma recherche vise ainsi à exploiter les informations contextuelles **au-delà du calcul des scores de risque** pour fournir un raisonnement plus fin sur l'adéquation des méthodes d'authentification. L'objectif est donc d'**améliorer la conception, le déploiement et l'évaluation des systèmes d'authentification adaptatifs**.

Le sujet de ma thèse fait partie d'un **contexte scientifique** riche centré sur l'authentification et la gestion de l'identité qui est une **préoccupation transversale** dans de multiples domaines. Parfois, les interprétations des termes ne sont pas les mêmes dans les différents domaines. Pour plus de clarté, il est donc important de définir le vocabulaire et de distinguer correctement les termes les uns des autres. C'est pourquoi, dans une première chapitre, je présente une **délimitation terminologique** de tous les termes utilisés dans cette thèse. Comme j'utilise ces techniques pour mes contributions, je présente également le contexte de la modélisation, de la métamodélisation et des langages spécifiques au domaine dans un premier chapitre.

De plus, j'analyse **la quête en cours pour remplacer les mots de passe** dans la litérature et en pratique. Je présente les approches existantes pour exploiter les informations contextuelles pour l'authentification dans la littérature à ce jour. Je me concentre sur les tendances (par exemple, Risk-Based Authentication (RBA), Multi Factor Authentication (MFA), Zero Trust), les attaques émergentes sur les systèmes d'authentification et les domaines de recherche interdisciplinaires qui s'attaquent aux défis de l'authentification. Je souligne la nature interdisciplinaire du domaine de recherche, qui englobe la sécurité

et la protection de la vie privée, l'apprentissage automatique, la gestion de l'identité et les systèmes adaptatifs, ainsi que les défis qu'il pose. J'énumère et j'ecxplore les travaux les plus pertinents. Puisque ma thèse présente une solution pour faire de l'AA au-delà du calcul des scores de risque, l'idée de ce chapitre est d'explorer les solutions existantes basées sur les scores et leurs limitations. En parallèle, j'analyse également le contexte industriel. Je me concentre sur les solutions commerciales pour l'AA et les études existantes sur la façon dont les informations contextuelles sont utilisées pour l'authentification par les principaux services en ligne. J'ai également réalisé des enquêtes auprès d'experts et des évaluations des besoins afin de déterminer ce que pensent les experts de l'exploitation des informations contextuelles pour l'authentification. Donc, ma thèse contient une analyse de l'état de la pratique, une identification des solutions commerciales d'AA utilisant des technologies d'IA pour l'évaluation des risques basée sur des facteurs contextuels, et des observations d'experts dans le domaine. En outre, ma recherche se penche sur les approches *Risk-Based Authentication* (RBA), soulignant leur potentiel pour une authentification sécurisée avec une bonne facilité d'utilisation, tout en soulignant leurs limites. Je soutiens que l'évaluation de l'adéquation des méthodes d'authentification nécessite une approche plus fine qui ne repose pas uniquement sur les scores de risque.

Dans cette thèse, j'apporte quatre contributions majeures. Premièrement, je propose une **étude de la litérature centré sur la modélisation des informations contextuelles pour les systèmes d'authnetification** afin de modéliser l'ensemble des informations contextuelles. J'analyse la manière dont la modélisation du contexte pour les systèmes d'authentification adaptatifs est effectuée et je détermine les propriétés souhaitées du modèle d'information contextuelle pour les systèmes d'authentification adaptatifs. Je démontre la capacité à capturer un ensemble commun de caractéristiques contextuelles pertinentes pour les systèmes d'authentification adaptatifs indépendamment du domaine d'application, et je souligne que malgré la possibilité d'un cadre unifié, il n'existe pas de norme pour la modélisation du contexte pour les systèmes d'AA.

Deuxièmement, je présente un **framework de modélisation de contexte pour les décisions d'authentification dynamique (CoFrA)**, dans lequel les informations contextuelles spécifient l'adéquation de la (des) méthode(s) d'authentification au-delà du calcul des scores de risque et en ce qui concerne les propriétés de sécurité, d'utilisabilité, de confidentialité et de déployabilité. CoFrA est un métamodèle précis, réutilisable et extensible qui caractérise le domaine de l'AA et fournit un langage permettant de déterminer la ou les méthodes d'authentification appropriées dans un contexte donné.

Troisièmement, je propose un **modèle d'explicabilité basé sur les valeurs de Shapley** qui peut être utilisé pour expliquer les scores de risque qui sont estimés avec des approches basées sur les scores afin de soutenir la transition des approches basées sur les scores vers une approche d'AA plus fine. Je montre que les risques peuvent être expliqués différemment et spécifiquement pour chaque tentative de connexion de l'utilisateur. Ce modèle d'explicabilité peut donc améliorer efficacement notre compréhension des risques. Les explications générées peuvent être utilisées pour raisonner sur l'adéquation des méth-

odes d'authentification en fonction de la sécurite, l'éxpérience de l'utilisateur, la deployabilité, et la protection de la vie privée pour chaque tentative de connexion de l'utilisateur, en tenant compte d'autres informations que le seul score de risque. Plus précisément, les explications peuvent être utilisées dans mon cadre CoFrA pour raisonner sur l'adéquation des méthodes d'authentification en utilisant efficacement ces informations.

Quatrièmement, je présente une **approche outillée pour la définition des modèles d'authentification les mieux adaptés**. CoFrA fournit un langage pour déterminer les modèles d'authentification adaptatifs. Pour une application, il peut y avoir plusieurs modèles valides, et la difficulté est de choisir celui qui convient à l'application en fonction de multiples critères de qualité. Ma quatrième contribution soutient ce choix. L'approche d'évaluation que je propose guide les praticiens et les chercheurs en authentification dans le processus d'évaluation et de comparaison des modèles CoFrA afin de définir le modèle le mieux adapté à des applications spécifiques.

Je valide les propositions de cette thèse par des études de cas et sur la base d'échanges approfondis avec des experts en authentification et en modélisation.

Je présente aussi des **approches implementées** issues de ce travail de recherche ainsi que la **mise en œuvre** de certaines des propositions dans des contextes industriels. J'explique le transfert de technologie pour intégrer les idées de cette thèse dans le système d'authentifi- cation Orange.

Cette thèse aborde les lacunes de l'utilisation exclusive des scores de risque pour déterminer l'adéquation des méthodes d'authentifica- tion. Les contributions de cette thèse visent ainsi à améliorer la conception, le déploiement et l'évaluation des systèmes d'authentification adaptatifs via raisonnement fin sur l'adéquation des méthodes d'authentification, au-delà du calcul des scores de risque. Les résultats de cette thèse permettent aux développeurs, aux administrateurs et aux chercheurs de créer des solutions AA efficaces et de soutenir une adoption généralisée dans la pratique.

Donc, dans cette thèse, je présente mon travail qui couvre les besoins de modéliser précisément le contexte pour l'AA et de raisonner sur celui-ci pour fournir la (les) méthode(s) d'authentification appropriée(s). Cependant, il y a encore beaucoup de travail à faire pour faire avancer la recherche dans ce domaine. Je discute donc de certains travaux en cours et des **perspectives** qui devraient être prises en compte dans la poursuite de mes travaux de recherche. Je présente également des perspectives industrielles pour souligner l'impact de mes recherches pour Orange™et d'autres entreprises. Dans le court terme, je prévois de démontrer la facilité d'utilisation des prototypes proposés par une évaluation structurée menée par des experts. Aussi, la méthode d'explicabilité proposée doit être étendue à d'autres ensembles de données et à d'autres modèles d'estimation des scores de risque. L'absence de mesures d'évaluation normalisées et de critères de référence pour les modèles d'authentification peut être attribuée au manque de discussions ouvertes au sein de la communauté. C'est pourquoi, en plus de l'approche outillée pour la définition du modèle d'authentification le mieux adapté présentée dans ma thèse, je vise à tirer parti de mes connaissances acquises dans l'industrie et le monde universitaire pour pro-

poser un ensemble complet de modèles d'authentification. Quatre problèmes déclenchant en plus quatre perspectives de recherche. Je les organise dans la boucle MAPE-K pour les systèmes AA en fonction des domaines qu'ils concernent. Le problème de l'information incorrecte du contexte due à l'utilisation de réseaux privés virtuels (VPNs) et de proxys ou d'empreintes digitales volées concerne le "Monitoring" (M). La difficulté de prendre en compte les préférences des utilisateurs en matière de méthodes d'authentification concerne le "Analysis" (A). L'absence de validation formelle de la sécurité d'un système d'AA concerne le "Planning" (P). La confidentialité limitée des systèmes Identity Federation (IF) qui augmentent la disponibilité de l'AA concerne le "Executing" (E). Je détaille ces quatre perspectives dans ma thèse.

Les contributions issues de cette thèse ont été publiées dans des conférences internationales à comité de lecture. Je détaille toutes les publications qui ont résulté de mes recherches au cours des trois dernières années.

Cette thèse est divisée en huit chapitres. Alors que le premier chapitre est l'introduction, le deuxième chapitre présente le contexte scientifique et industriel. Dans le troisième chapitre, je présente la première contribution de ma thèse, une revue systématique de la littérature sur la modélisation du contexte pour les systèmes AA. Sur la base de cette première contribution, je présente ensuite trois autres contributions, qui sont des approches basées sur des modèles pour les systèmes d'AA tenant compte du contexte. Dans le Chapitre 7, je détaille l'implémentation et l'industrialisation de mon travail de recherche. Enfin, le dernier chapitre comprend les conclusions et les perspectives de cette thèse.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter introduces the research activities conducted in the context of this thesis. I state the main problems and the research questions addressed, outline the thesis vision and the proposed solutions, provide a roadmap of the thesis, point out resulting publications, and describe the thesis environment in which this thesis was produced.

Contents

Digital identity has high relevance for individuals, organizations, and governments, as authentication represents a necessary basis for many transactions. In the past, contracts, trades and agreements were almost exclusively handled in person (face-to-face). Today, a large proportion of transactions is handled digitally. Depending on the case, this requires a form of digital authentication. Since transactions take place digitally, secure methods for digital authentication are crucial. Digital authentication is hence a significant and urgent scientific problem as online life becomes inter-winded with reality [29].

Research on digital authentication has shown over 40 years that passwords are flawed, insecure, and widely disliked by users [4, 87]. For these reasons, there have been many academic initiatives to find alternatives

to replace passwords, as well as proposals to alleviate the complexities of managing them [15, 75, 112, 129].

The focus of my research is not placed on finding a replacement, but on designing **technologies that can select the appropriate authentication methods, adapting their usage to the context of the login attempt**.

Researchers in different fields may have different understandings of the concept of context. Most scholars define context through enumerating examples [72]:

- *"Lighting, temperature, noise, humidity level, traffic conditions"* [109]
- *"Location, time, season, temperature"* [21]
- *"Emotional state, attention focus, orientation, date and time of day, objects, people in the user's environment"* [40]
- *"Capabilities of mobile devices, the characteristics of network connectivity, user-specific information"* [53]
- *"Time of the login, IP address, geolocation, operating system, browser configuration, account's patterns of usage"* [48]
- *"IP address, geolocation, country, user agent"* [129]

Furthermore, some scholars also use synonyms such as the environment state, surroundings, or situation to explain the meaning of context [72].

In this thesis, I define **context** as ***any information that can be used to characterize the situation of an entity.*** [a]

a. I define an **entity** as a human that has a distinct existence. Hence, in this work I focus on the authentication of human users. Nevertheless, some concepts may be transferable to authentication of computers and messages. I leave this open to future research.

The research field of context-aware, self-adaptive systems was born in the late '90s driven by the need to deal with the ever-increasing complexity of software systems and their dynamic environment [8]. Many researchers and practitioners have attempted to define context-awareness in various ways. I give below some commonly used definitions:

— *"Context-awareness is the ability of a program or computing device to detect, sense, interpret, act, and respond to aspects of the environment, such as location, time, temperature, or user identity"* [110].
— *"Context-awareness is the ability to automate a software system, modify an interface, and provide maximum flexibility of a computational service based on context information"* [107].
— *"A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task"* [42].
— *"A context-aware system is a system embedding contextual information in decision processes"* [43].

In this thesis, I define **context-awareness** as ***the ability of a system, to understand and adapt to its context.***

In the domain of authentication, context-awareness is used to make informed decisions about whether to grant access, what authentication method(s) to require, and what factors may indicate a risk. The context information influences the desired properties of authentication methods (*e.g.,* security [16, 137, 19, 5, 123, 93, 44], usability [16, 137, 136, 19, 5, 123, 44, 128], deployability [16, 137, 136, 5, 123, 131], privacy [104, 136, 5, 130]).

I define an **Adaptive Authentication (AA) system** as a ***context-aware authentication system that uses context to provide the appropriate authentication method(s), where appropriateness depends on the desired properties of the authentication method(s) in a context.***

Hence, AA allows a system to dynamically select the appropriate method(s) to authenticate a user depending on contextual factors.

The contributions of this thesis can be used as support for authentication practitioners as they provide valuable insights and findings that help navigate the complex trade-off analysis between context information, risks, and authentication methods in practice. I promote a feedback loop between

research and practice leading to more relevant and impactful results. In the context of my CIFRE Ph.D. fellowship, the ability to use my contributions as support for practitioners is particularly important because it helps ensure that the research being conducted is not only academically rigorous but also relevant and useful for Orange™ .

The remainder of this introductory chapter is organized as follows. I identify the problems that motivate my research in Section 1.1. Section 1.2 introduces the research questions that this thesis aims to answer. The vision of my research is presented in Section 1.3. Section 1.4 introduces my proposed solution. In Section 1.5, I summarize the structure of this thesis. Finally, in Section 1.6, I detail the publications derived from my research and in Section 1.7, I present the thesis environment in which this thesis was produced.

1.1 Problem Statement

Leveraging context information to reason about the appropriateness of authentication method(s) is not a straightforward task. I state the main challenge addressed by this thesis as follows:

Authentication technique weaknesses, like password-based authentication, are known [129], and service operators often implement additional authentication methods to limit the restraints of the individual techniques [87, 125]. The existing initiatives to leverage context information adjusting the authentication method(s) to request focus on calculating a risk score during password entry. Such risk scores are typically classified into three categories: low, medium, and high [83, 57, 48, 38, 54]. Additional authentication method(s) are usually required if a high-risk is detected [129]. These approaches (called **Risk-Based Authentication (RBA)**) aim to strengthen security while maintaining usability by monitoring how risky an access attempt is. They have the potential to provide secure authentication with good usability [48, 28]. However, given the diversity of concerns (*e.g.,* security, usability, deployability,

privacy), risk scores used as proxies of the appropriateness of authentication methods are too simple. Reasoning about the appropriateness of authentication methods requires a fine-grained understanding of the contextual situation (*e.g.,* type of risk faced, usability constraints in specific environments).

There are different types of risks. For each risk types, the effectiveness of different authentication methods varies. For example, there may be a risk that the password has been stolen within a phishing attack. Then password authentication is not efficient to counteract the risk. A method based on an external device, for example an *One Time Password* (OTP), can be more efficient. The potential attacker is in possession of the password, but not of the device. If there is a risk that the mobile phone has been stolen, then password authentication may be more effective. In the case of the risk of an automated attack (robot), a CAPTCHA can be sufficient. And all this only concerns the security dimension, but for usability also, there is no one-fit-all solution. For example, the authentication method "face recognition" may not be usable in the dark [1], and the authentication method "voice recognition" may not usable in a noisy environment. AA allows a system to dynamically select the appropriate method(s) to authenticate a user depending on contextual factors. If the selection is based only on a risk score, then the selected authentication method(s) may not be usable in the context. Hence, considering only the security aspect is not enough to reason about the appropriateness of an authentication method. An authentication method is also not appropriate when it is not deployable in a context (*e.g.,* high implementation costs, not browser compatible, the user has not registered the biometric data) or when it requests information that is too private.

In summary, scores are insufficient to select the appropriate authentication method(s) concerning two main points. First, the fusion of the contextually available features in a one-dimensional risk score reduces the

1. Modern face recognition systems, such as Android's Face Unlock and iOS's Face ID, work in the dark, but this is not the case for all systems. Hence, I take this as an example of an authentication method whose performance may be impacted by the surrounding context.

comprehensibility and explainability of risks. Second, context information not only influences the risk of an unexpected or suspicious access attempt (security) but also concerns other properties of authentication methods (*e.g.,* usability, deployability, privacy).

According to the use of the terms in the context of this thesis, **Risk-Based Authentication (RBA)** and **Adaptive Authentication (AA)** are related approaches but have some key differences. RBA uses statistical models to determine the risk level associated with a user's access attempt, based on the context. If the risk level exceeds a certain threshold, additional authentication method(s) such as a one-time password or biometric verification are required. AA, which I propose in this thesis, on the other hand, dynamically adjusts the authentication method(s) required, based on the current context and various factors (*e.g.,* the type of risk faced, and usability constraints). The contextual factors are used to determine the appropriateness of authentication method(s). In summary, RBA primarily focuses on assessing the risk level and triggering authentication steps if needed, while AA aims to dynamically adjust the authentication process to meet the desired properties in each contextual situation.

Let us consider the following example to illustrate the role of AA. Bob, a German traveler in France checks his emails at 2:00 am in a poorly lighted room. He enters the username and password correctly. His email provider can acquire contextual information: geolocation, luminosity, time, and typing speed. Bob's email provider determines some threats: Bob is not located in Germany as usual, he is checking his emails at an unusual time, it is dark around him, and he is typing slower. All these threats make the email provider assume that there is a risk that an intruder who has Bob's password might try to access Bob's emails. Bob has registered facial recognition and fingerprint as authentication methods. Password-based authentication can be bypassed by the intruder who has stolen Bob's password. Hence, the explanation of the type of risk helps here choosing the appropriate method, which would not be possible with a risk score only.

The face recognition system of Bob's device is not efficient to use in the dark. Therefore, the AA model used by the email provider determines that Bob needs to be authenticated with his fingerprint. Hence, the usability property is taken into account what would not be possible with a risk score only.

Someone reading this example might wonder how the context data (*e.g.,* geolocation, luminosity) is made available. The acquisition of context information and sensor technologies are indeed beyond the scope of this thesis, but previous work has shown it to be reasonable to consider used devices able to acquire significant information, because modern smartphones are equipped with a variety of sensors that can collect data about their surroundings [8, 23]. To use the context information more efficiently and to reason about the appropriateness of authentication methods beyond risks scores, efforts are necessary to find out which models are suitable to the field of context modeling for AA. Until now, context modeling for security applications (e.g., AA) has not been deeply studied, and I observe a limited usage of context with vague descriptions and ground. Also, many organizations already have implemented RBA systems and may not be ready to transition immediately to AA. The transition to AA can be a gradual process, and legacy RBA systems will likely be in place for some time. There is a lack of support for a smooth transition from RBA to AA allowing organizations to gradually incorporate AA solutions. During the implementation phase of AA, it is also important to take into account that different organizations or application domains may have different requirements (*e.g.,* specific security constraints, user requirements) that need to be considered in the AA system. Evaluating authentication systems is important to define the most well-suited model for a given system. Without a way to compare and evaluate authentication models, it is very hard to determine which models perform better than others under different conditions and which models are more suitable for specific application domains.

In Figure 1.1, I summarize the main problems that motivate this thesis. First, the black-box risk-score estimation (RBA) presents a significant challenge (P1), as it lacks transparency of risk types and a multi-dimensional

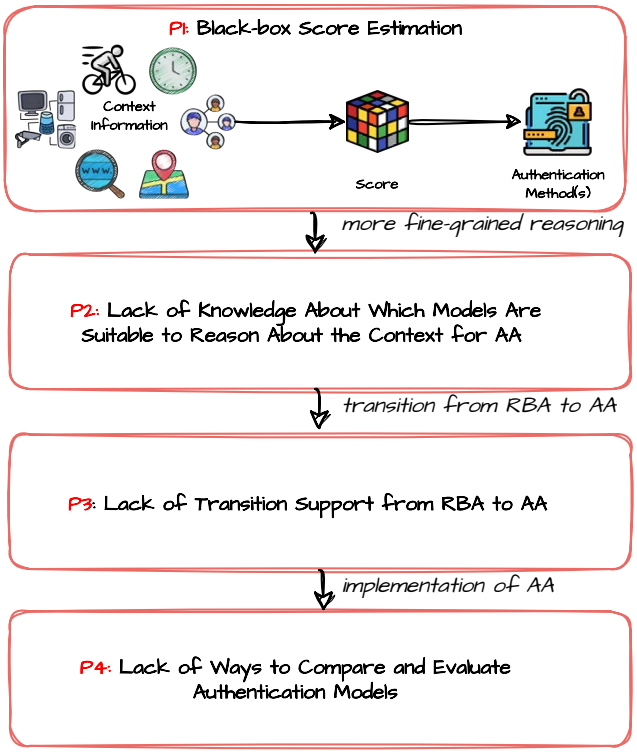

Figure 1.1 – Key Challenges Addressed in This Thesis.

vision. Second, in order to propose a more fine-grained reasoning approach about the appropriateness of authentication methods, representing context with appropriate and well-defined models is necessary. However, the appropriate context models for achieving this goal are not well known (P2). Furthermore, there is a need for a seamless transition from RBA to AA (P3). After a transition from RBA to AA has taken place, the most well-suited AA model for a given system must be selected for implementation.

1.2 Research Questions

More specifically, this thesis aims to answer the following research questions (RQs):

— **RQ#1:** What is the current body of knowledge about CM4AA?

This aims to investigate which context information determines the context of AA systems, how it is modeled, and for which phase of the authentication system life-cycle is the model used. Also, this question aims to determine the desired properties of the context information model and its use for AA.

— **RQ#2:** How to leverage context information to reason about the appropriateness (*e.g.,* for usability, security, privacy, and deployability) of authentication methods?
This aims to abstract domain knowledge about context modeling for AA systems and to provide a tool-supported language to determine the appropriate authentication methods in a given context.

— **RQ#3:** Can the risk scores estimated with RBA approaches be explained for suspicious authentication events to distinguish between different risk types?
This aims to investigate whether explainability models effectively improve our understanding of impersonation risks and whether contextual explanations can help to understand the suspiciousness of an authentication event and the risk type to support the transition from RBA to AA.

— **RQ#4:** How to evaluate and compare authentication models?
This aims to provide a trade-off analysis of multiple quality criteria and to support the selection of the most well-suited authentication model for a given system.

1.3 Thesis Vision

To address the aforementioned problems, this thesis aims to leverage context information beyond the calculation of risk scores and to provide a more fine-grained reasoning about the appropriateness of authentication method(s). As illustrated in Figure 1.2, this thesis promotes AA beyond RBA approaches. The contributions presented in this thesis are represented in green. I illustrate in Figure 1.2 how my four contributions (C1, C2, C3, C4) improve RBA approaches. RBA is based on the point of view that a risk

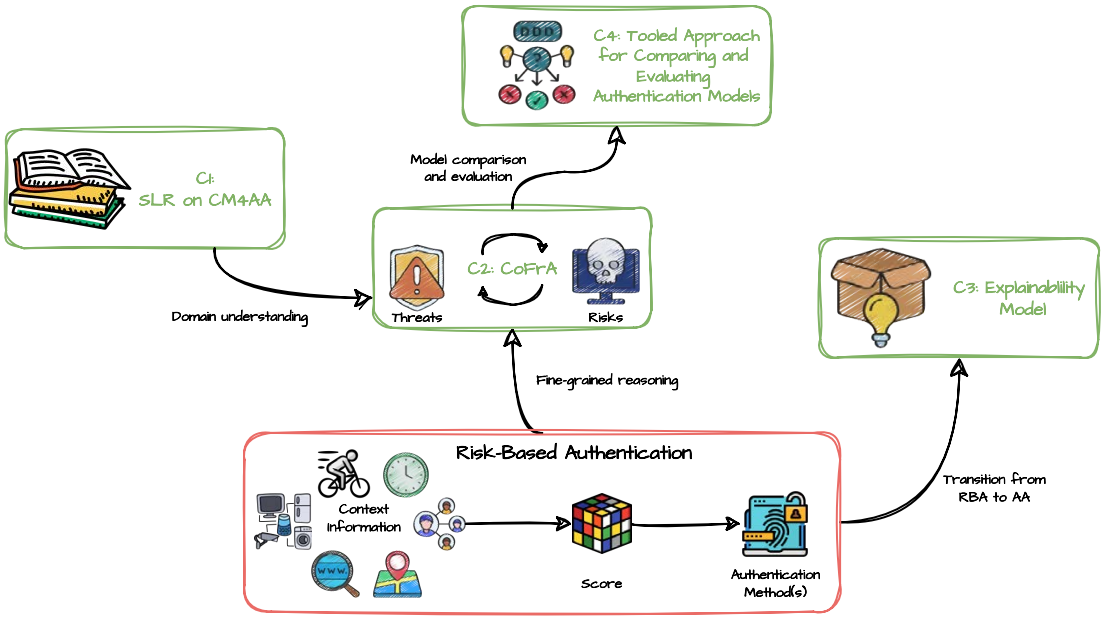

Figure 1.2 – Thesis Vision.

score is calculated, and it decides about the authentication method(s) to request. In the modeling framework proposed in this thesis named CoFrA (C2) context gives information about threats and risks, and the type of risk decides about the authentication method(s) to request. CoFrA is built based on a systematic literature review on context modeling for AA (C1). With the help of an explainability model (C3), I show that for a given estimated risk score there are different explanations for each login attempt. These contextual explanations can be used within CoFrA for a more fine-grained mapping between context information and authentication methods. To also support evaluating and comparing authentication models, I propose a tool-supported approach for the selection the most well-suited authentication model for a given system (C4), which helps selecting and tailoring authentication models for specific application domains according to multiple criteria. Within this contribution, I provide a methodology to

evaluate authentication models in specific contexts.

1.4 Proposed Solution

In this section, I provide an overview of the contributions described in this thesis. As stated before, the goal of my thesis is to propose the first framework to handle reasoning about the appropriateness of authentication method(s) beyond the calculation of risk scores. Hence, I aim to provide approaches, languages, and tools to leverage context information for AA. The main contributions of my work are summarized as follows:

Systematic Literature Review: On Understanding Context Modeling for AA Systems. Regarding RQ#1, this thesis aims to provide a structured review of the literature to date on Context Modeling for AA (CM4AA) to understand the current body of knowledge about CM4AA. This survey allows one to understand which context information determines the context of AA systems, how it is modeled, and for which phase of the authentication system life-cycle the model is used. It is also the basis to extract the desired properties of the context information model and its use for AA systems.

Therefore, my first contribution is to enhance the understanding of the current body of knowledge about CM4AA. I provide a comprehensive overview and analysis of research work on CM4AA. To this end, I pursue three goals based on the *Systematic Mapping Study (SMS)* and *Systematic Literature Review (SLR)* research methodologies. I first present a SMS to structure the research area of CM4AA (**goal 1**). I complement the SMS with a *Systematic Literature Review* (SLR) to gather and synthesize evidence about context information and its modeling for AA systems (**goal 2**). From the knowledge gained from goal 2, I determine the desired properties of the context information model and its use for AA systems (**goal 3**). I demonstrate the ability to capture a common set of contextual features that are relevant for AA independent from the application domain. I emphasize that despite the possibility of a unified framework, no standard

for CM4AA exists. This thesis addresses the need for standardization, abstraction, and a common language in AA, providing a modeling framework and domain-specific concepts to improve understanding and communication among researchers and practitioners.

CoFrA: A Context-Driven Modeling Framework for Dynamic Authentication Decisions. Regarding RQ#2, this thesis aims to propose a modeling framework to leverage context information to reason about the appropriateness (e.g., for usability, security, deployability, and privacy) of authentication methods beyond the calculation of risk scores. This framework relies on Model Driven Engineering (MDE) techniques. They help to extract and abstract domain knowledge about CM4AA learned from the structured literature review. Hence the modeling framework characterizes the domain of AA and provides a language to determine the appropriate authentication methods in a given context.

Therefore, my second contribution is to abstract the domain knowledge about context modeling for AA. I propose a Context-driven modeling Framework for dynamic Authentication decisions (CoFrA), where the context information specifies the appropriateness of authentication methods. CoFrA is based on a precise metamodel that reveals framework abstractions and a set of constraints that specify their meaning. The framework supports the complex trade-off analysis between context information, risks, and authentication methods, according to usability, deployability, security, and privacy. I validate the proposed framework through case studies and extensive exchanges with authentication and modeling experts. I show that model instances describing real-world use cases and authentication approaches proposed in the literature can be instantiated validly from the metamodel. This validation highlights the necessity, sufficiency, and soundness of the proposal.

An Explainability Model for a Better Understanding of Risk Scores And a Smooth Transition From RBAto AA. Regarding RQ#3, this thesis intents to use explainability models to obtain contextual explanations for risk

scores estimated with RBA approaches. I exploit Shapley values, a concept from cooperative game theory that assigns a value to each player in a cooperative game based on their marginal contributions to the overall outcome. I use contextual features (players) to explain the risk scores (outcome) of authentication attempts and show that these explanations can be used to reason about the appropriateness of authentication methods in a more fine-grained manner with the help of CoFrA. This supports the transition from RBA approaches to AA.

Therefore, my third contribution is to provide an explainability model that can be used for authentication decisions and, in particular, to explain the risk scores that arise during suspicious authentication attempts (*e.g.,* at unusual times or locations). The model applies Shapley values to understand the context behind the risk scores. Through a case study on 30,000 real-world authentication attempts from Orange™ , I show that risky and non-risky authentication events can be grouped according to similar contextual features, which can explain the risk of impersonation differently and specifically for each authentication attempt. Hence, explainability models can effectively improve our understanding of impersonation risks and support the transition from RBA approaches to AA. The risky authentication events can be classified according to attack types. The contextual explanations of the impersonation risk can help understanding the suspiciousness of an authentication attempt and the risk type, and hence to make a better decision.

Approach for the Selection of the Most Well-Suited Authentication Models. Regarding RQ#4, this thesis aims to provide an approach to evaluate and compare AA models conform to CoFrA. For such purpose, I exploit an approach providing constructs to apply AA models and to evaluate their quality in concrete contexts.

Therefore, my fourth contribution is an approach for the selection of the most well-suited authentication model for a given system. The approach allows to evaluate the quality of authentication models in terms of security, usability, privacy, and deployability. In contrast to the state of the art, this

is the first approach to not only compare individual authentication methods but to evaluate authentication models. The approach proposes constructs to apply an authentication model in a concrete context and to evaluate its quality in terms of security, usability, deployability, and privacy. In this way, multiple authentication models (*e.g.,* AA models, RBA models, static models) can be compared to select and tailor models for specific applications. Also, it is the first evaluation approach to allow a multi-dimensional trade-off analysis between different quality criteria instead of a one-dimensional evaluation metric. This evaluation allows choosing the correct model for an authentication system. Furthermore, they can use this approach to test and refine different models (*e.g.,* changing the contextual features, adding new authentication methods) during the whole life-cycle of the authentication system. This thesis gives an overview of the approach and evaluates it on diverse real-world authentication models. This evaluation highlights the approach's feasibility, usefulness, temporal and structural simplicity, and impact.

1.5 Thesis Roadmap

This thesis is divided into eight chapters as shown in Figure 1.3. Visually, I also divide my thesis into five parts in the figure. Preface (yellow), context (blue), contributions (green), implementation and industrialization (grey), and conclusion and perspectives (purple). While this is the introductory chapter, the second one encloses the scientific and industrial context. In the third chapter, I present the first contribution of my thesis, a systematic literature review on context modeling for AA systems. Building on this first contribution, I then present three other contributions, which are model-driven approaches for context-aware AA. In Chapter 7, I detail the implementation and industrialization of my research work. Finally, the last chapter includes the conclusions and perspectives of this thesis.

Chapter 2: Scientific and Industrial Context. The subject of this thesis is part of a rich scientific context centered on authentication and identity

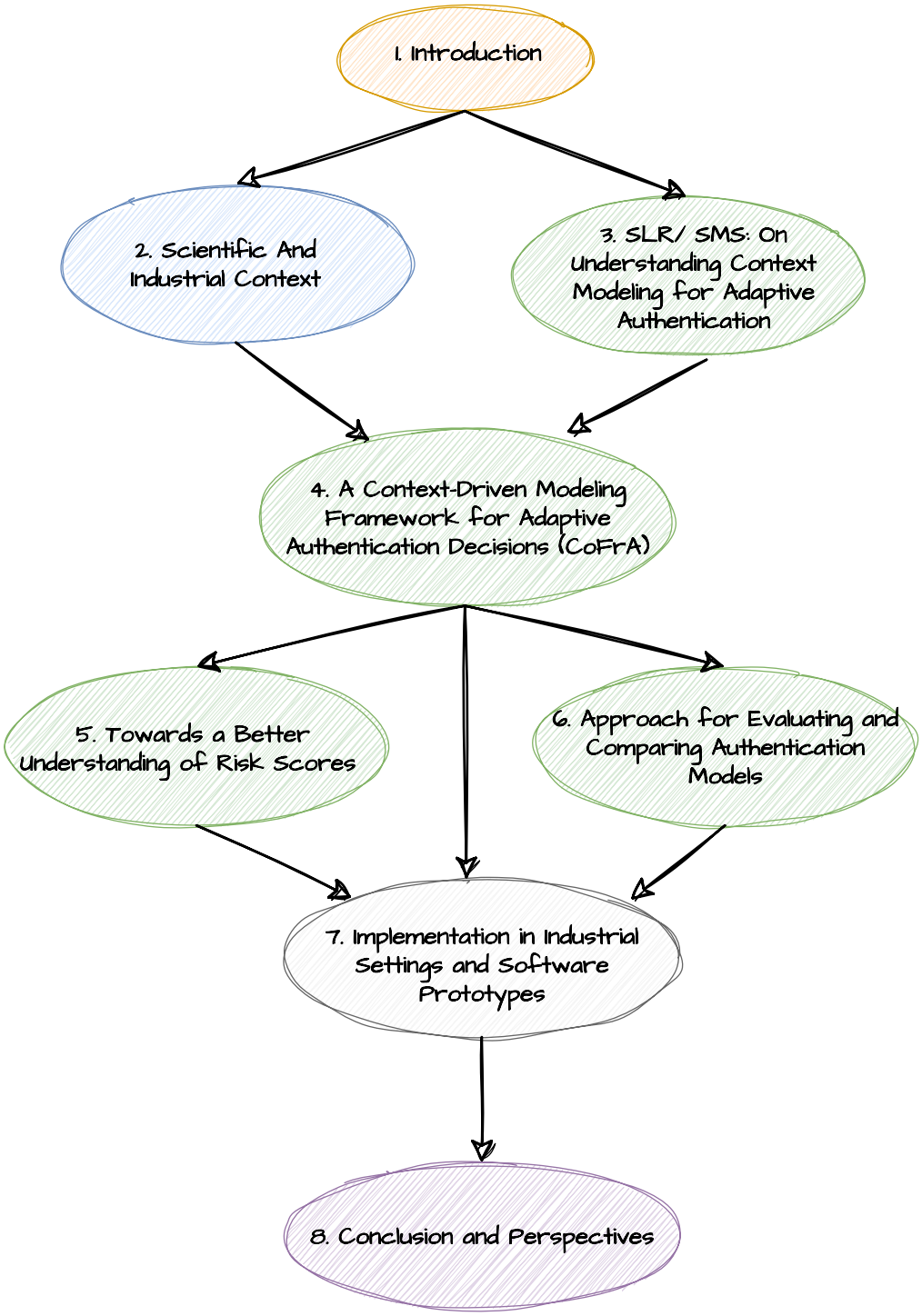

Figure 1.3 – Thesis Roadmap.

management which is a crosscutting concern in multiple domains. Sometimes the interpretations of the terms are not the same in different domains. For clarity, it is therefore important to define the vocabulary and to distinguish terms correctly from each other. Therefore, in this chapter, I present a terminological delimitation of all the terms used in this thesis. As I make use of these techniques for my contributions, I also introduce background on modeling, metamodeling, and domain-specific languages.

Then, I analyze the ongoing quest to replace passwords. I present the approaches that are proposed to leverage context information for authentication in the literature to date. I focus on trends (*e.g.,* RBA, *Multi Factor Authentication* (MFA), Zero Trust), emerging attacks on AA systems and interdisciplinary research areas tackling challenges for AA. I list and describe the most relevant works. Since my thesis presents a solution for doing AA beyond the calculation of risk scores, the idea of this chapter is to explore the existing score-based solutions and their limitations. In parallel, I also analyze the industrial context. I focus on commercial solutions for AA and existing studies on how context information is used for authentication by major online services. Also, I carried out expert surveys and need assessments to identify the thoughts of experts on leveraging context information for authentication.

Chapter 3: On Understanding Context Modeling for AA Systems. As context modeling for security application (*e.g.,* authentication systems) has not been deeply studied in the literature to date and I observe a limited usage of context information with vague descriptions and grounds, I present in this chapter, a structured review of the literature to date on CM4AA. Since my thesis presents a modeling framework for context-aware AA, the idea of this chapter is to explore the possibility of capturing a common set of contextual information for AA systems independent from the application domain, and to show the lack of standardization and a unified framework.

Chapter 4: A Context-Driven Modeling Framework for Dynamic Authentication Decisions (CoFrA). This contribution relies on Model Driven Engi-

neering (MDE), and particularly on the use of *Domain-Specific Modeling Languages* (DSML)s. I present the model-based approach for using context information for AA. The modeling framework CoFrA abstracts the domain knowledge obtained from the state of the art and the state of the practice and provides a language to determine the appropriate authentication methods in a context.

Chapter 5: Towards a Better Understanding of Impersonation Risks. In this chapter, I present the approach to explain the risk of impersonation estimated by a score-based RBA model. Based on Shapley values, I define a methodology that can be used on any score estimation model to obtain contextual explanations for suspicious authentication events. Then, I show that these explanations can be used to distinguish between different types of risks and that hence the methodology supports the transition from RBA to AA, as the explanations can be used to build CoFrA models.

Chapter 6: Approach for the Selection of the Most Well-Suited Authentication Model. A model instance of the meta-model CoFrA represents a valid model of an AA system. Different valid models exist, but it is difficult to evaluate them as multiple quality criteria (security, usability, privacy, deployability) must be considered, and these criteria may change over time. In this chapter, I present an approach for evaluating the quality of authentication models in terms of security, usability, privacy and deployability, allowing to choose the correct model for a system and to test and refine different models over time.

Chapter 7: Implementation in Industrial Settings and Software Prototypes. In this chapter, I present tooled approaches emerging from this research work as well as the implementation in industrial settings of some of the proposals. I explain the technology transfer to integrate the ideas from this thesis into the Orange™ authentication system.

Chapter 8: Conclusion and Perspectives. In this chapter, I conclude the work presented in this thesis. I discuss some limitations that motivate new ideas and future directions.

1.6 Publications

The contributions derived from this thesis have been published in international peer-review conferences. In this section, I detail all the publications that resulted from my research for the last three years.

1.6.1 International Conferences

— **Anne Bumiller**, Stéphanie Challita, Benoit Combemale, Olivier Barais, Nicolas Aillery, Gael Le Lan; "A Context-Driven Modeling Framework for Dynamic Authentication Decisions." SEAA 2022-Euromicro Conference Series on Software Engineering and Advanced Applications. 2022. [22]

— **Anne Bumiller**, Nicolas Aillery, Gael Le Lan; "Towards a Better Understanding of Impersonation Risks." 2022 15th International Conference on Security of Information and Networks (SIN). IEEE, 2022. [24]

1.6.2 International Journal

In addition, one journal article has been published:

— **Anne Bumiller**, Stéphanie Challita, Benoit Combemale, Olivier Barais, Nicolas Aillery, Gael Le Lan; "On Understanding Context Modeling for Adaptive Authentication Systems" ACM Trans. Auton. Adapt. Syst. Just Accepted (February 2023) [23]

During this thesis, I was among the 10 finalists of the "My thesis in 180 seconds" award organized by Orange™ .[2]

2. https://mastermedia.orange-business.com/pmBqkF4aOt

1.7 Thesis Environment

My Ph.D. is an industrial Ph.D.. The CIFRE (Convention Industrielle de Formation par la Recherche) Ph.D. foundation is a French doctoral program that aims to provide students with the opportunity to obtain a Ph.D. degree through an industrial research project. The program is jointly supported by the French Ministry of Higher Education and Research and industry partners. The goal of CIFRE is to promote collaboration between universities and companies to share knowledge and expertise between academia and industry. The program provides financial support to Ph.D. students who carry out their research projects in a company, under the supervision of both a university and a company mentor. The CIFRE Ph.D. foundation provides an opportunity for students to obtain a Ph.D. degree while also gaining valuable industrial experience. Hence, this thesis is supported by both the University of Rennes, and Orange™ . Orange™ , as a multinational telecommunications corporation has an interest in topics related to identity management and security and promotes this thesis to address the lack of means for leveraging context information for AA. DiverSE (formerly Triskell) is a research team of IRISA (mixed research unit grouping CNRS, University of Rennes, INRIA INSA Rennes in Rennes / Britanny / France).

Chapter 2

Scientific and Industrial Context

This chapter presents the scientific and industrial context of Adaptive Authentication (AA). The subject is part of a rich scientific context centered on authentication and identity management which is a crosscutting concern in multiple domains. I aim to give an holistic overview of this context from a scientific and an industrial point of view. I first introduce key concepts in the topic of AA and provide a terminological delimitation of the terms I use in this thesis. Then, I introduce background on model-driven engineering and domain-specific languages as I use these techniques for my contributions. Afterwards, I analyze the ongoing quest to replace passwords; first from a scientific perspective (literature on authentication trends and the evolving attack landscape); then from an industrial perspective (an expert survey to uncover needs in the industry, and commercial AA solutions). Last, I outline the interdisciplinary research areas tackling challenges for AA.

Contents

Many research initiatives to find alternatives to replace passwords have been proposed and the quest to replace passwords continues as re-

searchers and developers explore new solutions. Overall, the ongoing quest to replace passwords is driven by the desire to find an authentication solution that provides the right balance of desired properties (*e.g.,* security, usability) [34]. This is a complex challenge, and there is no one-fit-all solution due to heterogeneous devices and stakeholders interests, privacy concerns, and risks. With the rise of mobile devices, authentication solutions must work seamlessly across heterogeneous devices, including desktops, laptops, smartphones, and tablets. There are multiple stakeholders (*e.g.,* users, developers, auditors, regulators, vendors) involved in the design, development, and use of authentication systems, each with its interests. Additionally, with an increased focus on privacy, there is a growing concern about the amount of personal information that is being collected and stored by authentication systems. This makes it difficult to balance the need for security with the need to protect personal information. The number of attacks facing authentication solutions has increased in recent years, including phishing, malware, and social engineering attacks. This makes it difficult for authentication solutions to stay ahead in terms of security. Password replacements have generally failed to dislodge passwords due to the complexity of balancing usability, deployability, privacy, and security [34].

This chapter is organized as follows. First, I provide some background on AA together with a terminological delimitation in Section 2.1. Second, I introduce background on model-driven engineering and domain-specific languages. In Section 2.3, I analyze the ongoing quest to replace passwords. First, I study the literature on authentication trends emerging from the quest to replace passwords, and the constantly evolving threat landscape. Then, I provide an expert survey to identify expert thoughts on replacing passwords and using context for authentication. I also list commercial solutions for AA in this section. In Section 2.4, I outline interdisciplinary research areas tackling challenges for AA.

2.1 Terminological Delimitation for Adaptive Authentication

AA is part of a rich scientific context centered on authentication and identity management. In this section, I introduce key concepts in these topics and provide a terminological delimitation of the terms I use in this thesis.

In computer security, we mainly consider two forms of authentication: authentication of entities (verifying that either a human user or a computer entity is who he/she claims to be) and authentication of messages (verifying that the sender of a message is who he/ she claims to be) [45]. In this thesis, I focus on human entity authentication. I define an **entity** as a human that has a distinct existence. I define **authentication** as "the process of proving that an entity is genuinely who this entity claims to be" [58]. This is a commonly used definition in the research field [46, 76].

More formally, Woo et al. [1] describe the two fundamental objectives of authentication: to establish the identities of the parties involved in the process (O1), and to distribute a shared secret for further communication among the involved parties (O2). O1 means for an authenticating party to be ascertained of the identity of an authenticated party. O2 means that a secret is distributed between the involved parties to ensure future communications.

Authentication, Identification, and Authorization. Authentication is often defined as the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources [1]. Nevertheless, to ensure a clear understanding of the concepts and ideas presented in this thesis, I now clearly distinguish identification, authentication, and authorization. These terms refer to different aspects of the security process. Identification establishes who an entity is (real identity), authentication verifies whether the entity is who this entity claims to be, and authorization controls the entity's access to resources and actions.

1. https://csrc.nist.gov/glossary/term/authentication

Clearly defining and differentiating between these terms, is crucial to understand the proposals of this thesis.

Authentication is the ability to prove that an entity is genuinely who this entity claims to be and not necessarily a question of proving a unique **identity** [58]. For example, a company service may only be accessible to employees. This means that the entity claims to be an employee. Authentication here comprises the process of verifying that the entity is an employee, whereas **identification** means to verify the unique identity of the employee.

Besides identification, **authorization** also needs to be delimited from authentication. Authorization is the process of verifying what actions a user is allowed to perform [58]. Hence, in the example, it means verifying what permissions the employee has. Authentication is about the question of who the entity is and authorization is about the question of what permissions the entity has. This thesis does not focus on authorization. The authorization is orthogonal to authentication and normally takes place after it [8]. Therefore, existing authorization approaches can be integrated with authentication systems.

In this perspectives Figure 2.1 schematizes identity management incorporating the three major concepts of identification, authentication, and authorization. The order is not fixed and the processes do not necessarily all take place.

To establish the identities of the parties involved in the process (fundamental authentication objective), there is an interaction between a user, a Service Provider (SP), and an Identity Provider (IdP)/ Attribute Provider (AtP). A SP refers to an entity or organization that offers services or resources to users. An IdP verifies and authenticates the identity of users, while an AtP supplies additional user attributes that can be used by service providers (*e.g.,* for personalized services, or authorization). The user wants to access a service of the SP. The SP can manage the identities with own isolated IdP/ AtP. It is also possible for multiple SPs to connect their identity resources (IdPs and AtPs) with the online services they offer (SPs). Such IF systems provide **federated authentication** to users, meaning

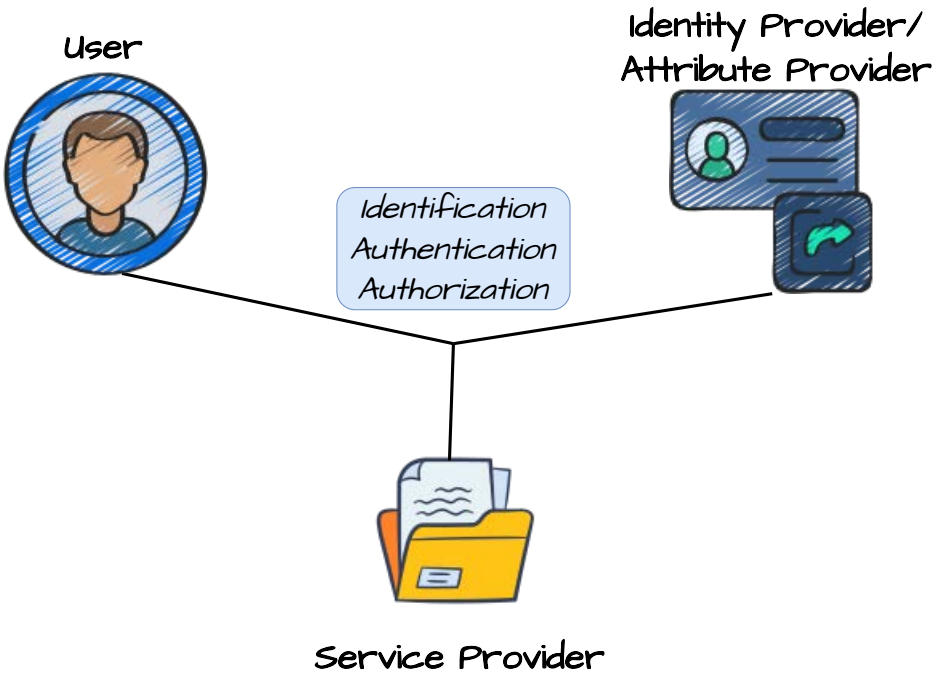

Figure 2.1 – The Concepts Identification, Authorization, and Authentication and the Relation between the User, the Service Provider and the Identity/ Attribute Provider.

that end-users can use their credentials, issued from one or more IdPs/ AtPs, to access any online service provided by a SP in the federation. The relation and data flow between the relying parties vary depending on the federation system. The research of this thesis is system independent. The proposed methods are applicable to different systems. Nevertheless, as one of the perspectives (Chapter 8) of this thesis, I plan to take a closer look at federations and to investigate the impact of AA on existing standards for federations.

Within this thesis, I focus on **authentication** for any identity management system, and more precisely on **adaptive authentication systems**.

I define an **adaptive authentication system** as an authentication system that uses context to provide the appropriate authentication method(s),

where appropriateness depends on the desired properties of the authentication method(s) in a context. In the following paragraph, I explain some more concepts related to AA systems.

Authentication Factors. Authentication methods require entities to provide information when they try to access resources in an information system or other authentication targets, such as services, devices, or systems.

Figure 2.2 – Three Well-Known Authentication Factors.

As illustrated in Figure 2.2, there are three well-known authentication factors on which authentication methods are based:

— **Something you know:** This factor refers to knowledge-based authentication, which typically involves a password or a PIN.

— **Something you have:** This factor refers to possession-based authentication, which involves a physical device such as a security key, smart card, or smartphone.

— **Something you are:** This factor refers to biometric authentication, which involves using a unique physical characteristic such as a fingerprint, facial recognition, or iris scan.

Several works consider additional factor like "where you are" ([32]) are "who you know" ([18]).

A Multi-Dimensional Trade-Off of Desired Properties. An authentication system is a system that uses authentication methods to prove that an entity is genuinely who this entity claims to be. Finding the balance between desired properties of such systems (*e.g.,* usability, security, deployability, privacy) is challenging. For this aim, the context needs to be taken into account so that the authentication method can be chosen accordingly. For example, the geolocation of an entity may influence the need to verify its legitimacy. A deviation from habits, such as an authentication attempt from another country, may be an indicator that the authentication attempt comes from an intruder. Assuming that an entity is situated at his workplace according to his habits, then an authentication challenge could be unnecessary and only disrupts the process. The role of AA is to balance security and usability, as illustrated in the example, and also other desired properties (*e.g.,* privacy, deployability) with the help of context information [10]. Deployability refers to the possibility of deployment of an authentication method (*e.g.,* reasonable implementation costs, accessibility, successful enrollment). Privacy refers to how invasive the authentication method is to privacy (*e.g.,* biometric authentication can be considered more privacy invasive than passwords due to the nature of the information (*e.g.,* uniqueness, linkability to real-world identity) it relies). A balance, which is commonly used to illustrate the classical usability-security trade-off in the security world, involves two opposing forces, intending to find the right balance between them. However, in AA, there are more factors and dimensions to balance, making the task more complex and requiring a higher level of precision.

MAPE-K Control Loop. For self-adaptive system realization in general, International Business Machines Corporation (IBM) introduced the MAPE-K control loop mechanism [33]. The MAPE-K is later discussed in the context of self-adaptive systems and is referred to as the adaptation loop. The MAPE-K adaptation loop includes the Monitor, Analyze, Plan, and Execute processes, and a shared Knowledge base. Managed resources refer to the system resources that are being monitored, analyzed, planned, and

executed by the adaptation loop.

Figure 2.3 shows a generic MAPE-K architecture for AA systems [8]. Mapping the architectural model of adaptive systems to the authentication domain, the managed resources are the authentication methods and contextual factors (available through user devices and applications via sensors and actuators), and the adaptation loop is the software layer in charge of adjusting the usage of the authentication methods according to the sensed situation.

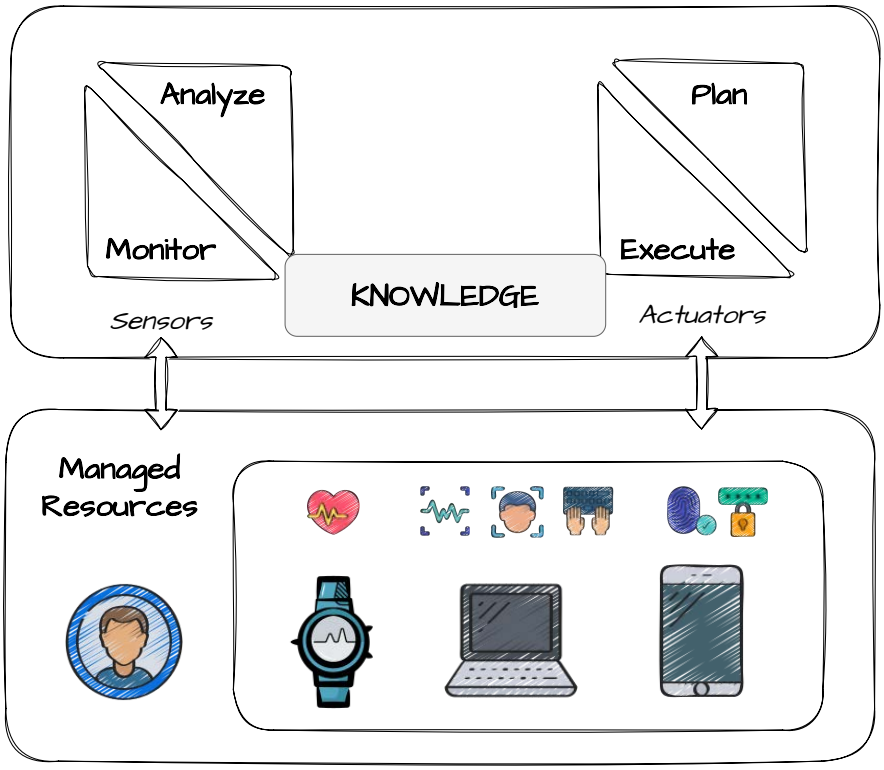

Figure 2.3 – MAPE-K Architecture for AA Systems [8].

Other Important Concepts. Commonly the term **continuous authentication** is defined as a means of proving the identity of an entity based on context information in a passive manner [8]. Passive authentication verifies the identity of an entity based on contextual information without requir-

ing direct user interaction, while active authentication requires explicit user involvement, such as providing credentials or performing an action. The terms adaptive and continuous authentication are not always clearly separated from each other. According to my definition of AA systems, I focus on providing the appropriate authentication method(s) according to the context information. I do not differentiate between active and passive authentication methods and hence do not differentiate between continuous and non-continuous authentication methods in this thesis.

To present my work, I also use the terms authentication event and user path. I define an **authentication event** as an attempt of a user to access a resource that takes place in a specific context and time. I define a **user path** as a sequence of successive authentication events. Figure 2.4 [2] shows an example of a user path. During the day, a user accesses different resources (app, mail, messenger, music, fitness, VoD) from different places (at home, in the bus, at work, in the restaurant, at the sport studio). Hence, the user is in different contexts (*e.g.*, alone/ surrounded by other people, quiet / noisy environments). For some of the accesses an authentication method is requested (password, fingerprint, face recognition, SMS OTP). The idea of AA is to choose the appropriate authentication method(s) at the different authentication attempts in the path.

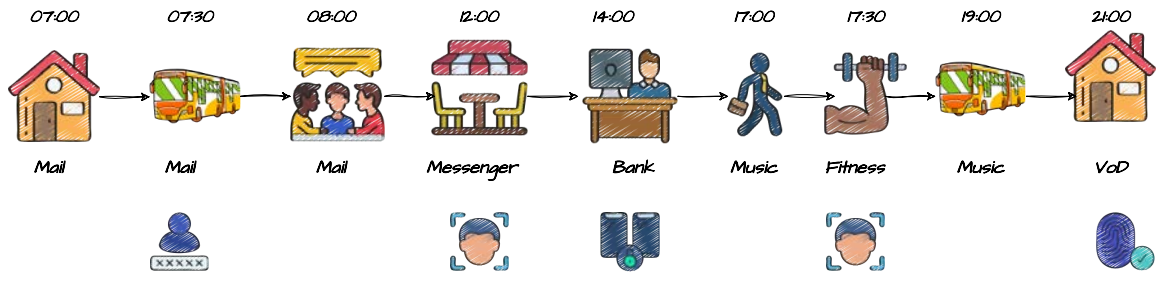

Figure 2.4 – Example User Path.

2. The authentication methods are allocated randomly in this path. It is just to give an example. I do not make any claim about the appropriateness of these models in this path.

The contributions of this thesis can be used as support for authentication engineers. In the following, I explain the role of an authentication engineer. In the remainder of this thesis, I use this term whenever I talk about people being supported by my contributions.

An **authentication engineer** is a person responsible for one or many aspects of authentication solutions within an organization. The tasks of an authentication engineer include modeling (developing models to understand/ analyze authentication requirements), analysis (analyzing the current authentication system), design (designing authentication systems), deployment (implementing and deploying the authentication system), management (managing the deployment/ maintenance of the authentication system), and reasoning (making informed decisions about the authentication system).

In the following I present an overview of the terms I introduced in this section.

- *I define an **entity** as a human that has a distinct existence.*
- *I define **context** as any information that can be used to characterize the situation of an entity.* [a]
- *I define **context-awareness** as the ability of a system, to understand and respond to its context.*
- I define **authentication** as *the process of proving that an entity is genuinely who this entity claims to be.*
- *I define an **AA system** as an authentication system that uses context to provide the appropriate authentication method(s), where appropriateness depends on the desired properties of the authentication method(s) in a context.*
- *I define an **authentication event** as an access attempt of a user to a resource that takes place in a specific context and time.*
- *I define a **user path** as a sequence of successive authentication events.*
- *I define an **authentication engineer** as a person responsible for one or many aspects of authentication solutions within an or-*

ganization.

— *I define an **IF** in this work as an approach that allows different organizations to connect their identity resources (IdPs and AtPs) with the online services they offer (SPs).*

a. Biometric and behavioural characteristics are included in this definition as they provide context about the user's identity and behavior. Authentication is not always a question of proving a unique identity, but it may be. The choice whether to use this contextual features depends on the specific goals of the authentication process. Systems that leverage biometrics and behavioral characteristics often use them as contextual features as well as authentication methods.

2.2 Model-Driven Engineering and Domain-Specific Languages

Model-Driven Engineering (MDE) improves the development of complex systems by allowing a more abstract vision than traditional programming [9]. In the last section, I introduced concepts linked to the domain of AA. This is the application domain of the contributions of this thesis. In this section, I introduce the modeling techniques of which I make use to develop my contributions.

In the *Model-Driven Engineering* (MDE) approach, the development of an application is driven by domain-specific models. **A model is an abstraction of a system that is sufficient to reason on specific properties.** A system can be described by different models linked to each other. The main idea is to use Domain-Specific Modeling Languages (DSMLs) and metamodeling to meet the requirements of a specific application domain [111]. In this section, I introduce the key principles of MDE. I first introduce the notion of model, the principles of DSMLs, and then I detail the associated metamodeling approach.

MDE is a software development approach that focuses on creating and using abstract models to drive the design, implementation, and deployment of software systems. MDE emphasizes the use of models as the primary artifacts for representing the software and its requirements, architecture, and behavior. This approach aims to increase the efficiency, productivity, and quality of software development by automating many tasks, reducing er-

rors, and promoting reusability. It also enables the reuse of models and metamodels, and the ability to evolve the metamodel to reflect changing requirements and technologies. MDE is based on the idea that modeling can provide a high-level, abstract view of the system, making it easier to understand, design, and manage complex software systems [9, 111]. **A model must cover all domain concepts (sufficiency) without specifying unnecessary, too many details (necessity)** [9, 111].

In MDE, the metamodel is the language used to describe the models that are used to represent the software systems. It defines the concepts and relationships that are used to describe the structure, behavior, and constraints of the software systems. **A metamodel is hence a model that defines the language of a model [111].** For a model to be efficient, it must be able to be manipulated by a machine. The language in which this model is expressed must therefore be clearly defined [111].

The model is conforming to the metamodel. This means that the model follows the structure and rules defined by the metamodel. The metamodel defines the concepts and relationships that are used to describe the software system, and the model provides the actual values and details for those concepts and relationships. The relation, linking the model and the language used to build it, is called *a conforming relationship* [47].

In summary, the metamodel-model relationship in MDE is a critical component in providing a structured and consistent approach to modeling software systems. It defines the concepts and relationships used in modeling, and acts as a blueprint for the actual models, ensuring that they follow a common structure and set of rules. Figure 2.5 shows the relationship between the system, the model, the metamodel and the language. In Figure 2.6, I take an example used in [47], which uses cartography to illustrate MDE. In this example, a map is a model (a representation) of reality, with a particular intention (*e.g.,* a road map, administrative map, relief map). In cartography, it is essential to associate with each map the description of the "language" used to produce this map. This is done in the form of an explicit legend. To be usable, the map must conform to this legend. Several maps can conform to the same legend. The legend is then

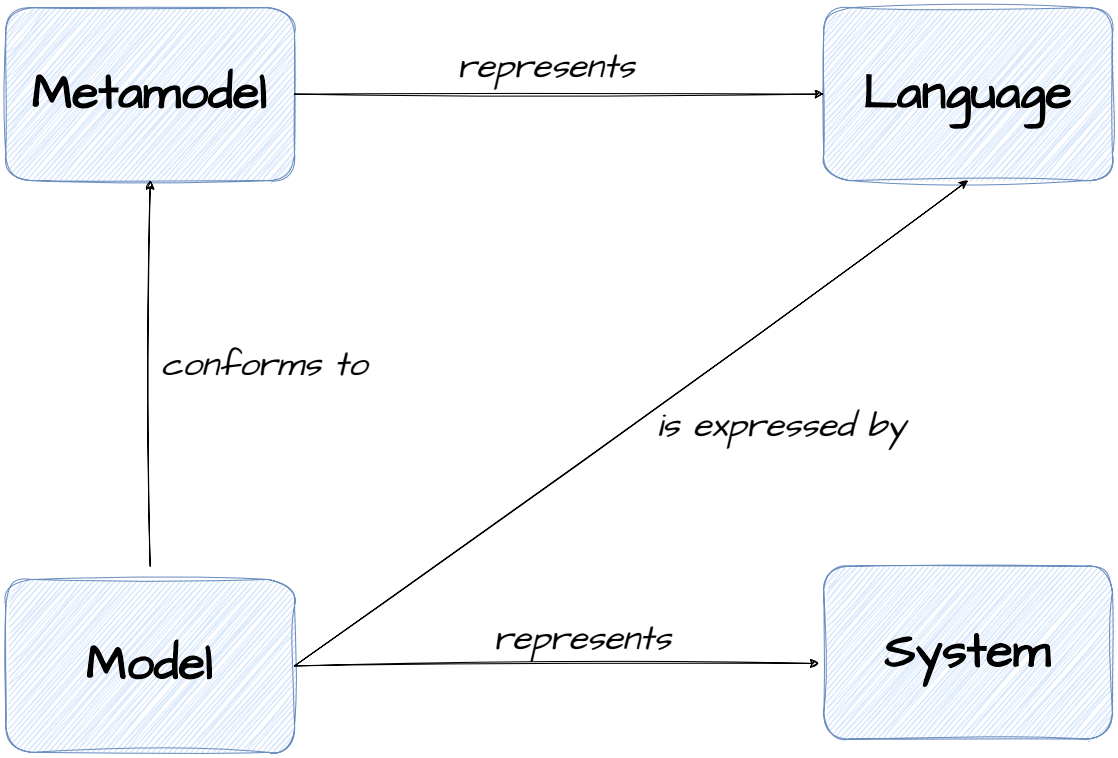

Figure 2.5 – Relationship Between the System, the Model, the Metamodel and the Language.

considered as a model representing this set of maps and to which each of them must conform.

2.3 The Quest to Replace Passwords

In this section, I analyze the ongoing quest to replace passwords. From a scientific point of view, I study the literature on the authentication trends emerging from the quest to replace passwords, and the constantly evolving threat landscape in Subsection 2.3.1. From an industrial point of view, I provide an expert survey to uncover experts' thoughts on replacing passwords and using context information for authentication in Subsection 2.3.2. Also, I list commercial solutions for AA in Subsection 2.3.3. Last, I outline

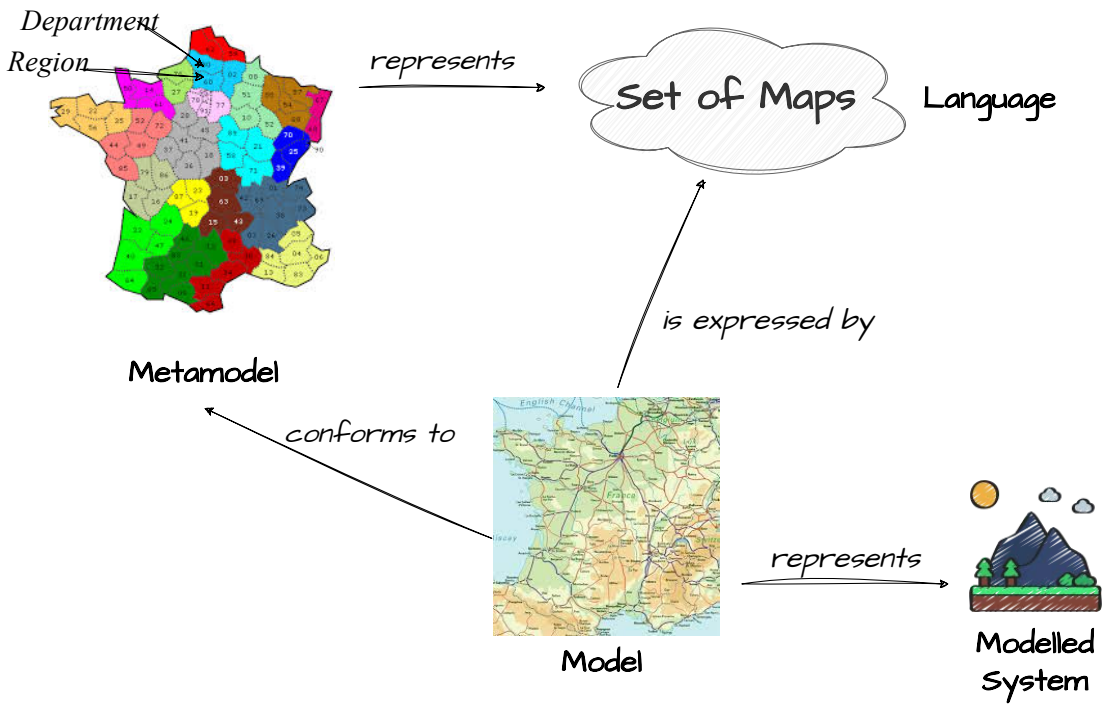

Figure 2.6 – Relationship Between the System, the Model, the Metamodel and the Language - Example [47].

interdisciplinary research areas tackling challenges for AA in Section 2.4.

2.3.1 Literature to Date: Authentication Trends and the Changing Attack Landscape

Over forty years of research have demonstrated that passwords are plagued by security issues and inconvenient for users [16]. The relevance of password reuse has been shown in [36] and [95]. The quest to replace passwords with more secure and convenient authentication methods, such as Multi-Factor-Authentication (MFA), Risk-Based Authentication (RBA), or Zero Trust (ZT), is emerging. MFA is an authentication process where a user is required to provide multiple authentication factors to provide an extra layer of security beyond password authentication. RBA is a method

of estimating the level of risk associated with an authentication attempt to adjust the authentication process. According to the National Institute of Standards and Technology (NIST) Special Publication 800-207 [3], ZT security models assume that an attacker is present in the environment and that an environment is not trusted. In this paradigm, an organization must assume no implicit trust and continually analyze and evaluate the risks. Hence, these protections usually involve continually authenticating the entities of each access request. Hence, the concept of ZT involves a shift from traditional authentication to a more granular, request-based approach. In ZT, all authentication requests are verified and validated, regardless of the trust in the authenticating entity.

Gavazzi et al. [49] present a study of 208 popular websites to understand the availability of MFA and RBA on the web. The study found that only 42.31% of sites support any form of MFA and only 22.12% of sites block an suspicious access attempts. However, the presence of IF [4] providers that offer MFA and/or RBA increases the availability of MFA and RBA to 80.29% and 72.60% respectively. However, using IF providers comes at a privacy trade-off as nearly all IF providers that support MFA and RBA are major third-party trackers. The study concludes that **more work needs to be done to make MFA and RBA more widely available and secure** for online users. Ometov et al. [94] review the evolution of authentication systems from single-factor authentication to MFA. They survey **available and emerging sensors** for user authentication and discuss **challenges** from both the user and service provider perspectives. The paper also proposes an MFA system and discusses **future trends in MFA**. Das et al. [37] propose a systematic literature review of 623 papers focusing on MFA technologies. They further analyze the papers performing any user evaluation research and showed that researchers found **lower adoption rate** to be inevitable for MFA, while avoidance was pervasive among **mandatory use**. Wiefling et al. [127] present an in-depth analysis of RBA

3. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

4. A federation is a process that allows the conveyance of identity and authentication information across a set of networked systems. It is an approach that allows different organizations to connect their identity resources (Identity Provider (IdP)s) with the online services they offer (Service Providers (SP)s).

as a method of strengthening password-based authentication. The authors analyze the behavior of two RBA implementations used by major online services and collect data from 780 users over 20 months to provide a behavior analysis. The study provides insights into the **most suitable contextual features for RBA**, and factors affecting RBA performance. The results show that **RBA needs to be carefully tailored to each online service**, as even small configuration adjustments can greatly impact its security and usability. The paper provides recommendations on the selection of features, their weightings, and risk classification to benefit from RBA. The same authors also present a study on popular online services in 2018 and found evidence that **Google, Facebook, LinkedIn, Amazon, and GOG.com were the early adopters using RBA** [129]. In [128], the **usability and security perceptions** of two variants of RBA are evaluated and compared to password authentication. The study also identified **usability problems** with RBA and provided recommendations for improvement. This study provides a deeper understanding of user perception of RBA and helps to improve its implementation for better user acceptance. In [131], the authors collect data from 3.3 million users and 31.3 million login attempts over a period of more than one year. The results provide insights into the **real-world characteristics of RBA** and its configurations, along with a machine learning-based method for optimizing RBA parameters. [5] In [118], the authors study **challenges and steps required to mitigate to ZT** architectures according to the NIST Special Publication SP800-207. Three major steps are outlined in the paper: identifying devices and users (1), removing explicit trust (2), and externalizing workflows (3). They also discuss a case study of ZT implemented by Google, called "BeyondCorp". In [35], the authors present the **advantages and disadvantages of ZT** and its potential for future authentication security. This paragraph discusses the emergence of new authentication solutions, such as Multi-Factor-Authentication (MFA), Risk-Based Authentication (RBA), and Zero Trust (ZT). Most works study the availability (*e.g.,* user adoption rates) of these solutions and discuss challenges. Overall, these

5. Wiefling et al. propose a webpage to understand RBA: `https://riskbasedauthentication.org`.

papers demonstrate a growing interest in finding alternatives to passwords and that there is not yet a common solution.

As authentication systems become more sophisticated, attackers also find new ways to bypass them. The realization of authentication systems that adapt to context opens new vulnerabilities and avenues for attacks. In [8], the authors identify the following issues: context manipulation, device theft, mimicry attacks, metric reliability, and attacks directed to the system. In [28], the authors analyze *Impersonation-as-a-Service* (ImpaaS) attacks applied to bypass risk-based authentication systems. In their work, they put forward **capabilities required to systematically bypass different authentication solutions**. The different capabilities of the attackers point out the need to consider the differences between the risks of different attacks for adapted authentication decisions. In [69], the authors explore **the use of browser fingerprinting techniques in authentication systems** and their potential security implications. The authors investigate the process of how target websites extract fingerprints from users' devices, and how phishing attackers can use this information to deceive risk-based authentication systems and bypass two-factor authentication. The study also looks at the evolution of browser fingerprinting practices in phishing websites over time and finds that attackers targeting certain financial institutions are becoming more capable of using this information for malicious purposes. The authors have disclosed their findings to vulnerable vendors to address the threat posed by these attacks. This paragraph discusses the evolving threat landscape, and explains how attacker find new ways to bypass RBA and MFA systems.

2.3.2 Experts Thoughts on Replacing Passwords and Using Context for Authentication

To reflect the current real-world practice of authentication, I aim to provide insights into the actual state-of-the-practice and the challenges and limitations that organizations and experts face. Therefore, I conducted an expert survey during the first year of my Ph.D (2020/ 2021). It helped me

to provide access to specialized knowledge and experience that may not be available through other sources. The expert surveys presented in this chapter, helped me to gain insights into the state-of-the-practice of replacing passwords and using context information for authentication. The experts have deep knowledge and experience in the field of identity management and authentication.

The questions fall into three categories: the **use of context information for authentication** (1), **impersonation risks and frauds** (2) and **desired properties of authentication methods** (3). The totality of the questions and anonymous answers are available on my companion webpage. [6]

The Expert Panel. The expert panel consists of eleven people working on identity management, authentication, and system security. They come from a multinational telecommunications corporation (Orange™), a multinational aerospace corporation (Airbus), two European university research institutes (University of Hohenheim, Chouaïb Doukkali University El Jadida), and a medium-sized family-owned company for smart sensor and image processing technologies (Wenglor Sensoric). I targeted people aware of the opportunity to use context information for authentication. It is not possible to identify and survey this entire population. Hence, I have chosen people from my professional network. All those people are authentication engineers and, therefore, users of the approaches presented in this thesis. Table 6.2 shows the job titles of the experts.

The Survey Procedure. In the first stage, the main idea of using context information for authentication was presented to the expert panel, followed by instructions on answering the online survey. [7] I invited them to contact me in case of any questions or if they are interested in having an in-depth discussion. In the second stage, the experts answered the three question types. Three of the experts contacted me to discuss the topic further.

6. Cf. https://github.com/BumillerAnne/CoFrA
7. https://msurvey.orange.com/AA_ENG

Table 2.1 – Job Titles of the Experts Participating to the Survey About Replacing Passwords and using Context for Authentication.

	Job Title
Auth. Eng. 1	Identity Transverse Architect
Auth. Eng. 2	Architect for Access Platforms
Auth. Eng. 3	PhD Student: Behavioral Biometrics
Auth. Eng. 4	Project Manager: AA
Auth. Eng. 5	System Architect of the Digital Identity Train
Auth. Eng. 6	Direction of the Identity and Trust Research Program
Auth. Eng. 7	Architect for Projects for Identity Anticipation and Research
Auth. Eng. 8	Head Of Identity and Access Management for Users
Auth. Eng. 9	Professor (Chair of Information Systems)
Auth. Eng. 10	Master student of Big Data Analytics and Biometrics
Auth. Eng. 11	Team Leader IT-Infrastructure

Analysis of the Responses. I first asked the experts what AA means for them.

I provide here a list of anonymous answers:

— *"The ability to find the best compromise between security and fluidity, by adapting the authentication process to the sensitivity of the service, the context, the means of authentication available to the individual, and even their authentication preferences."*

— *"Capacity of the authentication system to send challenges generating the least possible friction in the user path for maximum security as a function of the criticality of the resource requested and the current risk that the request is illegitimate. The risk is continuously assessed on the basis of a set of attributes of the request at time T."*

— *"The use of more varied information than normal to offer different, more appropriate authentication methods.*

— *"Offer the user "soft" (frictionless) authentication that is best suited to the known environment (manage habits)."*

— *"Adapt the authentication to be carried out by the user according to the context at a given moment, while guaranteeing the right level of security."*

— *"The possibility of modifying the authentication process depending on the context, service and usability required."*
— *"Adapting to the customer's means in order to offer the best possible experience that meets the level of security required to access the service."*
— *"A mechanism that seamlessly chooses the best-fitting approach for authentication."*
— *"Depending the level of trust (results of external parameters analysis like geolocation) your authentication journey is more or less simple to ensure that it is really you."*
— *"User-friendly authentication process for services/demands that makes the authentication process for the user as easy and automated as possible and for the system/requirement as secure and cheap as possible."*

All the answers acknowledge the importance of maintaining a balance between security and usability. Several experts mention the need to adapt the authentication process based on the context, such as the sensitivity of the service, the risk level, the user's environment, or the current situation. Multiple experts highlight the goal of providing a seamless and user-friendly authentication experience, minimizing friction and effort required from the user. The answers differ in terms of the contextual features they consider for the adaption. Each expert uses its own terminology and phrasing. The answers vary in their level of specificity and detail. Some experts focus on the user experience and convenience, while others emphasize security, risk assessment, or cost-effectiveness. To ensure consistency, effective communication, knowledge transfer, and to advance the research field, uniforming the understanding among experts is important.

The Use of Context Information for Authentication. For the analysis of the use of context information for authentication, I asked the experts whether contextual information is used to decide about the authentication methods to use in the current authentication system. I then asked which context information is used. For the contextual features IP address, device, web browser, user behaviour, localization, luminosity, time, user habits,

persons in proximity, and user activities, I asked the experts to evaluate their importance (1: not important at all, 10: very important). I asked the experts whether the contextual information is used sufficiently. Then, I asked whether and for which purposes other than authentication contextual information is used. I also asked whether the experts find that it would be beneficial to use this same contextual information for authentication.

Most of the experts claim that **context information is not sufficiently used for authentication**. Nine out of eleven experts agree that context information is used for authentication, but eight of them claim that it is not sufficiently used. The two experts claiming that context information is not used mention the reason that there is a "lack of knowledge about how to use it", and a "privacy problem". To the question of why not enough context information is used for authentication, the experts mention among others the following reasons:

- *"Difficulty in identifying them"*
- *"Difficulty in retrieving them"*
- *"Difficulty in interpreting them"*
- *"Privacy problems"*
- *"Not enough correlation of data between the different channels (between devices, between uses) during a person's digital life"*
- *"Need to adapt our technical solution"*
- *"Because most authentication methods mainly work the same independently of the context"*
- *"Legal constraints"*

Hence, experts need more support to use contextual information for authentication. Furthermore, the great diversity of answers to the question of which context information is used (*e.g.,* device, risk score, localization, browser fingerprint) shows that needs and perceptions vary greatly. This also points to the need for more support and unification. Table 2.2 shows which features are considered more or less important by the experts. Experts consider the device, the user behaviour, user habits, and the geolocation as the most important.

Nine out of eleven experts think that context information used for other

Feature Name	**Mean Importance**
IP Address	6.18
Device	8.27
Web Browser	5.91
User Behaviour (mouse movement, keystrokes, ...)	7.27
Localization	7.91
Luminosity	2.73
Hour of the Connection	5.73
User Habits	7.91
Nearby Persons	5.36
User Activities (running, driving, ...)	4.82

Table 2.2 – Importance of Different Contextual Features According to the Experts.

purposes than authentication should also be used for authentication.

Impersonation Risks and Frauds. For the analysis of impersonation risks and frauds, I asked the experts whether the authentication process is designed to counter identified risks. I also asked whether the risks are assessed during the authentication process and whether this assessment can trigger a change in the authentication path. I further asked which risks are assessed. Most of the experts claim that different **impersonation risks and frauds are not addressed during the authentication process**. Eight out of eleven experts are aware of different risk types, but agree that they are not addressed. The results show that risks are a concern for the experts but they are not addressed during the authentication process. To take full advantage of context information to identify risks, experts need more support. I observed a great diversity of answers to the question of which risks are important (*e.g.*, fraud, attack, the user is not who he claims to be, stolen password, fast location change, data loss, identity loss, credential loss). This shows that the experts do consider risks at different levels and that notions of risks are not unified in the domain. Support for using contextual information to identify risks and to distinguish between different risk types is necessary to take full advantage of context information for authentication.

Desired Properties of Authentication Methods. For the analysis of the desired properties of authentication methods, I asked the experts which authentication methods are proposed to the users and whether always the same methods are proposed. I then further asked how the methods change. I asked whether the experts think that enough authentication methods are currently used and why not more methods are proposed. I then asked how the relevance of an authentication method is assessed in a user path. Last, I asked whether the properties usability, security, deployability, and privacy are important for the evaluation of the authentication methods. The experts mention the following authentication methods to be used:

- *"Password"*
- *"Mobile based"*
- *"Knowledge factor"*
- *"Possession factor"*
- *"Being factor"*
- *"Biometrics"*
- *"OTP"*
- *"Authentication of the line"*
- *"Temporal PIN or password"*
- *"Tokens"*
- *"Behaviour biometrics"*

The answers show that experts are aware of the multiple authentication methods and differ them according to the factors they concern. Ten out of eleven experts claim that **not enough authentication methods are used** and that the exclusive use of passwords is not sufficient for diverse reasons. They mention for example that it is "difficult to adapt 'as closely as possible' to the user's context with very general authenticators". To the question of why not enough authentication methods are proposed the experts give among others the following answers:

- *"It is a question of time"*
- *"Not enough "finesse" in the user experience friction"*
- *"The combination of 'weak' authenticators should produce a strong result"*

— *"Behavioural biometrics and log analysis is missing"*
— *"Lack of flexibility in the authentication system"*
— *"Some methods are not available for all users"*
— *"Requires additional development"*
— *"Cost of implementation"*
— *"Lack of knowledge on the part of the project manager"*
— *"Lack of strategic vision"*

To the question of how the relevance of authentication methods is assessed in a user path, the experts give among others the following answers:

— *"Normally not assessed while being used/executed, but would be a good idea to be assessed by the user to get more feedback for the suitability in that situation"*
— *"Can not be evaluated outside of the concept by design and/or marketing"*
— *"Efficiency is linked to factors"*
— *"Depending on the "discretion" of use, and simplicity (minimum friction)"*
— *"Depending on its level of security"*
— *"Level of adoption by users"*
— *"Ease of use (including enrolment)"*
— *"Suitability for different channels (shop, online, customer service)"*

At least five experts consider each of the properties: security (9), deployability (5), usability (10), and privacy (9) essential to evaluate authentication methods.

Results. The survey results show that the experts need support to take full advantage of context information for authentication. I show that the experts are interested in **using contextual information** beyond risk scores, and that they do not yet make sufficient use of it. **Taking into account multiple risks** for authentication decisions and not only a risk score also interests the experts, and they find that this is not yet being done sufficiently. The **use of diverse authentication methods and their evaluation** regarding the context and along with the properties **se-**

curity, **usability**, **deployability**, and **privacy** is considered necessary by the experts.

2.3.3 Adoption in Practice

In [129], the authors analyze risk-based authentication "applied in the wild" and determine the contextual feature set used during user login by LinkedIn, Facebook, Google, Amazon and GOG.com. The adoption rate of MFA in practice remains low (Google $< 10\%$ [78], Facebook $= 4\%$ [92], Twitter $= 2.6\%$ [8]).

Furthermore, I searched for commercial AA solutions. With the help of *Expert Insights*[9], a cybersecurity research and review website, I identified common solutions. *Expert Insights* provides guides, expert advice and industry insights to help organizations to make informed, decisions when selecting cybersecurity solutions. They propose a list of top AA solutions. [10]

Prove MFA. Prove offers multi-factor authentication solutions that use users' mobile phones and phone numbers (phone-centric authentication) as the primary authentication method. The solution verifies a client's identity and validates the information provided by the client, assigning a trust score to each login to assess risks. The solution analyzes behavioral and phone-related indicators of suspicious activity. [11]

Duo. Duo offers MFA and *Single Sign-On* (SSO) to allow access while only verifying once the identity. Administrators can configure AA policies based on the user's location, device and role, among other factors. Duo then scans these security policies for anomalous access attempts to securely enable or deny access. [12]

8. https://transparency.twitter.com/en/reports/account-security.html#2021-jul-dec
9. https://expertinsights.com/
10. https://expertinsights.com/insights/the-top-10-risk-based-authentication-rba-solutions/
11. https://www.prove.com
12. https://duo.com

IBM Security Verify Access. This solution supports user authentication via one-time passwords, email verification and knowledge-based questions, and enables password-less SSO. Using the risk scoring engine, administrators can configure risk-based authentication policies to prevent anomalous login attempts. The risk scoring engine analyzes the login patterns of users, including information about their devices and regular session activities to detect and prevent unusual login attempts. [13]

Kount Control. Kount Control uses an AI-driven technology to analyze user login behavior based on device status, IP address reputation, geolocation and mobile and proxy indicators. Using this data, Kount detects anomalous access attempts that could be the result of attacks. In the case of a high-risk login, the system requires the users to verify their identity via an additional authentication method. [14]

LastPass MFA. LastPass MFA is an adaptive solution that combines contextual information such as geolocation and IP reputation, with biometric information, in order to analyze a user's risk score and verify their identity. [15]

Okta Adaptive Multi-Factor Authentication. Okta Adaptive Multi-Factor Authentication uses contextual factors such as device trust and geolocation to calculate a risk score for login attempts before prompting users to further verify their identity. The platform supports secondary authentication via mobile app push notifications and biometrics, as well as more traditional methods, including security questions and OTPs [16] sent via SMS, phone call and email. [17]

13. https://www.ibm.com/fr-fr
14. https://kount.com/products/kount-control/
15. https://www.lastpass.com/fr
16. A password sent via SMS, which is generated to be used and valid only during a single session or transaction.
17. https://www.okta.com

OneLogin SmartFactor Authentication. The solution aims to adjust authentication requirements in real-time based on the risk level associated with the context of each login attempt. The engine calculates risk scores based on user location, device security and user behavior, in order to determine the most appropriate action for each login to allow, deny or challenge the login by requesting up further verification. SmartFactor Authentication supports SMS, email and voice OTPs, security questions, push notifications via an app, and biometrics. [18]

Ping Identity PingOne Risk Management. The solution uses machine learning models to learn each user's login behavior, analyzing risk predictors such as device type, operating system, browser version, date and time to distinguish between normal user login behavior and anomalous login attempts. Authentication policies that enable the system to grant, deny, or challenge access can be implemented based on a risk score calculated using the data. [19]

SecureAuth Identity Platform. SecureAuth's Identity Platform utilizes artificial intelligence to produce a risk score for login attempts based on contextual information, such as device health, location, IP reputation and user behavior. If the risk associated with a login attempt is too high, SecureAuth will request further verification from the user. [20]

In summary, I observe that industrial solutions mainly aim **assessing the risk or, conversely, the trust in the user** often based on AI and machine-learning technologies to calculate risk scores and to detect anomalies and derivations from user patterns. Table 2.3 summarizes the different solutions. The providers call themselves by different names, although the approaches are all quite similar. They are mainly based on the calculation of a risk scores. There is a lack of unification. The current state of commercial solutions in authentication is often confusing, with concepts like MFA,

18. https://www.onelogin.com
19. https://www.pingidentity.com/en.html
20. https://www.secureauth.com

RBA, and SSO being mixed up, leading to a lack of clarity for authentication engineers. This thesis addresses this issue by contributing to the systematization of knowledge, providing a common modeling framework and language, supporting the transition from RBA to AA, and facilitating the comparison and evaluation of solutions. These contributions aim to enhance a common understanding among researchers and practitioners and enable a more impactful integration of commercial and academic initiatives in the field of authentication.

2.4 Interdisciplinary Research Areas Tackling Challenges for Adaptive Authentication

AA is an emerging interdisciplinary research field. The research is mainly driven by four communities: security and privacy, machine learning, identity management, and adaptive systems [8].

Figure 2.7 visualizes the interdisciplinary research areas whose interaction can tackle challenges for AA. In the following paragraphs, I discuss related work in all these four areas.

Machine Learning. There are several works proposing machine learning models for context classification and risk prediction in the context of AA. As stated before, the goal of my thesis is to go beyond the calculation of risk scores and to propose a more fine-grained mapping between context information, threats, risks, and authentication methods. In this paragraph, I highlight the variety of approaches that use machine learning to assess risks. These related works aim to assess the risk as accurately as possible and to distinguish correctly between the legitimate user and an attacker. Therefore, the risk scores are referred to as black boxes and none of these works differentiates between different risk types or deals with the appropriateness of the authentication methods according to the context.

Achituve et al. [3] propose an attention-based architecture for classifying online banking access attempts as either fraudulent or genuine. They achieve high classification accuracy with their method. De Silva et al. [39]

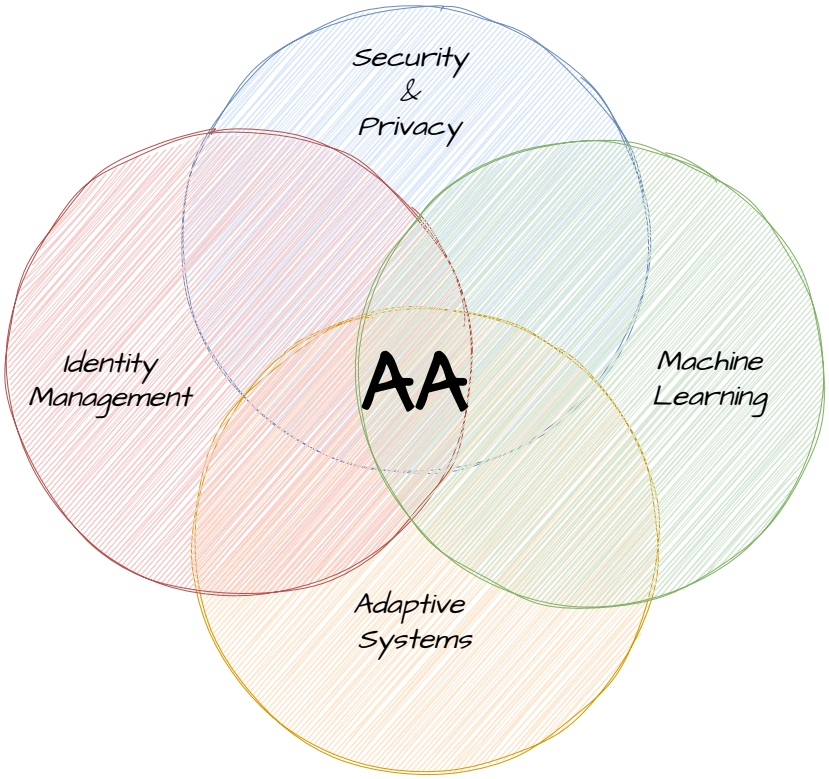

Figure 2.7 – Diagram Visualizing the Interdisciplinary Research Areas whose Interaction can Tackle Challenges for Adaptive Authentication [8].

propose an approach based on collectively analyzing the user's behavior, and device and network-related information with the help of a recurrent neural network algorithm named Long Short-Term Memory (LSTM). The decision of re-authentication or grant of access to the system is taken based on a risk score. Valero et al. [122] propose an authentication system that uses machine learning techniques based on the detection of anomalies. Brown et al. [20] present recurrent neural network (RNN) language models augmented with attention to detect anomalies in system logs. Kaiafas et al. [59] propose a novel method to extract features and a supervised learning technique for classifying authentication logs trustfully. The models are Random Forest, LogitBoost, Logistic Regression, and ultimately Majority Voting which leverages the predictions of the previous models and gives

the final prediction for each authentication event. Alom et al. [6] propose a novel approach for Intrusion Detection Systems (IDSs) using unsupervised Deep Learning (DL) techniques. Freeman et al. [48] propose a statistical framework for identifying suspicious login attempts based on the IP address and the device of the user. Chen et al. [30] present a framework named BEA, a general anomaly detection framework that can effectively detect anomalies on a dynamic bipartite graph with burstiness.

Main Challenges. There is a lack of fine-grained mappings between context information, threats, risks, and authentication methods. The machine learning based approaches tend to calculate risk scores as black boxes without distinguishing different risk types or authentication methods according to the context. The related works propose statistical or machine learning-based approaches to assess risks accurately and classify authentication attempts into legitimate and intrusive attempts. However, there is a need to manage complex mappings between contextual information and authentication methods based on identified threats and risks. While blocking risky attempts is an essential part of security, the choice of authentication methods should also take into account factors (*e.g.,* usability).

Identity Management. Identity standards are sets of guidelines and technical specifications that help organizations and individuals to establish, verify and manage digital identities. In this paragraph, I aim to explain some of the many identity standards that authentication engineers can use to improve the security and privacy of their authentication solutions. It is important for authentication engineers that adopt AA solutions to stay informed about the latest developments in identity standards to ensure that they are using the most secure and effective methods for managing digital identities. However, it is important to recognize that most of these standards are primarily designed for static authentication rather than AA. While they do offer the possibility to incorporate context information, they do not specify how to implement it effectively.

Some of the most important identity standards include:

— **OpenID Connect (OIDC):** A widely adopted protocol for authentication and authorization that enables third-party applications to verify the identity of users and access certain user data. [21]

— **Security Assertion Markup Language (SAML):** An *Extensible Markup Language* (XML)-based framework that enables the secure exchange of authentication data between organizations. [22]

— **FIDO (Fast IDentity Online) Alliance:** An industry consortium dedicated to advancing the state of online security through the development of open standards for simple and secure authentication. [23]

— **WebAuthn:** The Web Authentication API (also known as WebAuthn) is a specification written by the W3C and FIDO, with the participation of Google, Mozilla, Microsoft, Yubico, and others. The API allows servers to register and authenticate users using public key cryptography instead of a password. [24]

— **National Institute of Standards and Technology (NIST):** A federal agency that provides technical guidelines and standards to improve the security and privacy of sensitive information. NIST's Digital Identity Guidelines (SP 800-63) is a widely recognized resource for identity management and authentication. [25]

Rivera et al. [103] analyze authentication solutions based on standards such as the WebAuthn and FIDO. These standards aim to replace or complement traditional username and password authentication methods. The analysis compares and tests the current implementations of these standards, including their adoption and integration with existing systems, such as web applications, services, desktop, and server operating systems. The study provides a high-level analysis of the use cases of these standards. Hu et al. [56] analyze FIDO UAF (Universal Authentication Framework) Protocol. The paper discusses the cryptographic abstractions used in the

21. https://openid.net/connect/
22. https://www.oracle.com/security/cloud-security/what-is-saml/
23. https://fidoalliance.org/
24. https://webauthn.guide/#about-webauthn
25. https://www.nist.gov/

registration and authentication protocols of FIDO UAF and evaluates the security properties of the protocol. The paper also proposes three attacks, which aim to impersonate the legitimate user and pass FIDO UAF authentication. The attacks are based on assumptions such as an attacker corrupting the software on the user's device or two users sharing a FIDO roaming authenticator. Wilsen et al. [132] explain that while OAuth 2 provides a framework for authorizing applications to call APIs, it is not designed for authenticating users to applications. The OpenID Connect (OIDC) protocol is designed to provide an identity service layer on top of OAuth 2, enabling authorization servers to authenticate users for applications and return the results in a standardized way. The article discusses the need for a standard solution and how an application can use OIDC to authenticate a user. Morkonda et al. [86] investigate the privacy implications of using OAuth 2.0. The study collected data on the use of OAuth-based logins in the Alexa Top 500 sites per country for five countries, and evaluated popular services accessing user data from the authentication systems of four identity providers. The results reveal that services request different categories and amounts of personal data from different providers, with some choices more privacy-intrusive than others. The study identifies areas that could improve user privacy and help users make informed decisions.

Main Challenges. While adopting AA solutions, authentication engineers must stay updated on the latest developments in identity standards to ensure they employ the most secure and effective methods for managing digital identities. Various research papers have analyzed and explored the implementations and security aspects of identity standards like WebAuthn, FIDO, and OIDC. One of the main challenges is the constant evolution of identity standards due to technological advancements, changing regulations, and emerging security threats. Moreover, achieving interoperability among different systems while incorporating AA presents another significant challenge. Most existing standards were originally designed with a traditional, static authentication model in mind, and incorporating glsAA is not straightforward. Therefore, de-

veloping common protocols and guidelines that allow different systems to communicate and work seamlessly while incorporating AA can be a complex task for authentication engineers.

Adaptive Systems. Several adaptive system architectures for AA have been proposed. Calvo et al. [27] propose an adaptive system for automatically adapting security controls to changing risk scenarios in real time. The goal is to provide context-aware decision-making for security managers in response to changes in risk indicators and levels. The features IP address, login time, availability of cookies, device profiling, and failed login attempts are implemented in the AA system from Hurkala et al. [57]. The authors explain the design and motivation behind the adaptive system and highlight the security threats and risk factors at the system level. Lindeann et al. [70] describe an AA system that adjusts the level of security required for a transaction based on the user's risk level. The system consists of an AA module, a risk module, and an assurance analysis module. The risk engine analyzes data related to the user to determine a risk value, and the assurance analysis module determines the necessary assurance level required for the transaction. The AA module then selects one or more authentication methods to ensure that the transaction is secure. The adaptive systems community helps not only the design of AA, but also provides guidance from engineering tools like FESAS [62] or Genie [13]. These tools offer assistance in developing software for adaptive systems and can serve as a basis for creating similar tools that are tailored to the specific requirements of the authentication domain [8].

Main Challenges. These adaptive system architectures should be able to handle different types of authentication methods and risk assessment models, and should be easily adaptable to new technologies and risks. Efforts are necessary to map research in adaptive systems to the field of AA to help improve AA architectures.

Security and Privacy. Security and privacy are critical concerns in the research area of AA to ensure that these systems can effectively and safely authenticate users while protecting their sensitive information and privacy. Authentication systems deal with sensitive information and user data.

In [8], the authors identify issues related to privacy that derive from the need to comply with privacy regulations like the *General Data Protection Regulation* (GDPR). They mention the following issues: the privacy of data used for AA, the privacy of contextual data, which can reveal very sensitive information about the user, such as location or activity, and the incorporation of user consent for authentication-related transactions without decreasing the overall usability. Wiefling et al. [130] outline that context-aware authentication may expose potentially sensitive personal data, which conflicts with user privacy rights. The authors propose some potential improvements to balance privacy in context-aware authentication systems, and evaluate some privacy-preserving RBA enhancements with real-world data from 780 users. However, they state that privacy improvements are limited to certain parameters, and further research is needed to achieve widespread adoption of privacy-preserving authentication with high user acceptance. Liu et al. [73] discuss the growing privacy concerns of mobile applications on smartphones, which often request context information from users. The paper proposes using context-awareness to improve SSO solutions, thereby enabling mobile users to protect their private information. The privacy-based adaptive SSO (ASSO) system is suggested as a solution that can increase users' perceived ease of use of the system while giving service providers the necessary authentication security for their applications.

There are some legal requirements for informed consent and privacy by default that concern authentication systems:

— **The Art. 4 (11) GDPR** [26] says that consent must be freely given, specific, and informed. In the domain of context-aware authentication, this means that the user must be aware of the contextual data being used and the intended purposes of processing the data. Im-

26. https://gdpr-text.com/read/article-4/

plicit and opt-out consent and particularly silence, pre-ticked boxes, or inactivity are presumed inadequate.

— The **Data Protection by Default Principle of Art. 25 GDPR** [27] says that the default option should select the most privacy-friendly method or disclose less personal information. In the domain of context-aware authentication, this means that only the minimal data needed for doing AA should be mandatory.

— **Privacy by Design Principles** [28] say that user interfaces need to be human-centered, user-centric, and user-friendly, so that informed privacy decisions may be reliably exercised. This also holds for authentication interfaces.

Several works study the compliance of authentication solutions with legal requirements for informed consent and Privacy by Default [60, 11].

Main Challenges. Ensuring that the sensitive user data used in AA systems is protected and kept confidential from unauthorized access is challenging. Another challenge is incorporating privacy by default and privacy by design principles to ensure that AA systems are designed to protect user privacy and data. To address these challenges, it is crucial that users understand how AA systems work and how their data is being used to authenticate them.

2.5 Summary

In this chapter, I analyzed the scientific and industrial context of AA. This analysis provides the basis for understanding the current body of knowledge and the challenges faced in the field of AA. I discussed the ongoing quest to replace passwords, and outlined trends and challenges. More work is needed to make AA more widely available, secure, and usable. From an industrial point of view, the expert survey results show that experts need more support and a common language to make full use of context information and to address risks during authentication. I also identified commercial

27. https://gdpr-info.eu/art-25-gdpr/
28. hhttps://carbidesecure.com/resources/the-seven-principles-of-privacy-by-design/

AA solutions. These solutions use Artificial Intelligence (AI) technologies to assess the risk or trust in a user based on contextual factors, in order to determine whether to allow, deny, or challenge a login attempt. The providers have different names for their solutions, but the approaches are all mainly based on the calculation of a risk score. The current state of commercial solutions in authentication is confusing, with concepts like MFA, RBA, and SSO being mixed up. Hence, there is a lack of standardization and systematization of knowledge in this field. I also discussed challenges and approaches related to the interdisciplinary research field of AA, which involves security and privacy, machine learning, identity management, and adaptive systems. The existing machine learning-based approaches tend to calculate risk scores as black boxes without considering different risk types or the appropriateness of authentication methods according to the context, which is the main challenge. Identity standards are constantly changing due to technology, laws, and security threats, which makes it challenging for authentication engineers to stay informed. Incorporating AA solutions in existing standards designed for static authentication is also challenging. Interoperability between different standards and systems requires common protocols and guidelines for AA. I suggest that mapping research in adaptive systems can help advance the field of AA and improve authentication system architectures. The protection and confidentiality of sensitive information and user data in AA systems is also a challenging task. It is important for users to understand how AA systems work and how their data is used for authentication purposes. I found that in many situations, it is of interest for authentication systems to adapt to context beyond the calculation of risk scores, and that this is also what experts find important. Hence, representing the context with appropriate and well-designed models is crucial. I found that context modeling for security applications *(e.g.,* AA) has not been deeply studied until now, and that in the literature and the industry the usage of context is very limited, with vague descriptions and grounds [8]. That makes it difficult to reuse or extend AA systems due the lack of practical solutions and standardization. Hence, there is a need for s systematization of knowledge. Efforts are needed to find out what

models are suitable for the field of context modeling for AA to enable the use of context for authentication systems. Hence, I present a structured review of the literature to date on context modeling for AA in the next chapter.

Name	Self-designation	Context	Approach
Prove	MFA	Behavioral, phone-related information	Trust score assignment to every authentication attempt
Duo	SSO	Geo-location, device, role	Detection of anomalies based on contextual factors
IBM Verify Access	SSO	Login patterns, session activities	Risk scoring engine to prevent anomalous logins
Kount Control	AI-Driven Solution	Login behavior, device, IP reputation, geolocation, mobile- and proxy indicators	AI-based anomaly detection
LastPass	MFA	Geolocation, IP reputation, biometric information	Risk score calculation based on context
Okta	MFA	Device, geolocation	Trust scores for device and geolocation
OneLogin	Access Management Solution	Geo-location, device, behavior	Risk score calculation based on context
Ping	Risk Management Solution	Device, operating system, browser version, date, time	AI-based use behavior analysis for anomaly detection
SecureAuth	AI-Driven Solution	Device, geolocation, IP reputation, behavior	AI-based risk score calculation

Table 2.3 – Overview of Industrial Solutions for Adaptive Authentication.

Chapter 3

Systematic Literature Review: On Understanding Context Modeling for Adaptive Authentication Systems

This chapter presents the first contribution of my thesis, a systematic literature review on context modeling for Adaptive Authentication systems (CM4AA). It is an extended version of the paper "On Understanding Context Modeling for Adaptive Authentication Systems" [23] published in the ACM Transactions on Autonomous and Adaptive Systems (TAAS) journal. Context modeling for security application (e.g., authentication systems) has not been deeply studied in the literature to date and we observe a limited usage of context information with vague descriptions and grounds in the practice. Hence, this contribution helps to understand how context information modeling for AA systems can be performed and is the basis on which the modeling framework presented in this thesis (CoFrA) is build. Figure 3.1 highlights this first contribution in the global vision of this thesis. First, I explain the review methodology. Second, I present findings on the current body of knowledge about context modeling for AA. Third, I present the findings on context information and its modeling for AA. Fourth, I present the findings on the desired properties of the context information model and its use for AA systems. Fifth, I present a Strengths-Weaknesses-Opportunities-Threats (SWOT) matrix for the domain of CM4AA. Last, I discuss threats to the validity of the study.

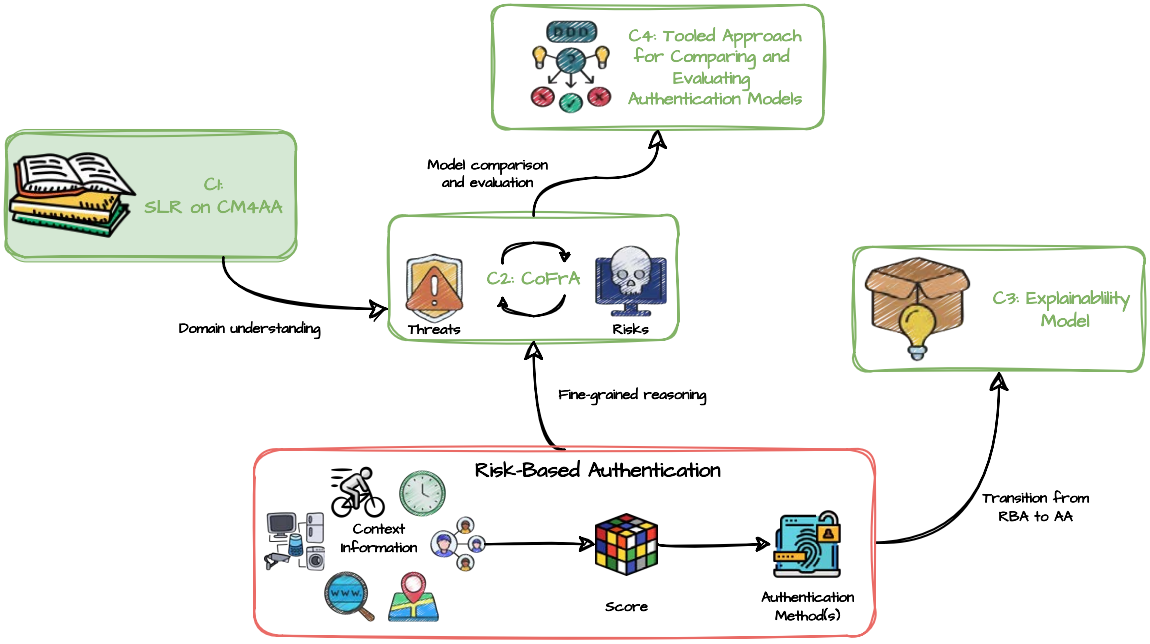

Figure 3.1 – Contribution 1: A Systematic Literature Review on Context Modeling for Adaptive Authentication.

Contents

DEVELOPING AA systems needs to be supported by adequate context information modeling techniques to reduce their complexity and improve maintainability [14]. I explained in the previous section, that context modeling for security applications (*e.g.,* authentication systems) has not been deeply studied in the literature to date and I observe a limited usage of context information with vague descriptions and grounds in the practice. I have seen in the analysis of the state-of-the-art and the state-of-the-practice that practitioners and researchers are mixing up concepts and technologies and that there is a need for a systematization of knowledge. Neither in the literature nor in practice, the research knowledge about Context Modeling for AA systems (CM4AA) has yet been materialized into concrete context models. Hence, I present in this chapter a structured review of the literature to date on CM4AA. To propose a modeling framework for AA, which

is the second contribution of this thesis, it is crucial to first enhance the domain understanding. Hence, the idea of this chapter is to explore the possibility of capturing a common set of contextual information for AA systems independent from the application domain, to show the lack of a unified framework and to analyze the shortcomings of the exclusive use of context information to calculate risk scores. I follow the procedures of the *Systematic Mapping Study* (SMS) and *Systematic Literature Review* (SLR) methodologies [97] to achieve **three complementary goals**. The former one (SMS) enables me to structure the research area and to get a comprehensive overview of the research topic of CM4AA (**goal 1**). The latter one (SLR) enables me to gather and synthesize evidence about context information, it is modeling for AA systems, and the use of the context information model (**goal 2**). The knowledge gained from goal 2 enables me to determine the desired properties of the context information model and its use for AA systems (**goal 3**).

This part of the thesis is related to Arias-Carbacos et al.'s survey on AA [8]. In their survey, the authors outline how to apply the design principles known in adaptive systems to AA systems but do not deeply study context modeling and how the context information model is used in the authentication system. Complementary to [8] and leveraging on their conclusions, in this study I focus on context modeling for AA systems and do not discuss self-adaptive systems design in general. In [8], the authors mention that most of the works surveyed in their article "show a limited usage of context, with vague descriptions and grounds". My analysis of state-of-the-art and state-of-the-practice comes to the same conclusion. Leveraging on this conclusion, I conduct efforts to find out what models are suitable for the field of context modeling for AA. This study is an important first step towards less vague descriptions and grounds for using context for authentication systems. Hence, my work is complementary with [8].

The rest of this chapter is structured as follows. I introduce the methodology in Section 3.1. In Section 3.2, I present the metrics and findings related to goal 1, in Section 3.3 those related to goal 2, and in Section 3.4 those related to goal 3. In Section 3.5, I assess strengths, weaknesses, op-

portunities, and threats of the research field of CM4AA. Threats to the validity of the study are discussed in Section 3.6. I summarize this chapter in Section 3.7.

3.1 Systematic Review Methodology

In this section, I present a systematic literature review approach based on the procedures of SLR and SMS [97] [1] (Figure 3.2). The three goals of this study manifest in the three following research questions:

— **RQ1:** What is the current body of knowledge about CM4AA?
The main activities to answer are:

1. to uncover which keywords and concepts reflect the research area of CM4AA to understand the nature of the research area and the notations in the domain,
2. and gaining an overview of the distribution of works in the research field of CM4AA regarding the year of the publication, the application domain, and the type of contribution to understand the structure of the research area, when, how and from which point of view the research is conducted,

— **RQ2:** Which context information determines the context of AA systems, how is it modeled, and for which phase of the authentication system life-cycle is the model used?
The main activities to answer are:

1. establishing a holistic overview of which context information determines the context of AA systems,
2. analyzing context modeling approaches for AA systems in the literature to date to understand the data structure according to which the context information model is built,
3. and analyzing the use of the context information in the authentication system life-cycle.

1. All supplementary material (figures, tables with raw search results) is available on my companion website: https://github.com/BumillerAnne/CoFrA-Studio/tree/main/Literature%20Review.

— **RQ3:** Which are the desired properties of the context information model and its use for AA systems?
The main activity to answer is:

1. to uncover the desired functional and non-functional properties of the context information model and its use for AA systems.

Figure 3.2 visualizes the relation between the three research questions and how I use the methodologies SMS and SLR to solve them.

Within RQ1, I aim to structure the research area of CM4AA to understand the current body of knowledge about CM4AA. According to [97], SMSs are used to structure a research area, while SLRs are focused on gathering and synthesizing evidence. Hence, for solving RQ1, I apply the procedure of a SMS, and for solving RQ2, that of a SLR. Findings about the current body of knowledge about CM4AA (RQ1) allow us to understand and interpret those related to RQ2. With the help of the findings related to RQ2, I can determine the desired properties of the context information model and its use for AA systems (RQ3).

In the following subsections, I describe the methodology to conduct the SMS and the SLR. I introduce the structure of the reusable search clause in Subsection 3.1.1 and explain the exclusion criteria applied to the raw search results in Subsection 3.1.2.

3.1.1 Logical Search Clause

I first analyzed the recent literature in top academic venues and exchanged with domain experts (people working on identity management, authentication, and system security. I used the snowball method to find literature by using the first references. Hence, I obtained a set of representative papers to derive key terms.

The search clause, consisting of a cartesian product of the terms presented in Table 3.1, is applied on GoogleScholar, ACM Digital Library, IEEE, Scopus, and SpringerLink. Essentially the search clause is a conjunction of the term “authentication system”, “context modelling” and a disjunction of terms expressing the adaptation capability of the authen-

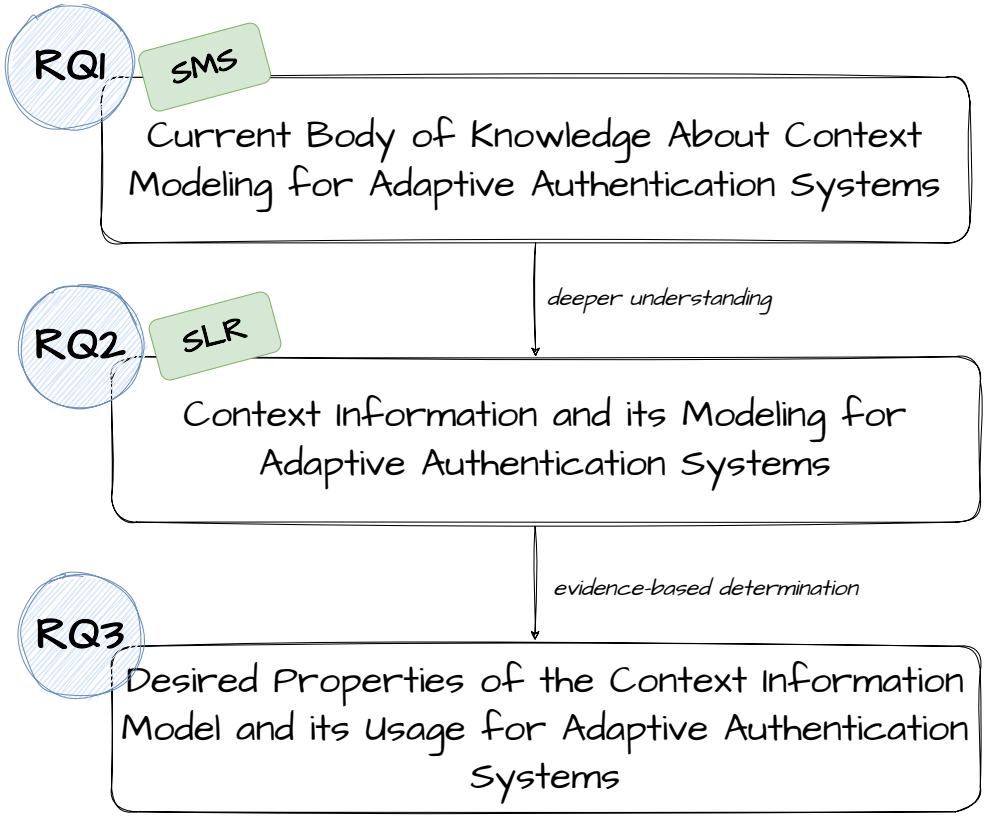

Figure 3.2 – Research Questions and Methodological Approach to Answer Them.

“authentication system”	“adaptation” “adaptive” “reinforced” “progressive” “risk-based" “risk based” “risk-aware” “context-based” “context based” “context-aware” “context aware”	“context modelling” “context modeling”

Table 3.1 – Representation of the Logical Search Clause.

tication system elicited after an initial scan of the literature published. For terms expressing the adaptation capability of authentication systems, I leveraged the terms used in [8]. Thanks to a snowballing approach, I assessed that "reinforced authentication" [48], "context-aware authentication" [51], "context-based authentication" [77], "progressive authentication" [102], "risk-based authentication" [129] and "risk-aware authentication" [55] are used in the literature appropriately to express the adaptation capability. Publications contributing to CM4AA need to use at least one of these terms. I included the spelling "context modeling" for "context modelling", the spelling "context-aware" for "context aware", the spelling "context-based" for "context based", the spelling "risk-aware" for "risk aware" and the spelling "risk-based" for "risk based". Authorization is the process of verifying what specific resources an entity has access to. Hence, I do not include works focusing on "context-aware authorization".

I restricted the scope to papers that contain "authentication system" because I only want to analyze modeling approaches where the context information is modeled for an authentication system and hence to use the information for authentication. After an initial literature scan, I observed that papers that do not contain the term "authentication system" but only the term "authentication" often discuss authentication as a security aspect of a context-aware application, but the context is not modeled for the purpose of authentication (*e.g.,* [2]). To find out in which form context is represented so that it is suitable for authentication systems, I want to exclude such papers.

I searched for parts of the query separately (full-text search) and joined the results manually to deal with the lack of support for complex clauses. I downloaded the citations in multiple parts and fused the results afterward.

Search Results.

To mitigate sampling and publication bias, I conduct searches on formal databases (*e.g.,* ACM Digital Library) and indexes (*e.g.,* GoogleScholar). The raw search results of the logical search clause contain 111 publications:

— **GoogleScholar:** 69
— **IEEE:** 9
— **SpringerLink:** 16
— **Scopus:** 15
— **ACM Digital Library:** 2

I deleted 31 duplicates in the first step. I classified the remaining 80 publications according to the exclusion criteria described in the following section. Figure 3.3 visualizes the publication selection procedure. The publications of the type review or study are helpful to gain background information on CM4AA and to analyze the year of publication and the contribution type, but the other analysis metrics have only been applied to contributions of the type concept, method, and tool (24 papers).

3.1.2 Exclusion Criteria

Based on common inclusion and exclusion criteria for systematic literature reviews proposed by the University of Melbourne [2], I determine the exclusion criteria for this work:

— The paper is not in English.
— The paper is not accessible electronically.
— The paper is a short paper ($\leq$ 4 pages) or a teaser.
— The paper is a patent. [3]
— The journal/conference/workshop is not international.

2. https://unimelb.libguides.com/sysrev/inclusion-exclusion-criteria
3. Patents are excluded from further analysis, but the high number of existing patents shows industrial interest in the topic and suitability of the research domain for the industry.

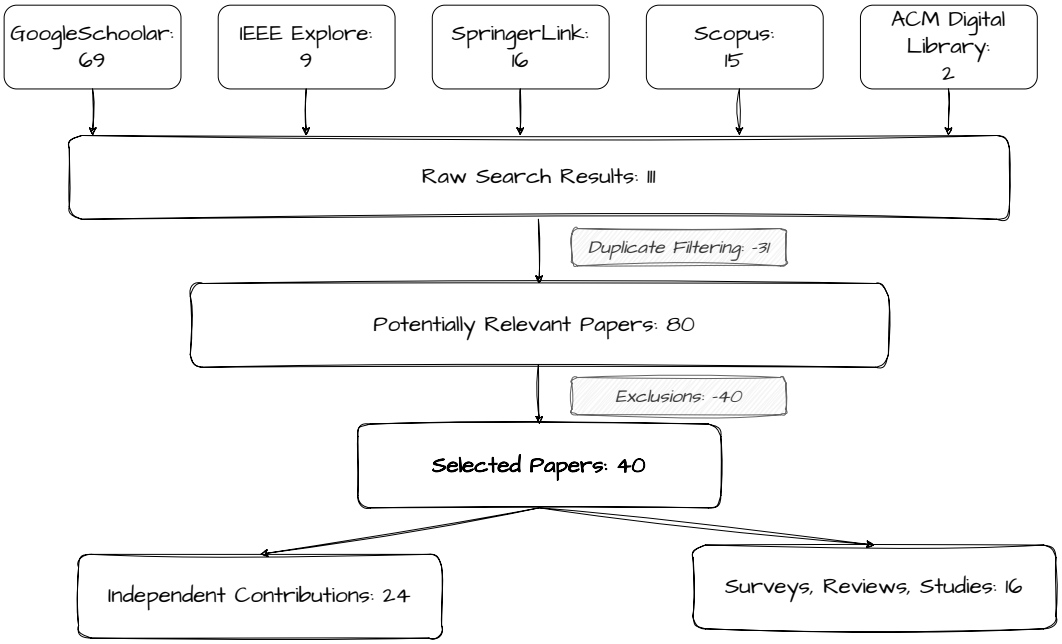

Figure 3.3 – Publication Selection Procedure.

Table 3.2 – Number of Publications per Year.

Year	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Relevant Publications	4	2	1	3	3	3	8	2	5	5	4

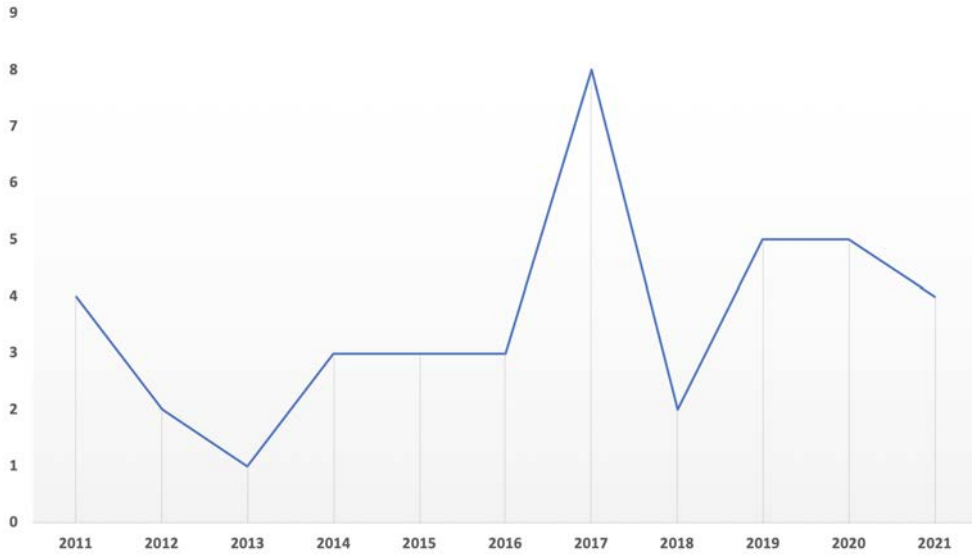

Figure 3.4 – Course of Publications Over the Last Ten Years.

Retaining papers per year.

After having deleted the duplicates and having applied the exclusion criteria, I kept **40** publications for further analysis. Table 3.2 shows the number of kept publications per year from 2011 up to now.

Figure 3.4 shows the course of publications over the last 10 years and shows a continuous interest in the research area of CM4AA with a peak in 2017. Some fluctuation in the number of publications across different years can be observed but interest in the topic always exists. The problem does not seem to be solved.

3.1.3 Analysis Process

For each research question (Section 3.1), I consider several metrics to analyze the publications. First, all six analysts worked together to determine which raw data is needed for each metric. Second, I divided the papers among ourselves (six subsets) and each analyst collected the necessary raw data from a subset of the reviewed papers (manual extraction

after reading). Third, this study analyzes the data according to the metric (*e.g.,* classification, frequency of occurrence). For this, each analyst has analyzed a subset of papers. For a set of 10 papers, all the six analysts conducted the analysis independently and discussed the results altogether. This discussion served to align the typical answer types and share a common understanding regarding the different criteria. For the other papers, at least two experts did the analysis and discussed the results. Three of the analysts are experts in the field of AA, the other three are experts in the modeling domain. In regular synchronization meetings, I discussed the analysis. I solved conflicts according to the majority principle if it was possible. If not, I asked another reviewer to read the paper and make a decision.

3.2 Current Body of Knowledge about Context Modeling for Adaptive Authentication

The first research question (RQ1) which I address within this literature review concerns the current body of knowledge about CM4AA. In particular, I aim to better understand the research field of CM4AA, such as which keywords and concepts reflect the research field, what is the distribution of works concerning the year of publication, the application domain, and the type of contribution to better appreciate the nature of the findings in the following research questions.

3.2.1 Metrics for the Publication Analysis

I apply the methodology of a SMS to structure the research area of CM4AA. I present in this section the metrics considered to analyze the relevant publications (Main Keywords, Contribution Types, Covered Application Domains).

3.2.1.1 Main Keywords.

I aim to uncover which keywords and concepts reflect the research area of CM4AA.

Raw data. I collect the titles, the abstracts, and the author-specified keywords (if exist) for the selected papers.

Metric. Based on the raw data collected from each article, I filter the common keywords [4] and calculate the frequency of appearance of each word based on Stem algorithm [100]. The 30 keywords that appear the most often in the abstracts, titles, and author-specified keywords of the publications are assumed to be the main keywords in the research field. The title and the abstract of a publication are usually the first introductions readers have to the work and therefore contain the main concepts. Additionally, authors specify keywords that mostly reflect their work. I think that 30 is a reasonable number because with a larger number, the words are repeated (synonyms), and with a smaller number, only the ones from the search clause are repeated. The keywords are visualized in a word cloud (Figure 3.5). As a visualization tool, I use TagCrowd [5], because of its ease to read, analyze and compare. [6]

3.2.1.2 Contribution Types.

I aim to uncover how research is conducted in the research area of CM4AA.

Raw data. I classify the publications along the type of research they conduct to understand how research is performed in the field of CM4AA. I classify the contributions based on [98] into concepts, methods, tools, studies, and reviews:

4. based on the following list https://tagcrowd.com/languages/English and according to my research goals

5. https://tagcrowd.com/

6. Additionally, I show the keywords in a table on my companion webpage.

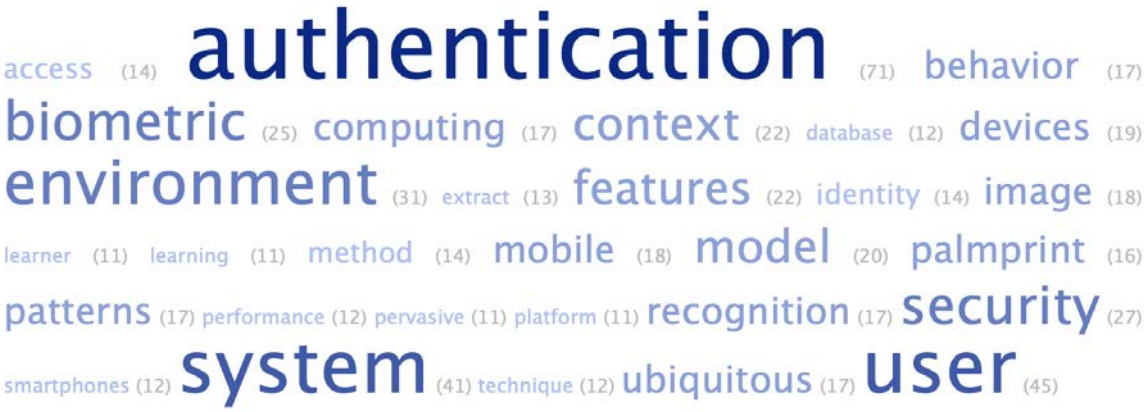

Figure 3.5 – Word Cloud Keywords - Titles, Abstracts, Author-Specified Keywords.

— **Concepts:** papers suggesting abstract ideas of how to model context for AA systems by observing and analyzing already present information.
— **Methods:** development of concrete ways of CM4AA.
— **Tools:** papers presenting novel systems, prototypes, or software tools.
— **Reviews:** papers reviewing related literature.
— **Studies:** papers analyzing and evaluating existing tools, methods, or concepts.

One of the contribution types, concept, method, tool, review, or study, is assigned to each of the reviewed publications. I did the assignment in a disjunctive manner: papers, suitable for more than one research type were discussed and assigned the most suitable contribution type. Here I consider the most suitable type to be the one at the focus of the contribution.

Metric. Figure 3.6 is a pie chart that visualizes the proportions of the contribution types.

3.2.1.3 Covered Application Domains.

With the analysis of the application domains, which are covered in the field of CM4AA, I aim to uncover application domains in which CM4AA plays a crucial role.

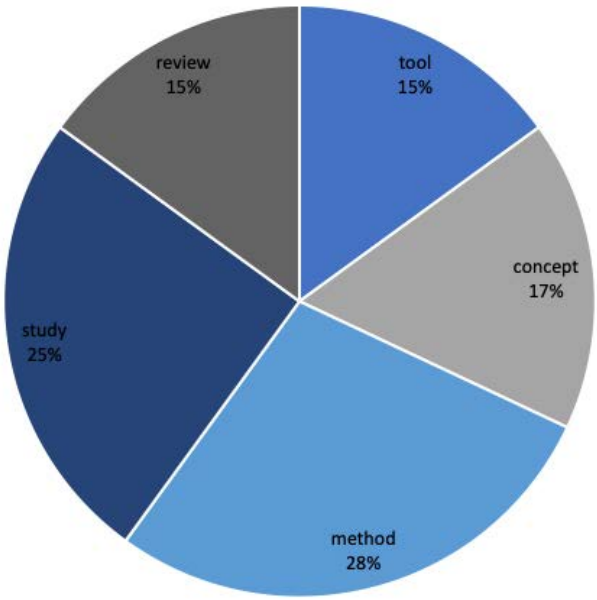

Figure 3.6 – Partition of the Contribution Types of the Publications Relevant to this Study.

Raw data. The application domain of a publication is the segment of reality (*e.g.,* telecommunication, healthcare, education) that is addressed within the publication. For each of the reviewed papers, I classify it according to its primary application domain if there is one or I indicate that the approach is generic.

Metric. After classifying the papers along the **years of publication** (Figure 3.4), the **keywords** (Figure 3.5) and the **contribution types** (Figure 3.6), they are classified along the **application domain**, to enable the identification and discussion of domain-specific trends. An application domain is assumed to be covered if at least one contribution addresses the domain. 92% of the analyzed publications are not specific to any application domain and can be applied to CM4AA in any domain. I identified two papers specifically relevant to the domain of education [74, 50].

3.2.2 Findings on the Current Body of Knowledge about Context Modeling for Adaptive Authentication

I present in this section the findings on the current body of knowledge about context modeling for AA.

3.2.2.1 Main Keywords.

That the words *authentication* (71), *system* (41), *context* (22), and *model* (20) occur frequently is not surprising regarding the search clause, but confirms the significance of the search terms. That *authentication* appears more than twice as often as *model* can be interpreted as a clue that the research field of CM4AA is mainly authentication driven. The modeling community seems to have fewer contributions. This can also be seen as a reason for the lack of standardized context modeling methods for AA systems. As I have explained, I focus on papers based on context modeling and explicitly exclude papers that deal only with authentication, and yet these seem to be driven by the authentication community.

Our search clause contains a disjunction of words expressing the adaptation capability of authentication systems. None of them is among the 30 most frequent words in the abstracts, titles, and author-specified keywords of the papers. In a generic MAPE-K architecture for adaptive systems, there is one concern about gathering and representing managed resources and another concern about the actual adaptation logic. In an AA system, the first concern refers to the capability to take into account the context information (context-awareness), while the adaptation logic refers to the capability of a system to change its behavior in response to the context. In this study, I target papers that focus on context-awareness and I observe that such works deal little or not at all with the actual adaptation logic.

The keywords *biometrics* (25) (*palmprint* (16)), *behavior* (17) and *patterns* (17) show the trend of using these *features* (20) for AA [80, 79]. *Databases* (12) from which the information can be *extracted* (13) seem to be important. The state of environmental elements (*environment* (31)) plays a role in AA. Authentication is the ability to prove that an entity

is genuinely who this entity claims to be (see Section 2.1) and is not necessarily a question of proving a unique identity. When contextual features are used that confirm a unique identity then often the term *recognition* (17) is used. It seems to be common to use contextual features that determine a unique *identity* (14). This justifies also the frequent appearance of the word *image* (18). In approaches working with images, those are often used to recognize biometrics (*e.g.,* palmprint, iris). In the works, the *performance* (12) of the approaches is often evaluated. *Platforms* (11) seem to be a relevant authentication target. The word *user* (45) indicates that the entity being authenticated is often the user. The frequent appearance of the word *security* (27) can be justified by the fact that authentication is an essential security aspect of systems [66]. *Smartphones* (12) and *ubiquitous* (17) *computing* (17) environments are important concepts in the research field of CM4AA. Context information acquirement with *mobile* (18) *devices* (19) is often easier than with non-mobile devices. Overall, biometric and behavioral information can be acquired more easily from mobile than from non-mobile devices. Anyway, non-mobile devices do not need to be neglected. The keyword *learning* (11) can be interpreted as a clue that the works often propose machine learning algorithms for AA. The keyword *learner* (11) points out that education is a relevant application domain in the research area of CM4AA. *Access* (14) control is frequently used semantically similar to authentication. The terms authentication and access control are not always clearly separated from each other. I observe that terms that are clearly defined in the security domain (see Chapter Section 2.1) are not always used properly in the domain of CM4AA.

3.2.2.2 Contribution Types.

There is a large number of studies and reviews (40%). Gaining an understanding of the existing research relevant to CM4AA seems to be in the interest of many researchers. The works fall in the categories of context and context-awareness, authentication modalities, AA in specific computing environments, and AA in general. There is no review of works on context modeling for AA systems. 15% of the contributions are of the con-

tribution type tool. AA is a new research area and not yet every proposed concept of how to model context information for AA systems goes beyond conceptualization and results in a tool. There are contributions of the type method (28%) and concept (17%). These works do not (yet) result in tools. CM4AA seems to be a conceptual and methodological research field. This research type, generally related to abstract ideas or schemes is a potentially powerful way to introduce new ideas, identify problems and appropriate solutions in new ways, and provide new frameworks. Difficulties related to methods and concepts are the conflicts that may arise within the different approaches and their unsuitability for real-world applications. Due to privacy and confidentiality issues, there is a lack of public authentication data, that would allow pushing further the development of tools. For AA system designers, it is challenging to use context information efficiently without the support of tools.

3.2.2.3 Covered Application Domains.

Most of the publications are not specific to any application domain (92%). This sheds light on the fact that CM4AA is a cross-domain research topic. The danger is that terms are confused or concepts are understood differently. The right balance between desired properties of authentication mechanisms which is crucial in the context of AA needs to be adjusted according to the domain. Based on the publications identified to be specific to an application domain, CM4AA seems to be particularly relevant in the domain of education. For online learning platforms, it is crucial to adapt content to the entities' roles and needs. For example, students need, unlike teachers, not to have access to exam results. Anyway, it is possible that researchers who study CM4AA are teachers and therefore use the education application domain. However, this does not necessarily mean that education is a field of application in which CM4AA is particularly important.

Lessons Learned. I observe a **continuous interest** in the research field of CM4AA over the last ten years. Works related to CM4AA focus on **context-awareness** and the actual **adaptation** capability of authentication systems is often disregarded. The research field is mainly driven by the **authentication** community. There is a trend of using **biometric** and **behavioral** contextual features that can be used to identify a unique entity. It seems to be disregarded that authentication is not necessarily about proving a **unique identity**. In the research area of CM4AA, terms are not always clearly **delimited** from each other (*e.g.,* access control and authentication), what sheds light on the **lack of a standard** for CM4AA. **Mobile computing environments** and authentication on **mobile devices** are crucial in the research area of CM4AA. CM4AA is a **cross-cutting concern in multiple domains**, that integrates information from multiple disciplines or bodies of specialized knowledge. There are **concepts** and **methods** proposed in the literature that do not go beyond conceptualization and do hence not result in concrete **tools**. Due to **privacy** issues, there is a lack of publicly available data to push further the development of tools and benchmark solutions. By providing tools and methodologies to model and implement AA, I aim to bridge the gap between context-awareness and effective adaptation with this thesis. I also contribute to bringing insights from the modeling community to a community that is mainly driven from the authentication point of view. I also aim to establish a common language and a standard foundation for CM4AA. I also provide a flexible modeling framework that accommodates various computing environments, including mobile, and traditional desktop contexts.

3.3 Context Information and its Modeling for Adaptive Authentication Systems

The second research question (RQ2) which is addressed within this review concerns context information and its modeling for AA systems.

3.3.1 Metrics for the Publication Analysis

I gather and synthesize evidence about context information, its modeling for AA systems, and the use of the model in the authentication system life-cycle within the methodology of a SLR and with the help of several analysis metrics (Context Information, Modeling Formalisms, Authentication System Life-cycle Stage).

3.3.1.1 Context Information.

With the analysis of the context information that determines the context for AA systems, I aim to uncover the context information which is most commonly used. I assume the context information to show up in a triplet *[Informing Entity, Contextual Feature, Assigned Entity]*, which allows me to analyze the entities and their situations in an AA system in a detailed manner to be able to refer to the definition of context information from Dey et al. [41] (*"Context is any information that can be used to characterize the situation of an entity"*). For example, the contextual feature location can originate from a smartphone and be attributed to a user: *[smartphone, location, user]*.

— **Informing Entities (IE).** Informing entities, such as devices or users, are entities that inform about the context. For example, a mobile device can inform about the contextual feature location.

— **Contextual Features (CF).** A contextual feature is a feature which is characterizing the context of an entity (*e.g.,* its location, its behavior). I consider contextual features coming up at two different **levels of transformation**. At the low transformation level (*e.g.,* raw sensor information like the location), and at the high transformation level (*e.g.,* information transformed from sensor information like an entity's behavior).

— **Assigned Entities (AE).** Entities whose context is determined with the contextual features are entities the context is assigned to (*e.g.,* user, device).

Raw data. For each of the reviewed papers, I collect the information regarding the concepts of *IE*, *CF*, *AE* that appear within the publications. This information is directly extracted from the papers. I do not establish an a priori list of elements that can appear in this list. If an article does not discuss an element of this triplet, it is not classified in the corresponding category.

Metric. The metric for the three categories is a partition for each category of the frequency of occurrence of the collected items.

— Figure 3.7 shows the partition of the most frequently **informing entities**. The device as IE means that the information is taken from the device (*e.g.,* integrated sensors). In some cases, the information is directly taken from the environment (*e.g.,* with the help of a thermometer, or light sensor). The system is assumed to be the IE when the system provides information directly (*e.g.,* diagnostic and troubleshooting information related to the operating system, hardware, and software). Especially in the context of signal processes, images are used as input data to extract information. In some work, the user is assumed to inform about the context.

— Table 3.3 shows the percentage occurrence of the most frequently used **contextual features**. Behavior describes how an entity acts or conducts oneself (*e.g.,* typing behavior), biometric describes biological measurements or physical characteristics (*e.g.,* fingerprint), activity describes the way in which an entity conducts towards the system (*e.g.,* requested resources), device information describes the piece of equipment which is used by the entity (*e.g.,* name of a mobile phone), environmental factors describe factors external to a person (*e.g.,* luminosity, background noise), location describes a particular place or position (*e.g.,* France), personal user information is any information related to an identifiable user (*e.g.,* address, phone number), roles describe an entities privileges (*e.g.,* administrator) and time the measured or measurable period during which the authentication attempt happens (*e.g.,* October, 10th 2021 at 09:09:09). I also calculate

Feature Name	Percentage of Occurance
Biometric	42%
Behaviour	38%
Location	33%
Environmental Factors	21%
Activity	13%
Device information	13%
Roles	8%
Personal Identifiable Information	8%
Time	4%

Table 3.3 – Percentage Occurrence of the Most Frequently Used Contextual Features.

the percentage of papers which consider contextual information on a transformed level (*e.g.,* the behavior) and not only on the raw sensor level (*e.g.,* the temperature).

— In 92% the user is the **assigned entity**. In the remaining works, the context information is assigned to the device or the system.

3.3.1.2 Modeling Formalisms.

This study analyzes the **modeling formalisms** for modeling the context for AA systems proposed in the publications relevant to this study. I aim to uncover how context information modeling for AA systems is performed to analyze how context models that are suitable for the field are defined and evaluated.

The modeling formalism consists of two parts:

1. **Modeling Concepts:** The abstraction of the ideas and the definition of their precise meaning and relationships
2. **Modeling Technique:** The technical approach (technological stack) according to which the model is built (*e.g.,* a standard modeling language) defining the textual or graphical syntax of the model

Raw data. For each of the reviewed articles selected, this tudy analyzes whether the introduced **modeling concepts** are generic, specific to an

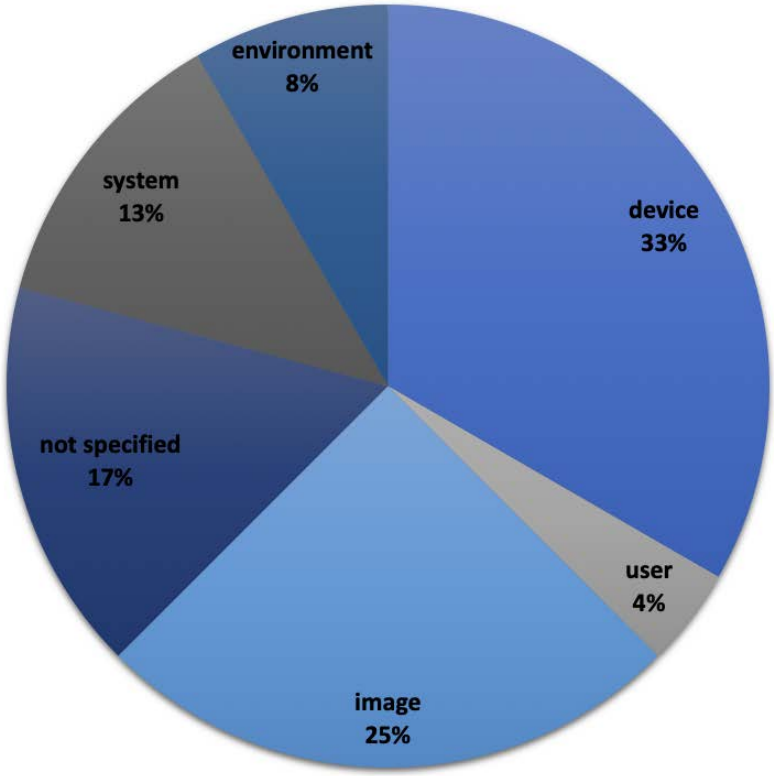

Figure 3.7 – Partition of the Most Frequently Used Informing Entities.

application domain, or authentication specific:

— **Generic Concepts.** The concepts are generic if they are kept abstract and general, without ideas related to the authentication problem or a specific application domain (*e.g.,* contextual feature).

— **Authentication-specific Concepts.** The concepts are authentication-specific if they are related to the authentication problem (*e.g.,* authentication attack).

— **Domain-specific Concepts.** The concepts are domain-specific if they are related to a specific application domain (*e.g.,* learner for the education domain).

I identify the following four objectives based on which the **modeling technique** is chosen:

1. Formalize mathematically complex relationships
2. Capture authentication security rules and threats

3. Visualize the organization and relationships among different functionalities of the system
4. Represent processes in the authentication system

For each of the papers selected, this study analyzes the **modeling concepts** and the **modeling techniques**, I classify the **modeling concepts** into generic, authentication-specific, and domain-specific concepts and the **modeling techniques** according to the underlying objective.

Metric. Figure 3.8 shows the proportion of domain-specific (8%), authentication-specific (17%), and generic (75%) concepts that are proposed in the publications relevant to this study. The assignment is done in a disjunctive manner [7] depending on the starting point the authors propose for the modeling concepts: general concepts, domain-specific concepts, or authentication-specific concepts.

Figure 3.9 shows the proportion of the underlying objectives of the used modeling techniques (Formalize mathematically complex relationships: 54%, Visualize the organization and relationships among different functionalities of the system: 21%, Represent processes in the authentication system: 17%, Capture authentication security rules and threats: 8%).

3.3.1.3 Authentication System Life-cycle Stage.

With an analysis of the distribution of the publications concerning the **authentication system life-cycle stage the context model is used for**, I aim to uncover lacks in existing context modeling approaches for AA systems.

Raw data. The context model defines how context data are structured and maintained to produce a description of the context information that

7. Papers that contain concepts from more than one category are assigned to the category that predominates.

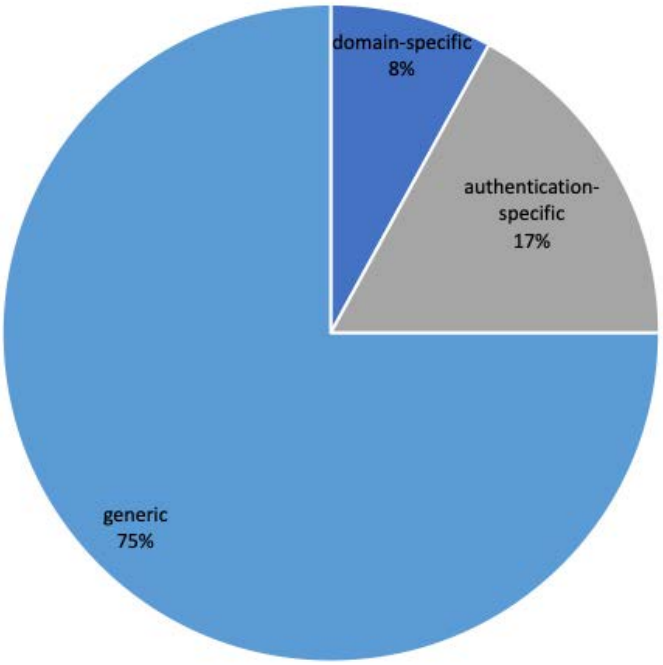

Figure 3.8 – Partition of Generic, Authentication-Specific, and Domain-Specific Modeling Concepts.

is present in the context-aware authentication system. There are three life-cycle stages of the authentication system: design (1), which is the phase of making design decisions regarding the architecture and structure based on gathered requirements and criteria, deployment (2), which is the phase of deploying the system in a production environment (configuring infrastructure, defining deployment strategy) and runtime (3), which is a representation of the authentication system that can be manipulated at runtime (the context information can be used at runtime) [12]. To structure and maintain the context information over the whole life-cycle of the authentication systems, concerns belonging to each stage should be considered in the model. I check for each context model identified in the literature for which stages it is intended and I classify the models to belong to one or more system life-cycle stages.

Metric. Figure 3.10 represents the proportions of publications relevant to this study that address the design-, deployment- and runtime stages.

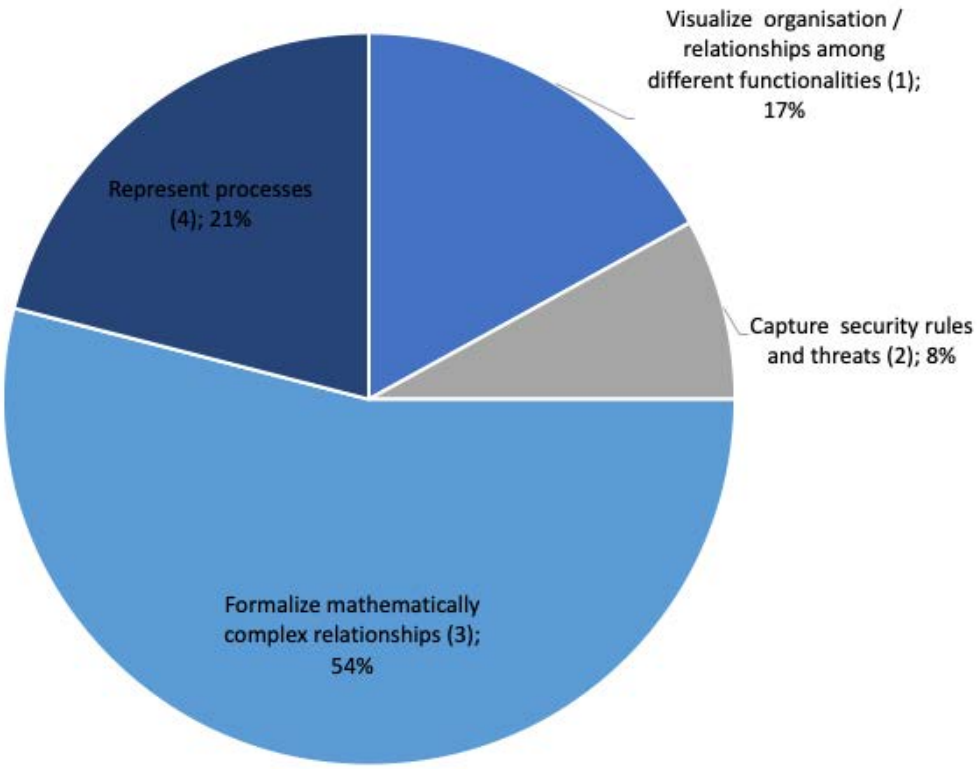

Figure 3.9 – Proportion of Underlying Objectives of the Proposed Modeling Techniques.

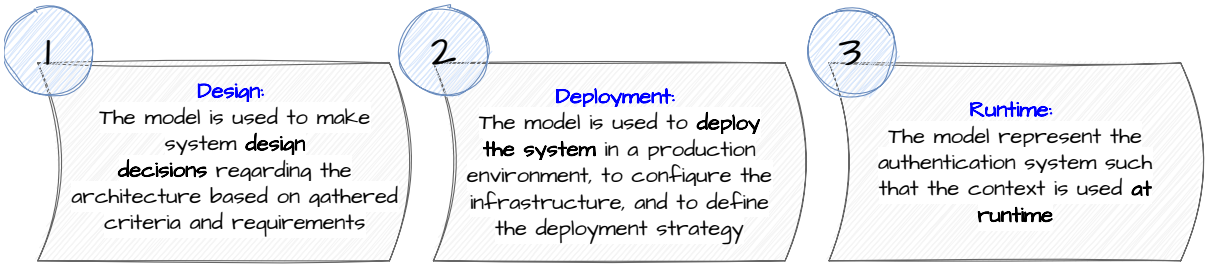

Figure 3.10 – Authentication System Life-Cycle Stages That the Context Model is Used For.

3.3.2 Findings Related to Context Information and its Modeling for Adaptive Authentication Systems

In this subsection, I answer RQ2, I discuss which context information determines the context for AA systems, how it is modeled, and how the model is used for AA systems. The findings related to RQ1 show that CM4AA is a cross-cutting concern in multiple domains. Hence, I do not analyze domain-specific trends in this section, and I take into account issues related to interdisciplinarity. According to the findings related to RQ1, biometric and behavioral information is commonly used for AA in mobile computing environments. Hence, in this section, I treat issues related to these contextual features and mobile computing environments.

3.3.2.1 Context Information.

Conforming to the context information triplet, this study analyzes the informing entities, the contextual features, and the assigned entities in the following.

Informing Entities. This study analyzes which entities are informing about context information, and I discuss the data types and formats of the given context information. In 40% of the works, authors propose the use of context information which is acquired from sensors of mobile devices [82]. Mobile devices are crucial for data acquisition in the research area of CM4AA.

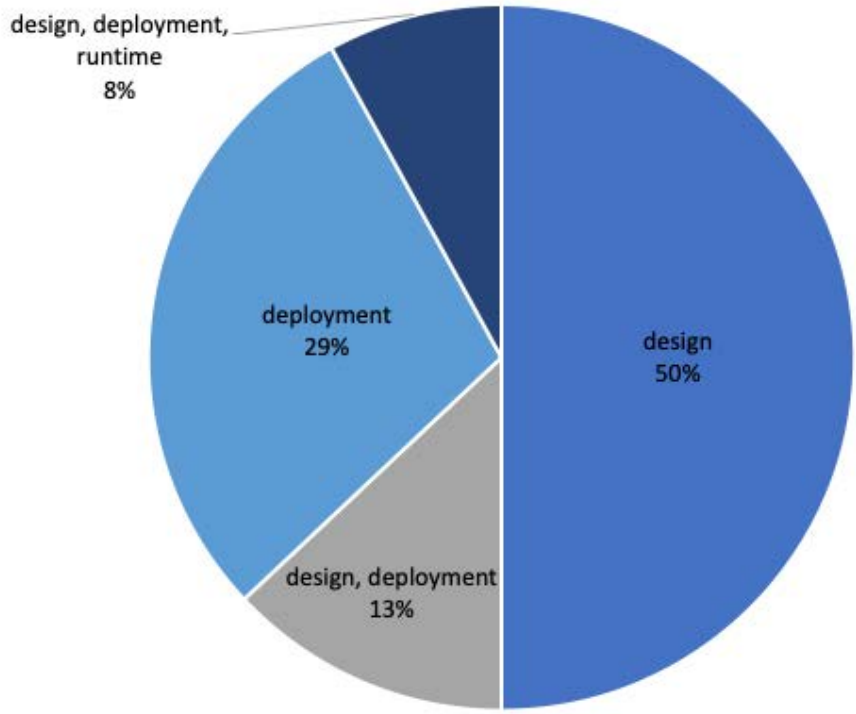

Figure 3.11 – Partition of the Context Models Used for the Design, Deployment, and Runtime Life-Cycle Stage of the Authentication System.

The constant use of mobile devices has become a normality in our society. Hence, following this trend, authentication is increasingly discussed for mobile devices. This shift is also related to data acquisition: mobile devices are increasingly equipped with sensors, which makes the use of context information for authentication possible. This is an advantage, but it also brings new challenges to light, including the use of multiple devices in smart home and mobile computing environments. Despite the increased dominance of mobile devices, non-mobile devices must not be disdained either. Accelerometer, *Global Positioning System* (GPS), and touchscreen sensors are frequently used. Witte et al. [133] propose to automatically acquire the geolocation with the GPS sensor of a mobile device.

Images (30%) are crucial as well to inform about the context (*e.g.,* for the comparison of palm print images [64]). In 9% of the works, the environment is informing about the context (*e.g.,* [68].

Depending on how the context information is used in the proposals,

the data is represented in several data formats. Server logs [79] and time series [91] are popular formats, especially in works that are reasoning patterns and trends from the context information. In several works, the authors specify the data storage and discuss related issues. Often the data is stored in databases [68], in central repositories [96] or local repositories [108].

Contextual Features. Table 3.3 shows that the biometric (42%) and behaviour (38%) are the most frequently used contextual features. In some works, the location is modeled for AA systems (33%). Environmental factors, like nearby people or devices, the luminosity, or the noise, are often referred to as well when the context for AA systems is modeled (21%). In their AA system design methodology, Arias-Cabarcos et al. [7] propose taking into account geolocation as a contextual feature. In the work from Ramakrishnan et al. [101] activities are modeled to detect anomalies. Neverova et al. [91] propose a method for active biometric authentication based on motion patterns.

61% of the contributions do not only rely on raw sensor data information (*e.g.,* location, temperature) but consider context information on a transformed level like the user's activities or behavior.

Assigned Entities. In 92% of the reviewed works the **user** is the entity the context is assigned to (*e.g.,* [96, 105]). Ma et al. [74] assign the context information to **resources**. In other reviewed papers [65], the context information is assigned to the device. In the paper specific to the domain of education [50] the context information is assigned to the learner (domain-specific user).

3.3.2.2 Modeling Formalisms.

This study analyzes the modeling concepts and the modeling techniques to understand how the context information is built for an AA system.

Modeling Concepts. Most of the reviewed papers are not specific to any application domain and hence only 8% of the papers introduce domain-specific modeling concepts. In two papers education domain-specific modeling concepts are introduced [50, 74]. The fact that those papers that belong to a specific application domain (education) introduce domain-specific concepts shows that formalizing the authentication system structure, behavior, and requirements within particular domains is important.

The largest part of the identified modeling concepts are generic (75%). In this way, concepts are related to abstract types but do not require specific descriptions or relationships related to an application domain or the authentication problem. The fact that mainly generic concepts are introduced demonstrates the ability to capture a common set of concepts and relationships for CM4AA. It is interesting to note that despite this possibility, no general standard for CM4AA exists.

There are also some authentication-specific modeling concepts (17%), which show that CM4AA is driven by the authentication community.

Modeling Technique. I cannot identify a trend in the use of a particular syntax for CM4AA. Different structures to represent complex concepts and relationships visually or textually are presented in the reviewed works.

Nevertheless, four main objectives emerge: visualize the organization and relationships among different functionalities of the authentication system (1), capture authentication security rules and threats (2), formalize mathematically complex relationships (3), and represent processes in the authentication system (4).

- (1) Visualize the organization and relationships among different functionalities of the authentication system
  - **Component-based Modeling,** which focuses on the decomposition of the model into individual components. It provides a higher level of abstraction and divides the problem into sub-problems (*e.g.,* context gathering and context analysis) [133, 71, 89, 50].
  - **Blockchain Modeling,** which is a modeling approach based on an interlinked systematic chain of blocks that contains the his-

tory of data (*e.g., to take into account the history of contextual information*) [74].

- (2) Capture authentication security rules and threats
  - **Attack-Tree Modeling**, which deals with how vulnerabilities are exploited (*e.g.,* distinguishing between different attack types) [82].
  - **Rule-based Modeling,** which is a modeling approach that uses a set of rules that indirectly specifies a model (*e.g.,* security rules) [114].
- (3) Formalize mathematically complex relationships
  - **Mathematical Modeling,** which is a description of a system using mathematical concepts and languages (*e.g.,* the representation of context information in a vector) [68, 26, 106, 117, 61, 79, 91, 7, 101, 88, 90, 99].
  - **Biological Modeling,** which is a modeling approach inspired by biological phenomena (*e.g.,* modeling context information as a Chromosome where each individual context is a gene) [108].
- (4) Represent processes in the authentication system
  - **Flowchart Modeling,** which is a type of diagram that represents a workflow or process (*e.g., to model the reasoning about context information for AA within a flow of steps*) [96, 65, 105, 64].

I see in Figure 3.9 that many works (54%) focus on formalizing mathematically complex relationships. The authors aim to exactly represent the real problem situations. I have already noted that approaches are often presented that identify a single entity. This requires precise calculations and comparisons. (*e.g.,* for the comparison of palm print images [64]). For this purpose, a mathematical modeling syntax is well-suited.

In 21% of the works, different functionalities of the authentication system are separated and represented in different model components. The models describe the components used to make the desired functionalities of the authentication system. Component diagrams can also be used to construct executables by using forward and reverse engineering.

In 17% of the reviewed works, system processes are described in the proposed model. A flowchart is an important tool for planning and designing a new system, it provides an overview of the system and also demonstrates

the relationship between various steps.

In 8% of the proposed modeling approaches the main objective is to capture security rules and threats. As authentication is an important security aspect of the system it is important to take into account such threats and rules.

3.3.2.3 Authentication System Life-cycle Stage.

Within an analysis of the contributions regarding the life-cycle stage of the authentication system that the context model is used for, I aim to detect trends and gaps in the literature.

More than half of the publications (63%) focus on the **design** of the system. In these works, the context model serves as a representation that can aid in defining and analyzing a set of concepts of the AA system. In [50] for example, the model serves as a representation of the concepts of learning system architecture. The concepts (*e.g.,* "service credential request") are used to analyze the authentication procedure. An overview of different functional components of the system is represented in the model in [101]. In 13% the design stage is addressed together with the deployment stage.

In 29% the **deployment**-stage is addressed. In those works, the model is implemented but not used at runtime. In [68], the model representing the system architecture has additional modules that allow the system implementation.

In 8% of the works design, deployment, and **runtime** issues are addressed. In these works, the authors explicitly address the system execution. A common purpose for models at runtime is self-adaptation [12]. This is the case also for the works I identified that treat CM4AA at runtime. The fact that only a few papers deal with adaptation shows again that this aspect is not a major issue in the papers that deal with context modeling.

I mentioned earlier that existing run-time solutions are mainly based on the calculation of a one-dimensional risk score. Using the context information model at runtime for AA systems in a more extensive manner is rarely studied.

Lessons Learned. Most of the works are based on context information acquired from **mobile devices**. Those are therefore crucial for data acquisition in the research area of CM4AA. **Non-mobile devices** are usually disregarded. The commonly used **context information** (biometrics, behavior, location) is highly **privacy** sensitive information. This makes it difficult to ensure the user's willingness to disclose private context information even if it is used for authentication. It is common to determine **patterns** and habits from the authentication history of users. This can be an advantage regarding the **storage** of the context information. In some cases, only the habits, like the usual location, need to be stored and not the whole history of authentication attempts. Regarding the **privacy** this can be an advantage as well. Other **anomalies** than derivations from patterns and habits are often disregarded. In works that focus on human identity authentication, the context is usually assigned to the entity which needs to be authenticated. That there are only a few works also considering contextual features assigned to other entities sheds light on the fact that the **contextual relations** between different entities often are omitted when context information for AA systems is modeled. The largest part of the identified modeling concepts are generic (75%). In this study, we cannot observe a trend in the use of a **modeling technique** to model context information for AA systems despite the clear identification of the underlying goals. There is a great diversity of syntax proposed in the literature, which sheds light on the lack of a modeling **standard** for CM4AA systems. This is also related to the fact that the research area of CM4AA is mainly authentication driven and the influence of the modeling community is limited. The lack of standards makes it difficult for authentication engineers to model context information efficiently and structure. Also, standards would help to clarify **reglementations** regarding privacy issues, and users would be more willing to share context information if it is modeled according to an accepted standard and used for AA in a regulated manner.

The NIST proposes **guidelines** for authentication and the management of digital identities, which need to be used also to establish appropriate modeling standards. The context information models are mostly used at the **design time** (63%) and **deployment time** (42%) of AA systems. There is a lack of works treating CM4AA systems at runtime (8%).The lack of works treating CM4AA at **runtime** is due to the lack of concrete implementations and data available. AA is still a **young research area** and is not yet much applied at runtime.

3.4 Desired Properties of the Context Information Model and its Use for Adaptive Authentication Systems

The third research question (RQ3) which is addressed within this literature review concerns desired properties of the context information model and its use for AA systems.

3.4.1 Metrics for the Publication Analysis

I do not identify a standard from which I can derive desired properties on the context information model and its use for AA systems. Nevertheless, the authors of the reviewed papers identify constraints on how context information modeling is done successfully for AA systems. I observe that various properties have been identified as important for the context model to be suitable for AA systems. Some of these constraints are also evaluated empirically in the reviewed works. To understand which properties the authors consider important, I perform an analysis of these constraints.

Raw Data. From each paper, I extract the constraints on the context information model and its use for AA systems put forward.

Metric. This study analyzes the properties and identify some that are commonly put forward.

The metric extracts the properties put forward in the reviewed publications and the frequency of papers putting them forward. I also analyze which of the properties are used as empirical evaluation metrics.

3.4.2 Findings on Desired Properties of the Context Information Model and its Use for Adaptive Authentication Systems

I extracted ten desired properties of the context model. Seven properties relate to the ability of the context model to handle specific characteristics of context information (1). The other three properties relate to the ability to be integrated with an AA system (2).

1. Properties related to **the ability of the context model to handle specific characteristics of context information**
   — **Dynamicity:** The context model can take into account changes in the context information along the authentication process.
   — **Quality:** The context model can evaluate the exactitude of the context information.
   — **Temporality:** The context model can take into account temporal information which may impact the interpretation of the context.
   — **Complexity:** The context model can consider the context as a mesh consisting of many different and connected information.
   — **Heterogeneity:** The context model can take into account that the context consists of dissimilar or diverse information.
   — **Abstraction:** The context model can reduce the amount of complexity of the context information.
   — **Privacy:** The privacy requirements associated with the context information are taken into account in the model.
2. Properties related to **the ability of the context model to be integrated with an AA system**
   — **System relevance:** The context model can provide machine interpretability and sufficient support for the authentication system's development process.

— **Accuracy:** The context model can reason on the context information in an accurate manner.
— **Response time:** The context model can reduce the total amount of time it takes to respond to an authentication request.

Table 3.4 shows an overview of which authors of the publications relevant to this study put forward which desired properties. A bullet means that the authors put forward the property in the discussion of their approach. Two bullets mean that the authors use the property as an empirical evaluation metric.

Dynamicity (58%). In some works the dynamicity of the users' behavior is taken into account in the context model [114, 50, 105, 133, 91, 79]. Other authors model context in highly dynamic environments [7, 88, 108, 68]. Kumar et al. [65] study phone movement patterns under static and dynamic conditions. Ramakrishan et al. [101] assume security politic to be dynamic. The authentication of mobile dynamic identities is addressed in [90] and [89].

Quality (38%). Some authors analyze the quality of contextual information [71, 64, 88, 117, 26, 61]. The quality of classification algorithms for the classification of context information is discussed in some works [65, 91]. Lima et al. [68] analyze the quality of sensors to acquire context information.

Temporality (71%). Some authors analyze the temporal dimension of contextual features (*e.g.,* the hour of the connection) [71, 114, 105, 61, 7, 90, 89, 101, 96]. To take into account the *temporal* dimension, Gunjal et al. [50] propose checking the users' credentials on a *periodic* basis. In some works, the challenge of providing anytime authentication services, e.g. in ubiquitous systems [108] or the *Internet of Things* (IoT) [88], is discussed. In [68], the used space-time permutation model allows us to take into account the temporal dimension of contextual features. The contextual features are analyzed in different time windows in [65] and [133]. The use of *time* series

	Dynamicity	Quality	Temporality	Complexity	Heterogeneity	Abstraction	Privacy	System Relevance	Accuracy	Response Time
Al-Muhtadi et al. (2011) [89]	•		•	•	•		•	•		
Liu et al. (2021) [71]		•	•						• •	
Kumar et al. (2021) [64]		•		•					• •	
Solano et al. (2020) [114]	•		•	•	•		•		• •	
Pititheeraphab et al. (2020) [99]				•				•	• •	
Gunjal et al. (2020) [50]	•		•				•			
Miraoui et al. (2019) [82]						•			•	
Ma et al. (2018) [74]								•	• •	• •
Mozzaquatro et al. (2017) [88]	•	•	•		•	•				
Arias-Cabarcos et al. (2017) [7]	•		•	•	•		•			
El-Tarhouni et al. (2017) [117]		•		•		•	•		• •	
Kumar et al. (2017) [65]	•	•	•						• •	•
Neverova et al. (2016) [91]	•	•	•	•			•	•	• •	•
Milton et al. (2016) [79]	•		•						• •	
Ramakrishnan et al.(2015) [101]	•		•	•			•	• •	• •	
Perumal et al. (2015) [96]			•	•					• •	• •
Roth et al. (2014) [105]	•		•						• •	•
Samyama et al. (2014) [108]	•		•							• •
Witte et al. (2013) [133]	•								• •	• •
Cai et al. (2012) [26]		•					•		• •	
Kisku et al. (2012) [61]		•	•	•		•			• •	
En-Nasry et al. (2011) [90]	•		•	•			•	•		
Saedi et al. (2011) [106]			•	•					• •	
Lima et al. (2011) [68]	•	•	•	•					• •	

Table 3.4 – Overview: Addressed Desired Properties of the Context Information Model and its Use for AA systems.

data in [105, 106], enables taking into account the temporal dimension of contextual information.

Complexity (54%). Kumar et al. [64] discuss the complexity that human beings have almost the same palmprints. The complexity of the users' behavior is discussed in some works [114, 68]. Pititheeraphab et al. [99] discuss the complexity of image processing for the representation of context information. The complexity of algorithms to reason on context information is discussed in various works [7, 117, 91, 101]. In [96, 61, 106], the complexity of patterns is taken into account. The complexity of mobile identities is discussed in [90]. Al-Muhtadi et al. [89] model the complex usage patterns of devices in IoT environments and hence address the complexity of the contextual feature.

Heterogeneity (17%). Access patterns are assumed to be heterogeneous (*e.g.,* connections from multiple devices and locations due to travel) in [114]. Mozzaquatro et al. [88] discuss business opportunities based on a heterogeneous network of objects and their owners over the internet. Arias-Carbacos et al. [7] discuss the heterogeneity of authentication mechanisms in different contexts. In [89], the heterogeneity of IoT devices is discussed.

Abstraction (17%). To take into account the condition of reducing the amount of complexity, Miraoui et al. [82] discuss the right abstraction level of context to reduce and limit the set of contextual information. Multiple abstraction levels to provide meaningful information to understand the environment are discussed in [88]. In [117], the palmprints are represented on an abstracted level. Different abstraction levels of image fusion schemes are discussed in [61].

Privacy (38%). Several works address privacy issues related to context modeling. To take into account the condition of protecting private information, Solano et al. [114] split the keyboard into different areas to reduce

privacy concerns for the analysis of keystrokes. Unacceptable privacy invasion is discussed in [50]. *Privacy* issues concerning the collection of user data are discussed in [7], [117] and [90]. Neverova et al. [91] discuss privacy issues concerning cloud computing. The users' needs regarding the protection of private data in social media are discussed in [101]. Private keys are used for the embedding algorithm in [26]. Al-Muhtadi et al. [89] aim for privacy protection with the help of third parties (clouds). I observe that privacy is still rather abstract and there is no clear consensus in the field of authentication on which data belongs to the user and which data can be exploited.

System Relevance (25%). To take into account the condition of providing machine interpretability and sufficient support for the system's development process, authors aim to ensure the ease of implementation [99, 90]. In [74], the processing power of the central server is taken into account. The storage, memory, and processing power of devices are addressed in [91]. The system relevance is evaluated empirically in [101] in terms of energy efficiency. Al-Muhtadi et al.'s [89] framework is implemented in the IBM cloud platform.

Accuracy (75%). Many authors calculate accuracy metrics (*e.g.,* Equal Error Rate (EER), False Positive Rate (FPR), False Negative Rate (FNR)) to evaluate their approaches [71, 64, 114, 99, 74, 117, 65, 91, 79, 101, 96, 105, 133, 26, 61, 68, 106, 105].

Response Time (29%). To take into account the amount of time it takes to respond to a request for a service, several authors discuss the speed of their algorithms [65, 91]. Metrics for evaluating the response time of the system are proposed in [74, 96, 133]. Roth et al.'s [105] overall goal is to explore a biometric with a short response time for detection. Samyama et al. [108] evaluate empirically the time spend for the generation of authentication certificates.

Successful context models for AA systems have at least some of these properties, although no existing context model has them all. As CM4AA is a cross-cutting concern in multiple domains, there is a great diversity of desired properties, which play different roles in the different domains. Also, the right balance between the properties varies from domain to domain. *Accuracy*, which is the ability of the context model to reason on the context information in an accurate manner, is put forward in 75% of the reviewed papers. Biometrics are frequently used contextual features and biometric system accuracy testing is common. Also, I have seen that it is common to use contextual features that determine a unique identity. The *accuracy* of such determinations is crucial. In almost every work (94%) which is addressing *accuracy*, the property is evaluated empirically with the help of common metrics (*e.g.,* FPR, EER). These are metrics often used to evaluate the performance of machine learning algorithms. For CM4AA, it is common to use learning algorithms, for example, to detect derivations from patterns or other anomalies. Often, their *accuracy* is evaluated. The properties *response time* and *system relevance* are evaluated empirically in some works as well. Overall, however, only one-third of the properties are evaluated empirically. The desired properties of the context model seem not to be standardized enough (*e.g.,* there are no benchmark solutions for how to take into account changes in the context information along the authentication process), which is also because needs vary greatly across the different application domains. Another frequently addressed property is temporality (71%). It is common to take into account the temporal dimension of contextual information which may change its interpretation. Patterns and user habits are often based on time. The ability to take into account the changes in the context information along the authentication process is addressed as desired property in 58% of the reviewed works. The authors consider aspects of the environment that may change in the authentication system.

Lessons Learned. I observe a great diversity of desired properties of the context information model and its use for AA systems because CM4AA is a cross-cutting concern in multiple domains. The ten observed desired properties can be divided into two classes: properties related to the ability of the context model to handle specific characteristics of context information (1), and properties related to the ability of the context model to be integrated with an AA system (2). Successful context models for AA systems have at least some of these properties, although almost no context models have them all. A big challenge is to find the right balance between different properties. Very commonly the properties accuracy (75%), temporality (71%), and dynamicity (58%) are put forward. To evaluate the properties empirically benchmark solutions are missing. I provide a benchmarking methodology in this thesis to push further the development of benchmark solutions. Through the modeling framework presente din this thesis, I address the challenge of balancing desired properties. My contributions enhance the empirical evaluation of context models and provide a practical and uniformed approach to context modeling for improved AA.

3.5 SWOT Matrix - *(Strengths, Weaknesses, Opportunities, Threats)*

I summarize the findings in a SWOT analysis on CM4AA. SWOT analysis is a technique for assessing strengths, weaknesses, opportunities, and threats. With this tool, I aim to analyze what is done best right now in the research area of CM4AA, and to devise a successful strategy for future research and practice. Figure 3.12 shows the SWOT Matrix, which I derive from the analysis.

Strengths. Strengths are things that are done particularly well in the research area of CM4AA. Research conducted by observing and analyzing context information for AA systems and resulting in abstract **concepts and ideas** is well advanced. The ability of (mobile) devices to sense

their physical environment and adapt their behavior accordingly (context-awareness) is helpful to successfully model context for AA systems. Another strength is the capability to analyze **biometric and behavioral information**. These also exist thanks to modern technologies and advancements in the research area. Also, accurate approaches for **anomaly detection** exist to detect derivations from patterns.

Weaknesses. Harmful to successfully modeling context information for AA systems is the **lack of standards and benchmark solutions**, which makes it difficult to compare approaches or to present a holistic overview of context information for AA systems. **Public data** is missing, and companies do not publish their **state of the practice**. There are only **few tools** for modeling context information for AA systems which makes it difficult for AA system designers to use context information efficiently. There are only a few works treating context CM4AA at **runtime**. The **context of other entities than the user** is often disregarded. Many works are focusing on a limited set of contextual features, but there is a lack of works regarding what context information can be used for AA in a **holistic manner**.

Opportunities. Despite the weaknesses, there is a great variety of opportunities in the research field of CM4AA. There are more and more opportunities for **context-awareness** thanks to the ability of (mobile) devices to sense their physical environment and adapt their behavior accordingly. CM4AA is a **young research area** and I observe a **steady interest** in the topic. **Mobile computing environments** are great opportunities, especially for data acquirement. Another opportunity is the **use of less privacy-sensitive context information** in cases in which it is not necessary to identify a unique entity. **Privacy regulation standards** like GDPR can also be seen as an opportunity for the research area. Having different restrictions in different countries extend the scope of adaptability. Having guidelines allows for adapting in a regulated manner. Also, **anomalies** that are not based on the user's patterns and habits are an

opportunity in the research area.

Threats. I also identify threats harming successful CM4AA. The GDPR data protection standard is a threat regarding **private data collection**. It can be difficult to acquire contextual information according to these restrictions. **Disregarding non-mobile devices** is a threat as well. Often, approaches are based on mobile devices and their sensing abilities. If AA is used on non-mobile devices, the data must be acquired differently. For example, the contextual feature "location" can be acquired easily from mobile devices equipped with GPS sensors, but hardly from non-mobile devices. The **interdisciplinary** of the research area is a threat as well because notions and needs differ across the disciplines. I have seen that the balance between desired properties of authentication mechanisms is crucial for AA. This balance may also depend on the domain. The **heterogeneity of context information and devices** is another important threat because they need to be taken into account when the context information is modeled for AA systems. Desired properties of the context information model and its use for AA systems are still rather abstract and it is hard to evaluate them empirically.

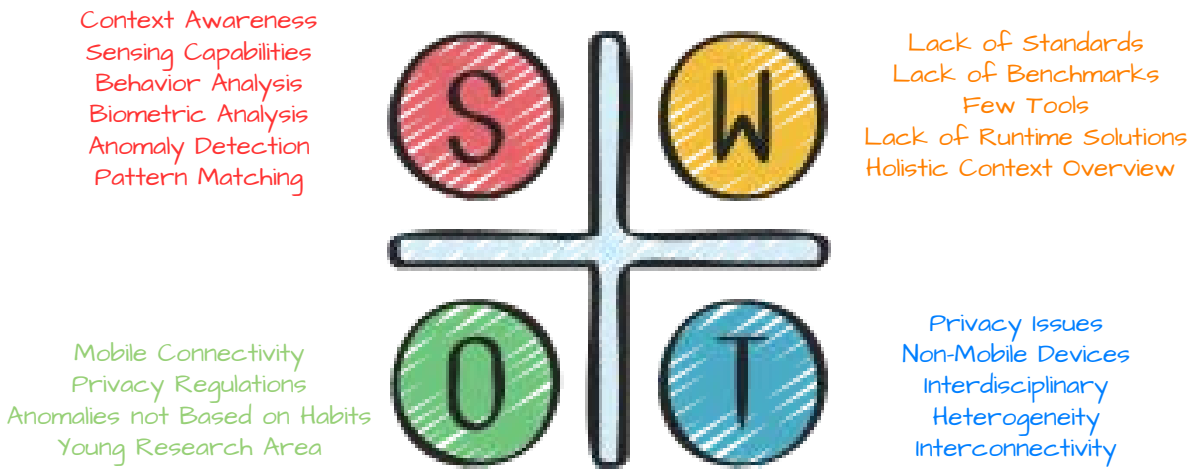

Figure 3.12 – Research field of CM4AA - SWOT Matrix.

In my research, I focus mainly on the identified weaknesses to further advance the research field. Points that already belong to the strengths I treat less intensively. Threats and Opportunities mainly motivate my future research perspectives.

3.6 Threats to Validity of the Study

Troya et al. [120] study four basic types of validity threats that can affect studies like ours. I cover three of them in the following. As this work is a review of a specific topic, I do not intend to make any generalizations and hence do not treat the threat type *external validity*.

Conclusion Validity. Issues that affect the ability to conclude and whether the review can be repeated concern the conclusion validity [120]. The availability of the raw search results and the set of excluded studies on my companion webpage mitigates these threats. The analysis metrics can easily be repeated and verified. Like Troya et al. [120], I did not include works not (yet) published or submitted even if they might alter the results of the study. I assume that the disadvantages of inclusion (*e.g.,* lack of quality, the difficulty of identification) outweigh the advantages. I am aware that the number of the articles is relatively small. As there are many different works in the field of context-awareness and modeling, I prefer to concentrate on this particular selection of works to ensure the meaningfulness of the analysis for authentication systems.

Construct Validity. I mitigate the issue known as meno-method bias [120], that might arise during research design by following the methodologies of SMS and SLR. Another threat regarding the construct validity is that particular works can be categorized in more than one dimension of the analysis aspects. I mitigate this issue by assigning the dimension that fits best according to multiple analysts from the authentication and the modeling domain. I observe that there is no clear consensus on which are the most important properties of the context information model and its use

for AA systems. The definition of the terms is still rather abstract. The analysis therefore only indicates what can be crucial, but I do not have any evidence to justify that if none of these properties is satisfied, the technique is not successful.

Internal Validity. According to [120] the main factors influencing the publication selection process and therefore affecting the results of the evaluation are keywords, digital libraries, the language of publication, and time frame. I avoid too restrictive decisions by including a disjunction of terms expressing the adaptation capability of the authentication system in the search clause. Also, I included different spellings of the terms. To mitigate sampling and publication bias, I conduct searches on formal databases (*e.g.,* ACM Digital Library) and indexes (*e.g.,* GoogleScholar).

3.7 Summary

Within this chapter, I synthesize the current body of knowledge about CM4AA, what context information determines the context of AA systems, how the context information is modeled, how the context information model is used, and what are the desired properties of the context information model and its use for AA. I shed light on three research questions and I offer an overview of existing research that authentication engineers and non-domain experts can use. For each research question, I collected a certain amount of raw data on the selected articles, and I defined a set of metrics allowing me to analyze this raw data.

I observe a **continuous interest** in the research field of CM4AA over the last ten years. Most of the reviewed publications (91%) are **not specific to any application domain**. 16% of the contributions are of the contribution type **tool**. AA is a new research area so not yet every proposed concept of how to model context information for AA systems goes beyond conceptualization and results in a tool. In the research field of CM4AA, it is widespread to acquire context information from **sensors of mobile devices** to describe the context of a **user**. The most frequently used con-

textual features for AA systems are **biometrics**, the **entities behavior** and the **location**. The contextual features are mostly analyzed in **time**. I cannot observe a trend in the use of a **modeling technique** to model context information for AA systems but I can identify a set of common goals. There is a great diversity of modeling formalisms proposed in the literature. The context information models are mostly used at the **design time** (63%) and **deployment time** (42%) of AA systems. There is a lack of works treating CM4AA at **runtime** (8%). According to the percentage of works putting forward each of the desired properties, accuracy (78%), temporality (74%), security(70%), and dynamicity (61%) seem to be the most important desired properties of the context information model and its use for AA systems.

The results of this literature review motivate the following contributions of this thesis and report the body of knowledge about CM4AA. Efforts are necessary to find out how to leverage context information for authentication decisions beyond risks scores. The need for standardization, abstraction, and a common language in the field of AA is evident due to the lack of clearly delimited terms, the cross-cutting nature of AA, and the diversity of context information and modeling approaches. My thesis aims to address these challenges and promotes a consistent understanding and communication among researchers and practitioners. By providing a modeling framework for AA called CoFrA, I contribute to the development of reusable and modular concepts, models, and protocols. This facilitates the translation of concepts into concrete tools and promotes better regulation and increased user willingness to share context information for authentication purposes. While existing works in context-aware AA often focus on context-awareness alone, my thesis emphasizes the importance of the system's ability to adapt and apply suitable authentication methods based on the context. Constructs are proposed to enable reasoning about the appropriateness of authentication methods in different contexts, ensuring that both context-awareness and adaptation are considered. Furthermore, I introduce domain-specific concepts and a domain-specific modeling framework to authentication, addressing the limitations of generic modeling con-

cepts proposed in the literature. This provides engineers with familiar notions and a more precise and expressive way of modeling authentication systems. Due to privacy concerns and the lack of publicly available data, developing tools and benchmark solutions in AA is limited. My thesis tackles this challenge by proposing a methodology for comparing and evaluating AA models. The evaluation metrics and methodology contribute to the development of benchmarks, facilitating advancements in the field. Additionally, my thesis addresses the gap in capturing authentication security rules and threats in the context model, as only a small percentage of existing works consider these aspects. The modeling approaches proposed in this thesis capture security threats and risks.

Looking at the SWOT analysis presented in this chapter, I mainly focus my research on the identified weaknesses to further improve research in the field. Points that already belong to the strengths are not the focus of my work. More precisely, with my thesis, I address the lack of standards and propose the first common language for AA. With the help of the framework's abstraction, I enable a holistic context overview. This standardization together with the transition support from RBA to AA also helps pushing forward the development of tools and runtime solutions for AA. I also propose a methodology to evaluate and compare authentication models to push further the development of benchmarks.

Chapter 4

A Context-Driven Modeling Framework for Dynamic Authentication Decisions (CoFrA)

This chapter presents the second contribution of my thesis, the CoFrA *modeling framework for Adaptive Authentication (AA). It is an extended version of the paper "A Context-Driven Modeling Framework for Dynamic Authentication Decisions (CoFrA)" [22] published in the 48th Euromicro Conference Series on Software Engineering and Advanced Applications (SEAA). I aim to abstract the domain knowledge obtained from the state-of-the-art and the state-of-the-practice and to provide a language to determine the appropriate authentication methods in a context beyond the calculation of risk-scores. Figure 4.1 highlights this second contribution in the global vision of this thesis. I first recall the main idea of leveraging context information to determine the appropriate authentication method(s). Then, I detail the* CoFrA *modeling framework. I describe the metamodel, its properties, the framework usage, and the framework evaluation.*

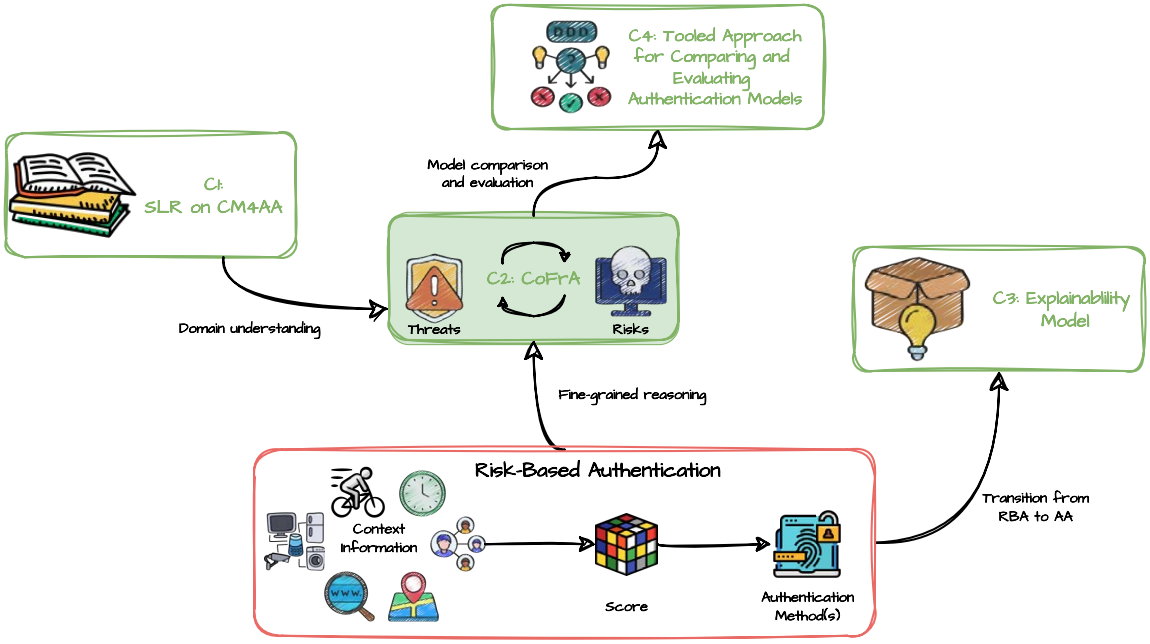

Figure 4.1 – Contribution 2: A Context-driven modeling Framework for adaptive Authentication (CoFrA).

Contents

4.1 Leveraging Context Information to Determine the Appropriate Authentication Methods

Due to the diversity of modeling approaches and their heterogeneity (Chapter 3), context modeling for AA is not a straightforward task. Nevertheless, I have shown within the literature review the ability of capturing a common set of contextual features that are relevant for AA independent from the application domain. Despite the possibility of a unified framework, no modeling framework exists. In this chapter, I hence introduce the **Context-driven Modeling Framework for dynamic Authentication decisions (CoFrA)** to address this issue. We have seen in Chapter 3 that research about CM4AA is mainly driven by the authentication community. Hence with this contribution, I also aim to link the fields of authentication and modeling to advance and improve AA. This enables the fusion of context-awareness (mainly driven from the authentication point of view) with adaptation (mainly driven from a modeling point of view). This framework is based on a fine-grained mapping of context information to authentication methods. The main objective is to abstract domain knowledge about context modeling for AA systems gathered from the literature and experience in the industry in a modeling framework and to support authentication engineers to take full advantage of context information beyond a risk score. The diversity of concerns (*e.g.,* security, usability, deployability,privacy) and details about the contextual situation (*e.g.,* type of risk faced, usability constraints) are taken into account. As stated earlier, until now, context information is primarily used to calculate risk scores, which estimate the probability of impersonation [48, 119]. Nonetheless, the question of which authentication methods are appropriate (*e.g.,* for security, usability, deployability, and privacy) in the given context is disregarded. I stated in Chapter 1 that scores are insufficient to select the appropriate authentication methods concerning two main points. First, the fusion of the contextually available features in a one-dimensional risk score reduces the comprehensibility and explainability of risks (1). Second, context information not only influences the risk of an unexpected or sus-

picious login attempt but also concerns other properties of authentication methods (*e.g.,* usability, deployability, privacy) (2). More specifically, to tackle the restrictions of RBA approaches and to support authentication engineers in a more fine-grained mapping, I propose CoFrA. To go beyond risk scores, context information specify the appropriateness of authentication methods, along with four required concerns identified in the literature and the practice[1]:

— **Usability**, which is the condition of being able to be used (*e.g.,* the authentication method is easy to understand for a user)
— **Deployability**, which is the condition of being able to be deployed (*e.g.,* the user's smartphone is equipped with a camera to perform face recognition, the implementation costs of the authentication methods are not too high)
— **Security**, which is the capability to protect the major system aspects along the authentication process (*e.g.* by minimizing the likelihood of an attack)
— **Privacy**, which is the ability to protect private context information (*e.g.,* by confirming consent for the request for personal identifiable information)

The CoFrA framework has been generated based on knowledge obtained through the systematic literature review, together with the experience from industry gathered through extensive exchanges with authentication, security, and identity experts.

4.2 Metamodel

The purpose of this metamodel is to define and represent the relationships between various components involved in the reasoning process about the appropriateness of authentication methods according to the context. It provides a structured way to model and understand the dependencies between context information, threat situations, risks, and authentication

1. The conception of the framework allows for extension. Additional properties can be taken into account and weightings can be chosen according to specific needs.

methods allowing authentication engineers to select appropriate authentication methods based on contextual factors and their associated properties (usability, security, privacy, and deployability). By using the metamodel, authentication engineers can design AA systems, considering diverse factors like context information availability, privacy-sensitivity, environmental circumstances, and the characteristics of threats and risks. This facilitates the decision-making process for implementing authentication systems to mitigate security risks while ensuring optimal usability, deployability and privacy.

The structure of CoFrA is represented in Figure 4.2 [2] and captures the core domain concepts and relationships. CoFrA is based on the de-facto standard MDE framework *Eclipse Modeling Framework (EMF)*. I use sufficient generalization (inheritance) to group common elements from different classes sharing abstract definitions. Considering the difficulty of expressing some information in a diagrammatic way, I specify 15 textual constraints in *Object Constraint Language* (OCL) to restrict the scope of some defined concepts. [3] For example, to align with the **Data Protection by Default Principle of Art. 25 GDPR** [4], I define a OCL constraint ensuring that the use of less privacy-sensitive context information is privileged in the model. In [31], the authors investigate metamodel inaccurate structures that are often completed with OCL constraints. Based on their analysis, I propose sufficient constraints to avoid such inaccuracies. The defined constraints restrict how the structural elements can be instantiated and assembled to form a valid model with respect to the domain semantics.

Figure 4.2 shows the main concepts of CoFrA in an Ecore-based metamodel.

A **ContextInformation** defines any context information that can be used for AA, *e.g.,* the geolocation of an entity. ContextInformation can be either **RequiredContextInformation** that represents any context information required in the authentication system, or **AvailableContex-**

2. For visibility reasons I do not show the root class ModelingFramework.
3. The totality of the OCL constraints is available on my companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/tree/main/CoFrA%20Metamodel%20Implementation).
4. https://gdprhub.eu/Article_25_GDPR

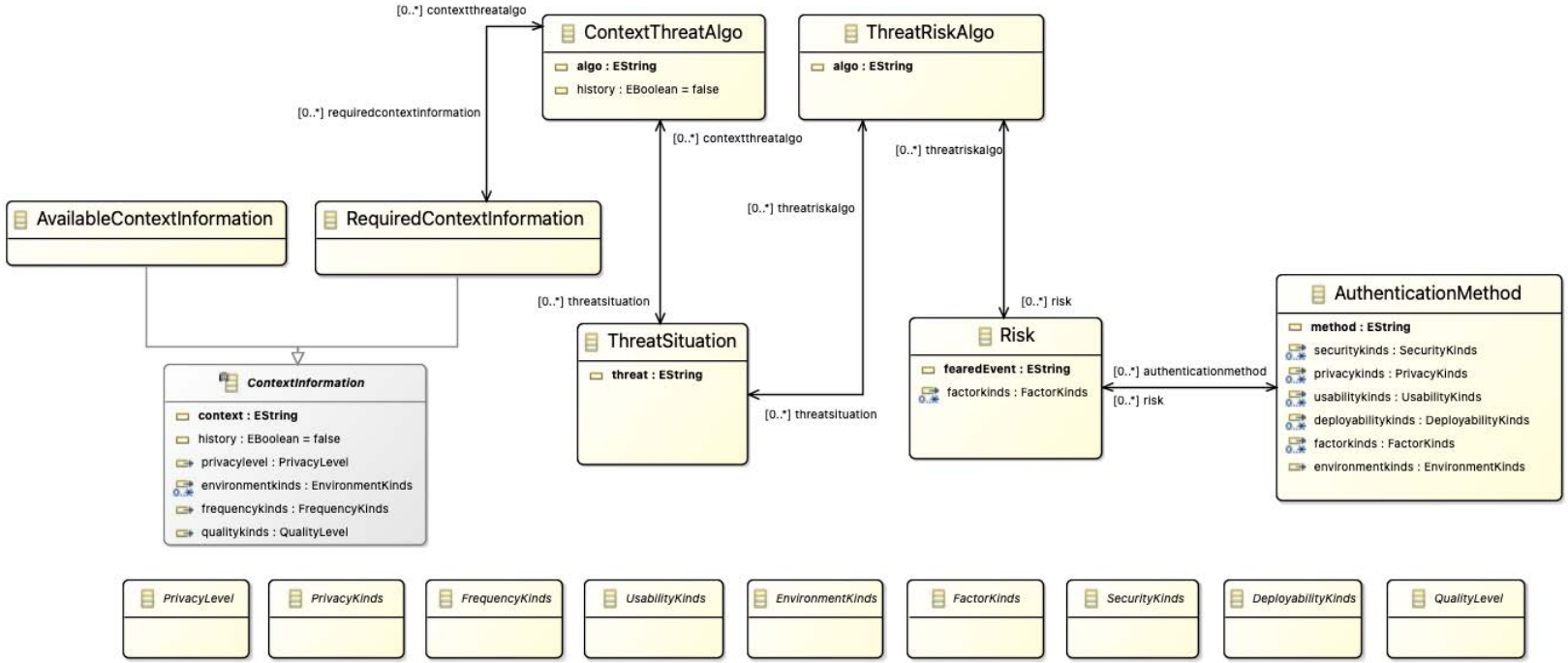

Figure 4.2 – Ecore Diagram of the CoFrA Metamodel.

tInformation that represents any context information actually available in the authentication system. Available and required context information are aligned as soon as the required information is available and the formats of the available and required information match (the attribute values of the available information must match those of the required information). The question of availability arises for example when users use both mobile and static devices, as it is common today. Context information acquirement with mobile devices (*e.g.,* smartphones) is often easier (more integrated sensors) than with non-mobile devices. Anyway, non-mobile devices must not be neglected, and therefore, the question of availability must be considered. The *context* of a ContextInformation instance uniquely describes the context information (*e.g.,* "geolocation"), and the *history* describes whether the history of the context information is available or required, for AvailableContextInformation or RequiredContextInformation respectively. For example, the history of the context information "geolocation" is required to detect derivations from geolocation patterns. The *privacy* attribute describes the context information privacy-sensitivity level (*e.g.,* "luminosity" is not privacy sensitive while the user's "geolocation" is). The *environment* (*e.g., darkness*, *noise*, *activity*, *surrounded*) describes the environmental circumstances influenced by the context information. For example, the context information "luminosity" influences the "darkness" circumstance. The *quality* describes the quality of the context information (*e.g.,* precision level). Finally, the *frequency* describes the frequency at which the context information is available. For example, to determine fast location changes of users, which are suspicious, the "geolocation" needs to be used at a high frequency.

A RequiredContextInformation is related to a **ContextThreatAlgo** that determines **ThreatSituation**s from the context information, *i.e.,* defines any algorithm that can be used to determine ThreatSituations from required context information (*e.g.,* an anomaly detection algorithm to determine derivations from a user's usual "geolocation"). The *algo* of a ContextThreatAlgo describes uniquely the actual algorithm (*e.g.,* "anomalyDetector"). The *history* of a ContextThreatAlgo in-

stance describes whether the history the algorithm makes use of the history of a RequiredContextInformation. The *threat* of a ThreatSituation instance describes uniquely the threat (*e.g.,* "newLocation").

A ThreatSituation is related to a **ThreatRiskAlgo** that characterizes **Risk**s from ThreatSituations. For example, the risk of a stolen password can be characterized by a derivation of a user's habits regarding the geolocation, because it may be an intruder who is using the legitimate user's password from another geolocation. The *algo* of a ThreatRiskAlgo describes uniquely the algorithm (*e.g.,* "StolenPasswordCharacterization"). Any Risk is characterized by the *fearedEvent* (*e.g.,* "StolenPassword") and the *factor*s (*i.e.,* a list of possible secrets owned by the intruder (*e.g.,* knowledge)).

Finally, any Risk is related to **AuthenticationMethod**(s) (*e.g.,* "username password") describing which authentication methods can be applied to provide countermeasures against the risk. The *method* describes uniquely the method (*e.g.,* "username password"). The *usability* attribute is a list of usability benefits (*e.g.,* nothing to carry, memory-wise effortless), the *security* attribute is a list of security benefits (*e.g.,* resilient against phishing), the *privacy* attribute is a list of privacy benefits (*e.g.,* no personal user information), and the *deployability* attribute is a list of deployability benefits (*e.g.,* negligible costs per user, browser compatible). The *factor* attribute describes the credential exchanged between the entity to be authenticated and the authenticating entity used by the authentication method (*e.g., knowledge*, *possession*, *being*). The *environmentKinds* describes the environmental circumstances in which the authentication method is efficient to use (*e.g., darkness*, *noise*, *activity*, *surrounded*).

A set of values for *EnvironmentKinds*, *PrivacyLevels*, *FrequencyKinds*, *PrivacyKinds*, *FactorKinds*, *DeployabilityKinds*, *SecurityKinds*, and *UsabilityKinds* are provided within a standard library included in the modeling framework. I built the library based on reviewed scientific literature (*e.g.,* [44, 123, 124, 16, 128]), as well as interviews with domain experts:

— **SecurityKinds:** Resilience to Physical Observation, Resilience to Targeted Impersonation, Resilience to Throttled Guessing, Resilience

to Unthrottled Guessing, Resilience to Internal Observation, Resilience to Phishing, Resilience to Physical Theft, Resilience to VPN Attack, Resilience to DoS Attack, Resilience to Replay Attack, Resilience to Replay Attack, Resilience to Internal Observation, Resilience to Observation from Third Parties, Requiring Explicit Consent, No Trusted Third Party

— **UsabilityKinds:** Memorywise Effortless, Nothing to Carry, No Additional Network Access, Frictionless Setup, Scalable for Users, Affinity to Users, Ease to Use, Ease of Learning, Ease of Recovery, User Choice, Scalability for Users, Physically Effortless, Infrequent Errors, Not too Complex, Efficient to Use, Social Acceptability, Low Annoyance
— **DeployabilityKinds:** Accessibility, Negligible Costs per User, Negligible Implementation Costs, Server Compatibility, Browser Compatibility, Maturity, Non-Proprietary
— **PrivacyKinds:** Information Sensitivity, User Anonymity, Information Collection, Compromise of User Personal Details, Unlinkability, Concealability
— **PrivacyLevels:** low, medium, high
— **EnvironmentKinds:** noise, darkness, surrounded
— **FactorKinds:** knowledge, possession, being, location, behaviour, human
— **FrequencyKinds:** low, medium, high

I also provide a list of common instances for the meta-classes with references and explanations[5]. I further explain the usage of the library in Chapter 7.

5. The values are available on my companion webpage: https://github.com/BumillerAnne/CoFrA-Studio/tree/main/StandardLibrary.

4.3 Evaluation of Authentication Methods Based on Security, Usability, Deployability, and Privacy

With the help of CoFrA, the appropriateness of authentication methods can be evaluated according to multi-criteria optimizations of four required properties as identified in the literature review and expert interviews: *security*, *usability*, *deployability* and *privacy*.

Security. To evaluate the security of authentication methods, other works evaluate their resilience against different attack types [44, 123, 124]. With the same intention, the framework focuses on the resilience against risks (*e.g.,* the risk of stolen memorial credentials). I argue that an authentication method is resilient against a risk if an attacker does not own the authentication *factor* that the authentication method is based on. Therefore, the Risk class and the AuthenticationMethod class own the attribute *factor* and I enforce this property with a OCL constraint. To further describe the authentication methods, they also own an attribute *security* which is a list of desirable security benefits of authentication methods that are put forward in the literature to date.

The following OCL invariant concerns the security property. The risks are characterized by the authentication factors that the intruders are in possession of. Authentication methods applied to provide countermeasures against the risks must not be based on the factors that the intruder is in possession of. For example, in the case of a stolen password, the intruder owns the “knowledge" factor, and the authentication method “password" based on the “knowledge" factor must not be used. The OCL invariant *FactorCheck* makes sure that the intruder does not own an authentication method’s factor.

```
class Risk
    invariant FactorCheck:
        self.authenticationmethod.factor
            ->excludesAll(self.factor));
```

Usability. To ensure the usability of an authentication method in a context, I take into account the environmental circumstances influenced by the context information and ensure that the used authentication method is efficient to use in these circumstances. For example, it is guaranteed that face recognition is not used in the dark. I also take into account desirable **usability** benefits of authentication methods that are put forward in the literature to date. The authentication method class owns the attribute *usability* which describes the usability of the method.

The following OCL invariant concerns the usability property. When context information impacts the environmental circumstances, the authentication methods applied to provide countermeasures against risks that are characterized by this context information need to be efficient to use within the environmental circumstances. For example, when context information impacts the luminosity in a room so that it is dark around the user, I cannot use the authentication method “face recognition". In times of pandemic, a relevant example of the need to use contextual information to determine the efficiency of authentication methods in environmental circumstances is the non-efficiency of face recognition when face masks are worn. The OCL invariant *EnvironmentCheck* ensures the efficiency of authentication methods within the environmental circumstances.

```
class RequiredContextInformation
    invariant EnvironmentCheck:
        self.contextthreatalgo.threatsituation.threatriskalgo.risk.authenticationmethod.
            environmentKinds
            -> includesAll(self.environment);
```

Privacy. I take into account desirable **privacy** benefits of authentication methods that are put forward in the literature to date. The authentication method class owns the attribute *privacy* which describes privacy benefits. Also, the context information class own an attribute *privacy* which describes the privacy-sensitivity level of the context information. I enforce the property with an OCL constraint ensuring that the less privacy-sensitive context information available is used.

```
class ContextThreatAlgo
    invariant PrivacySensitivity:
    let lowestPrivacyLevel = self.requiredContextInformation->sortedBy(ci | ci.
        privacyLevel)->first() -> lowestPrivacyLevel.privacyLevel < self.privacyLevel;
```

Deployability. I take into account desirable **deployability** benefits of authentication methods that are put forward in the literature to date. The authentication method class owns the attribute *deployability* which describes deployability benefits. I enforce the property with an OCL constraint ensuring that the authentication method which is the most easily deployable is privileged.

```
class AuthenticationMethod
    invariant DeployabilityOptimization:
    self.DeployabilityKinds->size() >=AuthenticationMechanism.allInstances()
    ->select(oclIsNew()).DeployabilityKinds->size();
```

In this section, I presented four examples of the OCL invariants that I used to complete the metamodel's structure. In this way I ensure that I address the required properties of security, usability, deployability, and privacy. The totality of all OCL invariants is available on the companion webpage. [6]

4.3.1 Desired Properties of the Context Information Model and its Use for AA Systems

In addition to the required properties on authentication methods (security, usability, deployability, and privacy), I also identified desired properties of the context information model and its use for AA systems in Chapter 3. These properties go beyond the authentication method itself and pertain to the context information model and its use to enhance security, usability, privacy, and deployability. In the following, I describe how I address these desired properties in the CoFrA model.

— **Dynamicity:** A CoFrA model is instantiated with algorithms which are executed along the authentication process. Hence changes in the

6. https://github.com/BumillerAnne/CoFrA-Studio/blob/main/CoFrA%20Metamodel%20Implementation/modellingFrameworkContext4Authentication.ocl

context information are taken into account.

— **Quality:** The quality attribute of the ContextInformation class describes the exactitude of the context information.
— **Temporality:** Time can be instantiated as a context information and being taken into account by context-threat algorithms in a CoFrA model.
— **Complexity:** The context-threat algorithms can take as input an unlimited number of context information and hence consider context as a mesh consisting of many different and connected information.
— **Heterogeneity:** I propose a set of necessary and sufficient attributes to distinguish and describe heterogeneous context information.
— **Abstraction:** CoFrA has been shown to provide the right level of abstraction (necessity and sufficiency have been shown in the validation).
— **Privacy:** The privacy attribute of the ContextInformation class describes the privacy sensitivity of the context information.

These are all the properties I identified which are related to the ability of the context model to handle specific characteristics of context information. The second set of properties which I identified in Chapter 3 are related to the ability of the context model to be integrated with an AA system. I do not directly address them in the framework. They become important when it comes to the implementation of a CoFrA model. Hence, I discuss them in Chapter 7.

4.3.2 Framework Usage

In this section, I describe how CoFrA can be used by authentication engineers. The framework supports the authentication engineers in the complex trade-off analysis between context information, risks, and authentication methods, according to usability, deployability, security, and privacy. This enables the use of context information for authentication decisions not only to calculate a risk score but to reason on the appropriateness of authentication methods according to the contextual situation

and identified risks.

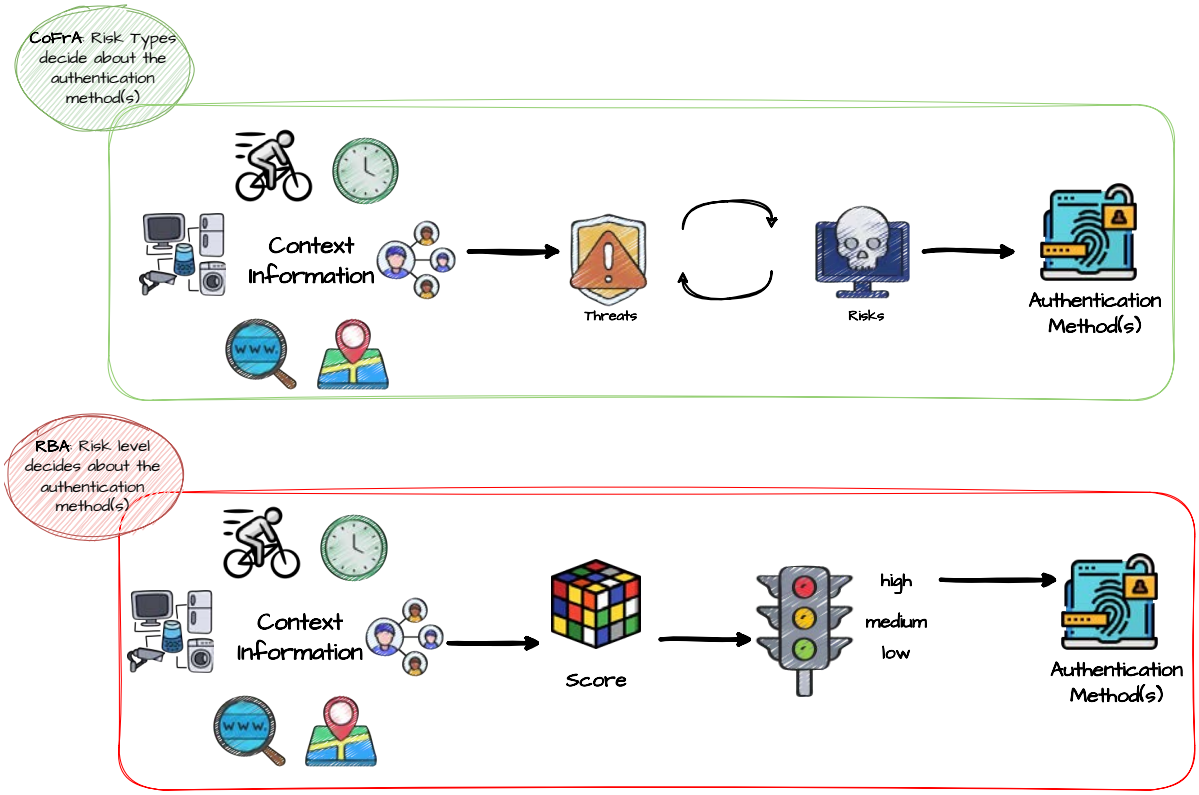

Figure 4.3 – The CoFrA Framework in Contrast to RBA Approaches.

Figure 4.3 shows the main functionality of CoFrA in contrast to RBA approaches (*e.g.*, [129]). Instead of using the context information to calculate a risk score and to choose the authentication method based only on this score, CoFrA enables a more complex mapping of context information to authentication methods with the help of multiple threat situations and risks. The final goal for an authentication engineer is to obtain an AA system design model: context information to use, threat situations to determine, risks to identify, and authentication methods to use.

Let us again take the example of Bob, the traveler (Chapter 1). If a RBA approach is applied to this model, it means that the email provider would assign a high-risk score based on the context information time, location, typing speed, and luminosity. However, without additional information, the email provider cannot determine the most suitable authentication method

among the three available options: password, fingerprint, and face recognition. For instance, without considering the type of risk (in this case, a stolen password), the intruder may be prompted to enter the password again. Additionally, face recognition may be selected as an authentication method even though the lighting conditions are poor. On the other hand, if an AA approach is used in this example, the type of risk is considered, and password would not be selected as an appropriate authentication method. Moreover, the usability aspect is taken into account, and the email provider would choose fingerprint over the password as the most suitable authentication method.

To provide an integrated no-code environment on top of the modeling framework and hence facilitate the usage, I created a graphical modeling workbench, named CoFrA Studio, by leveraging the Eclipse Modeling technologies, including the *Eclipse Modeling Framework* (EMF). This modeling workbench created with Sirius is composed of a set of Eclipse editors (diagrams, tables and trees) which allow the authentication engineers to create, edit and visualize CoFrA models. Hence, I propose a modeling tool which natively supports the vocabulary to create a valid CoFrA model. I provide details about the implementation in Chapter 7.

4.4 Framework Evaluation - Case Studies

In this section, I present the evaluation of the approach. I illustrate how the proposed framework can be used for context modeling of various authentication applications. For each application, I create an instance of the metamodel and run a OCL validation. The evaluation protocol consists of selecting hypothetical cases, cases from the literature, and real-world cases to validate the framework. This shows that the amount of abstraction covers all domain concepts (**sufficiency**) without specifying unnecessary, too many details (**necessity**). I demonstrate that the approach can handle all the cases and allows us to present them in a clear manner (**soundness**). Finally, I demonstrate that the approach can design, validate and deploy the AA system design for all the chosen cases.

4.4.1 Evaluation Setup

The goal of the CoFrA framework is to provide constructs for authentication engineers to reason on authentication methods according to the context. To validate the appropriateness of the abstraction provided, I discuss

1. The domain concepts coverage of the framework's abstraction (sufficiency)
2. The amount of detail required to specify most contexts (necessity)
3. The framework's ability to correctly handle concrete example cases and to present them in a clear manner (soundness)

I select hypothetical cases, cases from the literature, and real-world cases to support the discussion.

Cases From the Literature. I create CoFrA models of existing context modeling approaches for context-aware authentication proposed in the literature review (Chapter 3). For each identified modeling objective (Chapter 3), I selected one work.

— **Capture authentication security rules and threats:** Miraoui et al. [82] propose an approach that provides smartphones users with the appropriate method for authentication according to the current context based on rule-based modeling. The authentication method is chosen based on rules and more specifically on a mapping of each possible context vector to the appropriate authentication method. The approach relies on four ContextInformation instances: *noise*, *nearby people*, *driving*, and *alone*. Context vectors are build with every possible combination of contextual features. The three AuthenticationMethods *fingerprint*, *something you know*, and *voice* are then mapped according to their efficiency to use. This work can be modelled with the help of CoFrA and especially thanks to the attributes *environment* of the ContextInformation instances and the AuthenticationMethod instances. This work is exclusively based on rules concerning the efficiency of authentication methods in

different contextual situations. RISKs and THREATSITUATIONS are not considered.

— **Visualize the organisation and relationships among different functionalities of the system:** Gunjal el al. [50] propose a secured authentication scheme which is based on a trust evaluation with the context. Their approach is presented as a component diagram of the system architecture. This work is specifically for online learning systems. As CONTEXTINFORMATION, user data and device data is used: *time spent on the study-content*, *frequency of visits to similar type of study-content*, *frequency of device changing*, *location*, *knowledge level* and *types of queries asked*. A CONTEXTTHREATALGO validates the credibility of the learner. The THREATSITUATIONS based on the different levels of credibility are then analysed by a THREATRISKALGO checking the genunity of the learner. Depending on the genunity, the learner is asked to perform different AUTHENTICATIONMETHODS: *enter date of birth*, *assessment details*, *question about his service*, and *his route plan for studying*. These methods are all based on the *knowledge factor* and can hence only be differentiated by other properties.

— **Formalize mathematically complex relationships:** Lima et al. [68] propose an approach that provides a recommendation system for authentication methods based on the user behavior and the pervasive space where he belongs. The approach is based on a formal recommendation method where context is added as a new dimension to the model. Six CONTEXTINFORMATION are used: *user calls*, *user schedule*, *gps*, *device battery level*, and *user applications*. *Profiling* and *recommendation filter* are applied as CONTEXTTHREATALGOS. THREATSITUATIONS are build based on the similarity degree of the features and existing user profiles. A belief analyzer (THREATRISKALGO) then identifies the three RISKs of *normal attempt*, *suspect attempt*, and *abnormal attempt*. The AUTHENTICATIONMETHODS are then applied accordingly. This approach is quite similar to RBA approaches where the risk level decides about the authentication method(s) to

use.

— **Represent authentication system processes:** Kumar et al. [65] propose an authentication system based on unlabeled phone movement patterns collected through smartphone accelerometer. They present a flowchart diagram including the processes of context identification, preprocessing, feature extraction, clustering, training, scoring, and authentication. The input ContextInformation are *accelerometer records*. *Semi-supervised models* are used as ContextThreatAlgos to divide the phone movement patterns into well-known human activities (ThreatSituations). *Distance-based similarity* and *structural-based similarity* are used to identify the Risk of being an *imposter attempt*.

Hypothetical Cases. I create CoFrA models for two hypothetical cases: the motivational example of Bob introduced in Chapter 1 whose contextual situation considers an extreme case (*i.e.,* many derivations from the user's patterns), and a second hypothetical case of Alice whose contextual situation considers a standard case.

— **Bob - The Traveler.** This exemplary model consists of the ContextInformation *geolocation*, *luminosity*, *time*, and *typing speed*. The ContextThreatAlgos are *anomaly detection* algorithms to identify the ThreatSituations *unusual location*, *unusual typing*, and *unusual time*. The ThreatRiskAlgo is based on domain-rules of the email provider and determines the Risk of a *stolen password*. To ensure efficiency to use in the dark the AuthenticationMethod *fingerprint* is chosen from the set of available methods: *fingerprint*, *face recognition*, and *password authentication*.

— **Alice - The Employee.** Alice, an employee accesses her emails on a Monday at 09:03 AM as usual. She is in her usual workplace, and she is using her device. Her email provider can acquire ContextInformation: *IP address*, *user agent*, and *time*, and determines that there is no ThreatSituation concerning these features. This makes the email provider assume that there is no Risk. Therefore, the authen-

tication can be done with any method from a security point of view. The AUTHENTICATIONMETHOD which is the easiest to use for Alice is used.

Real-world Case. As a real-world case I take Orange™ 's *IAlerting* project. The project's origins come from the need to notify the user in the case of changes in the device or the country. The notifications are created based on successful authentication events containing the CONTEXTINFORMATION date (time), the IP address (country), and the user agent (device). Based on this information, indicators (THREATSITUATIONS) that the user needs to be notified (*new IP address*, *new location*, *new device*, *fast location change*, and *robot suspected*) are calculated. The indicators can be classified according to three RISKS: *stolen memorial credentials*, *stolen devices*, and *robots*. This real-world application consists of three CONTEXTINFORMATION instances, five instances of the class CONTEXTTHREATALGO, five THREATSITUATION instances, three instances of the class THREATRISKALGO, three RISK instances, and four AUTHENTICATIONMETHOD instances.

Model	Case Type	CoIn	CoThA	ThSi	ThRiA	Ri	AuMe
Miraoui et al. [82]	L	4	1	16	0	0	3
Gunjal et al. [50]	L	6	1	3	1	1	4
Lima et al. [68]	L	6	1	1	1	3	0
Kumar et al. [65]	L	1	1	4	1	1	0
Bob - The Traveler	H	4	3	3	1	1	3
Alice - The Employee	H	3	3	0	0	0	0
IAlerting	RW	3	5	5	1	3	4

Table 4.1 – Number of Instances of the Metaclasses (L: Literature, H: Hypothetical Case, RW: Real-World Case).

Table 4.1 shows an overview of the models and the number of instances for each meta class. There are a total of 7 models listed in the table, each representing a specific case type (Literature, Hypothetical Case, or Real-World Case). Out of the 7 models, 4 are based on Literature (L), 2

are Hypothetical Cases (H), and 1 is a Real-World Case (RW). The number of ContextInformation instances ranges from 1 to 6. The number of ContextThreatAlgo instances ranges from 1 to 5. The number of ThreatSituaton instances ranges from 0 to 16. The number of ThreatRiskAlgo instances ranges from 0 to 1. The number of Risk instances ranges from 0 to 3. The number of AuthneticationMethod instances ranges from 0 to 4. The small number of algorithms comes from the fact that the use cases address specific threats and risks. This underlines the challenge of developing models for various specific use cases and the complexity of integrating a large number of risks and threats into a single framework. We observe that the number of ContextInformation instances is usually larger than the number inferred ThreatSituations and Risks. Hence in the reasoning process about the appropriateness of authentication methods information gets lost. the fact that all these use cases can be modeled with CoFrA shows that this modeling framework enables the design of a more holistic AA model integrating a large number of risks and threats. The CoFrA models for these use cases can be found on my companion webpage [7].

4.4.2 Results

I present the results of the evaluation to validate a) the sufficiency, b) the necessity, and c) the soundness of the framework.

Sufficiency. To highlight the sufficiency of the framework, I create CoFrA models of the literature use cases. For each category of modeling objective, I modelled one approach and successfully built the model conforming to CoFrA. I can abstract all the notions of the approaches within the classes of the metamodel. I model the hypothetical cases of Bob and Alice, as well as the IAlerting application. All the notions can be abstracted within my metamodel's classes, highlighting my model's sufficiency.

7. https://github.com/BumillerAnne/CoFrA-Studio/tree/main/Use%20Case%20Models

Necessity. To model the use cases, I make use of all the meta-classes and all the OCL constraints for at least one of the CoFrA models. This demonstrates that there are no unnecessary metaclasses.

Soundness. I conduct a case study based on a hypothetical application whose contextual situation considers a standard case and an extreme case. I can successfully create a CoFrA model of these hypothetical cases. This shows the soundness of the metamodel in the presence of standard and extreme features. To prove the soundness of the framework in real-world applications, I model the IAlerting project. I can successfully model the project to conform to the metamodel, which shows the soundness of the metamodel in the presence of real-world cases.

The conducted case studies show that the amount of complexity allows covering all domain concepts (**sufficiency**) without specifying unnecessary, too complex details (**necessity**). Also, this studies show **soundness** of the model for standard and extreme cases as well as for real-world applications.

4.5 Summary

This contribution aims to cover an existing gap in the literature: the lack of a method for reasoning about the appropriateness of authentication methods according to the context and four required properties of the methods: security, usability, deployability, and privacy. I propose a modeling framework to realize this, which covers the shortcomings of existing works based on risk scores. Both the knowledge from literature and the experience from industry were gathered through this work to learn the needs of both sides and obtain added value to the proposals given by this contribution. The model's validity in terms of sufficiency, necessity, and soundness is ascertained through three case studies. My main contribution is creating a precise modeling framework and a domain-specific language based on the academy and the industry, which allows authentication engineers to use context information efficiently for authentication.

Chapter 5

Towards a Better Understanding of Risk Scores

This chapter presents the third contribution of my thesis, the explainability model for Risk-Based Authentication (RBA) models. It is an extended version of the paper "Towards a Better Understanding of Impersonation Risks" [24] published in the 15th IEEE International Conference on Security of Information and Networks (SINCONF). The explainability model helps the transition from Risk-Based Authentication (RBA) to Adaptive Authentication (AA) which can be a gradual process since many companies have already implemented RBA. Hence, the aim of this third contribution is to provide a support for the transition from RBA to AA. I aim to provide means to enhance the understanding of risk scores to distinguish between different types of risks and to enable a more fine-grained reasoning about the appropriateness of authentication methods with the help of CoFrA. Figure 5.1 highlights this third contribution in the global vision of this thesis. First, I explain the idea of explainable risks. Then, I detail the methodology, together with the application case study, and I explain how the explanations of the risks can be used to differentiate between risk types (e.g., password theft, device theft) and how these explanations can enable a more fine-grained reasoning about the appropriateness of authentication methods.

Contents

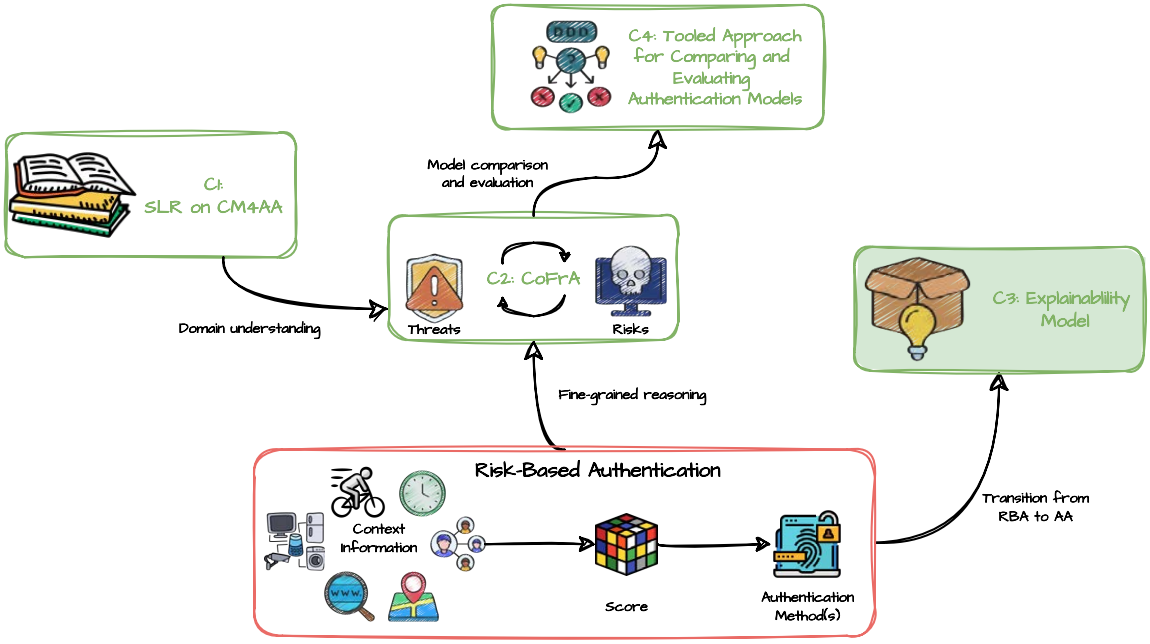

Figure 5.1 – Contribution 3: Explainability Model for Risk Scores.

5.1 Explainability of Risks

As stated earlier, RBA uses statistical models to determine the risk level associated with a user's login attempt, based on contextual features. When additional authentication methods are triggered, because the risk exceeds a certain threshold, the risk score is referred to as a **black box**, even if they do not contain any information about the context. Nevertheless, as stated earlier, there are several shortcomings of such risk-based approaches. In the last section (contribution 2), I hence presented a modeling framework that enables a more fine-grained reasoning about the appropriateness of authentication methods. Nevertheless, many organizations already have implemented RBA systems and may not be ready to transition immediately to AA. The transition to AA can be a gradual process, and legacy

RBA systems will likely be in place for some time. Hence, the aim of this third contribution is to provide a support for the transition from RBA to AA. I aim to provide means to enhance the understanding of risk scores to distinguish between different types of risks and to enable a more fine-grained reasoning about the appropriateness of authentication methods with the help of CoFrA. Therefore, I make use of explainability models for blackbox AI models to obtain explanations of estimated risk scores and use these explanations to design CoFrA models.

Explainable AI models provide details or reasons to make the functioning of AI straightforward or easy to understand. Explanations can answer different kinds of questions about *what the AI model is learning*, *which parts of the inputs are the most important for the prediction* and *can I trust the model's decision* [84]. From a mathematical viewpoint, "simple" statistical learning models, such as linear and logistic regression models, provide high **interpretability** but, possibly, limited predictive **accuracy**. On the other hand, "complex" machine learning models, such as neural networks, provide high predictive accuracy at the expense of a limited interpretability [84]. The same holds for risk scores calculated based on available contextual features during an authentication event. "Simple" statistical estimations are easy to understand, but when more "complex" models are used, it becomes hard to understand the risk prediction of an authentication event. Hence, it becomes difficult for authentication engineers to provide the appropriate authentication methods. Among other dimensions, explainability models can be distinguished according to the scope of explanations they provide. There are **global** explainability models which aim to explain the model as a whole and **local** explainability models that seek to explain individual predictions and that I propose to use to **explain the risk of a specific (individual) authentication event**. Also, we can distinguish between **model-specific** and **model-agnostic** explainability models. The latter, in contrast to the former, can be used without any knowledge about the AI model [84]. **Shapely values** provide local and model-agnostic explanations of AI algorithms by assuming that each feature is a player and the prediction is the outcome of the game [84]. The Shapley value of a feature

is the average of all its **marginal contributions** to all possible coalitions of the features [84]. Instead of how fair the distribution of a game's payout is, I want to analyze **how each contextual feature contributes to the risk score of an authentication event** that estimates the risk. I aim to answer the question of how to explain the risk of a suspicious authentication attempt. Here, the "game" is the risk score estimation. The "players" are the contextual features. They contribute to the risk score. The "gain" of one specific contextual feature is its marginal contribution to the risk score.

This contribution proposes a contextual feature engineering approach based on Shapley values. A case study on real-world authentication events shows that the risk can be explained differently and specifically for each authentication event. Hence, it shows that explainable machine learning models can effectively improve the understanding of risks. Authentication engineers can use these explanations in addition to the risk score to identify risk types and to choose the appropriate authentication methods with the help of CoFrA. Predicting when an authentication event is risky can be of use but more importantly, understanding the risk score can help to do a more fine-grained mapping of context information to authentication methods. With this contribution, I provide a framework for authentication engineers to apply the methodology of Shapley values to risky authentication events. I also propose a clustering of the explanations and a novel reasoning about risk types (authentication attacks) with the help of contextual information. The application case study shows for 30,000 real world authentication events that it is possible to explain the risk differently and specifically for each authentication event and that those explanations can help authentication engineers to reason about the appropriateness of authentication methods in a fine-grained manner.

5.2 Methodology

Figure 5.2 summarizes the methodology consisting of five steps. First, I extract the dataset of authentication events consisting of a number of

features to predict whether an authentication event is risky or not. Second, I fit a risk estimation model to the data, and then third, use the TreeSHAP method to get Shapley values for each authentication event in the test sample. Fourth, I cluster them to find patterns that can lead to better authentication decisions. Last, I reason about the obtained clusters to extract information about the risk types.

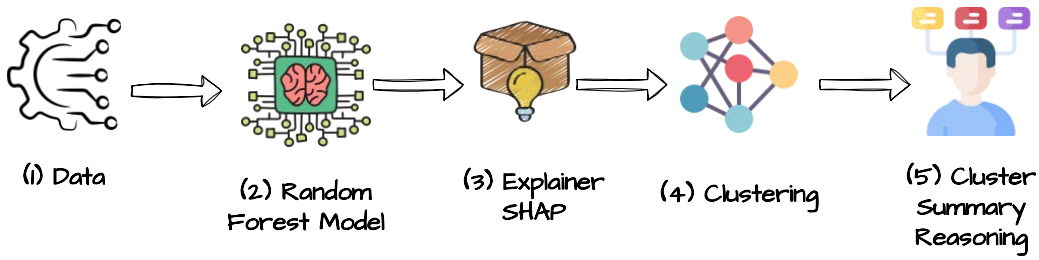

Figure 5.2 – Methodology to Identify Similar High-Risk Authentication Events through Clustering.

In this section, I detail the methodology. I first present a **statistical approach to measure risks**, which is proposed in [48]. Since RBA is not a standardized procedure, multiple solutions exist in practice. I focus on Freeman et al.'s [48] implementation, since other works showed good performance [129]. Also, this RBA model is known to be widely used, *e.g.,* by popular online services like Amazon, Google, and LinkedIn [128]. Afterwards, I explain how to exploit the explanatory context information contained in the risk score with the help of **Shapley values**. The Shapley method is **agnostic** (model neutral) applied to the predictive output, regardless of which model generated it. Hence, the method can be applied to any risk score estimation model. Also, with the Shapley method, **local explanations** can be obtained, and I can hence **explain every authentication event separately**. There are other local, model-agnostic explanation methods, *e.g., Individual Conditional Expectation* (ICE), Local Surrogate (LIME), Counterfactual Explanations and Scoped Rules (Anchors) [84].

According to [84], Shapley values might be the only method to deliver a **full explanation**, which is based on a **solid theory**. The problem of **allocating responsibility for risks** plays an important role in other domains as well (*e.g.,* in finance to evaluate the risk of an individual asset in a portfolio). I identify a set of works proposing the use of Shapley values for allocating responsibility for risks [25, 116, 17].

5.2.1 Statistical Approach to Measure Risks

Risk models are usually employed in the context of RBA to estimate the expected risk of an authentication event a of a given user $u \in U$. The most important component of a risk model is a **risk score**, which is usually estimated statistically employing context scoring models [129]. $s_a = p(X_a, u, Y_a)$ is the risk score of an authentication event a of a user u, where $X_a = (x_a^1, ..., x_a^d) \in X$ indicates a d-dimensional vector of explanatory context information characterizing an authentication event (*e.g., IP address, user agent*). $Y_a \in G, I$ is the class label of a genuine authentication event (G) or an imposter authentication event (I) and f is a classification function $f : s \rightarrow Y$.

5.2.2 Exploiting the Explanatory Context Information

I now explain **how to exploit the explanatory context information** contained in the risk score with the help of **Shapley values**. For an authentication event a, I propose to calculate the Shapley value for each contextual feature $x_a^i \in X_a = \{x_a^1, ..., x_a^d\}$ characterizing a. For each feature x_a^i, the Shapley value is defined as

$$\theta_{x_a^i}(a) = \sum_{z_a \subseteq X_a \backslash x_a^i} \frac{|z_a|!(d - |z_a| - 1)!}{d!} [p(z_a \cup x_a^i, u, Y_a) - p(z_a, u, Y_a)] \quad (5.1)$$

where p is the risk score estimation model and X_a the input vector of all d contextual features characterizing the authentication event a. $z_a \subseteq X_a \backslash x_a^i$ is a subset of X_a that does not contain the contextual feature x_a^i for which

the Shapley value is calculated. The quantity

$$[p(z_a \cup x_a^i, u, Y_a) - p(z_a, u, Y_a)] = MC_{x_a^i, z_a} \tag{5.2}$$

is the contribution of the contextual feature x_a^i to the risk estimation in the coalition $z_a \cup x_a^i$. This contribution is calculated as the difference between the risk score p estimated from $z_a \subseteq X_a \setminus x_a^i$ and p estimated from $z_a \cup x_a^i$. In Equation 5.2, I summarize the marginal contributions of x_a^i to all possible subsets $z_a \subseteq X_a \setminus x_a^i$. The fraction

$$\frac{|z_a|!(d - |z_a| - 1)!}{d!} \tag{5.3}$$

is a weighting function of $MC_{x_a^i, z_a}$. Depending on the number of contextual features in the subset z_a and the total number of contextual features d, $MC_{x_a^i, z_a}$ is weighted differently. If a contextual feature is added to an already large number of contextual features in z_a and yet the risk score is strongly influenced, then this must be weighted more than if the contextual information is added to an empty set. In the latter case, it is normal that the risk score is then strongly influenced.

Example. Let us take the example of $X_a = \{device, IP, location\}$ with $d = 3$ illustrated in Table 5.1.

z_a	$p(z_a, u, Y_a)$	$z_a \bigcup x_a$	$p(z_a \bigcup x_a^i, u, Y_a)$	$MC_{x_a^i, z_a}$	$\frac{\lvert z_a\rvert!(d-\lvert z_a\rvert-1)!}{d!}$	
{device, IP}	0.3	{device, IP, location}	0.9	0.6	0.33	0.198
{device}	0.4	{device, location}	0.7	0.3	0.33	0.051
{IP}	0.2	{IP, location}	0.6	0.4	0.33	0.034
{}	0.1	{location}	0.4	0.3	0.17	0.099

Table 5.1 – Example: Calculation of the Shapley Value.

I want to calculate the Shapley value of $x_a^{location}$. There are four subsets $z_a \subseteq X_a \setminus x_a^{location}$ (column 1). The risk score can be estimated for these four sets (column 2)and then for the union of these four sets and $x_a^{location}$ (column 4). $MC_{x_a^{location}, z_a}$ (column 5) is the difference between the estimated risk scores. Depending on the number of contextual features in

z_a, I calculate the weighting function (column 6). To obtain $\theta_{x_a^{location}}(a)$, I multiply $MC_{x_a^{location},z_a}$ with the weight (column 7) and sum up all the values: $\theta_{x_a^{location}}(a) = 0.198 + 0.051 + 0.034 + 0.099 = 0.382$. The Shapley value of $x_a^{location}$ feature is equal to 0.382. I can calculate the Shapley values for all the contextual features and compare their values to understand which contextual features contribute the most to the risk. The Shapley values can be used to indicate **which contextual features contribute more to the prediction of the risk** of an authentication event. Not only in general, as it is typically done by statistical models, but differently and specifically **for each authentication event**. As shown in Chapter 4, this information can then help to reason in a fine-grained manner about the appropriateness of authentication methods according to threats and risks.

Appropriateness of Shapley Values for Risk Attribution. Before explaining how I applied the methodology to a real-world dataset, I now explore, why the Shapley value properties (efficiency, symmetry, linearity, null-player) are **appealing in the context of risk attribution** [116]. *Efficiency* means that the sum of the Shapley values of all features equals the value of the coalition of all features, so that all the gain (risk) is distributed among the features [84]. Hence, the Shapley values reflect the risk diversification at the system level (at the authentication event level in this case). *Symmetry* means that for two equal features x_a^i and x_a^j $MC_{x_a^i,z_a} = MC_{x_a^j,z_a} \forall z_a \in X_a$ [84]. The symmetry property means that the labeling of individual components does not affect their measured contribution to system-wide risk. *Linearity* means that when two risk estimation models described by p_1 and p_2 estimate the risk, then $\theta_{(x_a^i,p_1)+(x_a^i,p_2)} = \theta_{(x_a^i,p_1)} + \theta_{(x_a^i,p_2)}$ and $\theta_{(x_a^i,p_1)*\lambda} = \lambda * \theta_{(x_a^i,p_1)}$ [84]. The linearity property is useful in contexts, where model and parameter uncertainty calls for robust estimates. Such estimates are often obtained by combining the outcomes of competing risk estimation models. The linearity property of the Shapley Value implies that a robust estimate of a contextual feature's contribution to the risk of an authentication event would be the (weighted) average of the Shapley values for this feature across different risk estimation models. A contextual

feature is a *null-player* if $p(z_a \cup x_a^i, u, Y_a) = p(z_a, u, Y_a) \forall z_a$. The Shapley value of a null-player is zero [84]. Given a player set X_a, the Shapley value is the only map from the set of all risk score estimations to risk score vectors that satisfies all four properties: **efficiency**, **symmetry**, **linearity** and **null-player**. Given the one-to-one mapping between two risk estimation models, I henceforth focus exclusively on the risk attribution problem and thus on the risk measure, s.

5.3 Application Case Study

I now present the application case study of the methodology on real-world authentication events. Within this case study I demonstrate that my proposed framework can be applied to a dataset of real-world authentication events of Orange™ and that the obtained explanations are useful for the authentication engineers to make adapted authentication decisions according to the attack types. Hence, this application case study serves as a proof of concept. Also, it guides authentication engineers from other companies in the application the framework in the same way and thus get information about attack types relevant to them.

I first describe the dataset which I used to test the model and explain the proposed method in detail. Afterwards, I present the obtained results. By describing the approach in detail, this chapter provides a framework that can be used by authentication engineers to apply the method in the same way on their data.

5.3.1 Data

I test the model to real user data supplied by Orange™ . In summary, the analysis relies on a dataset composed of contextual information on **30,000 authentication events** mostly based in France for the year 2022. The context information contains twelve categorical contextual features (see Table 5.2).

Context Information	Type	Description
changingIP	Boolean (0,1)	The IP address is known or unknown from the user's history
gatewayOwner	Boolean (0,1)	The user is or is not behind his or her own line
changingDevice	Boolean (0,1)	The device is known or unknown from the user's history
internISP	Boolean (0,1)	The *Internet Service Provider* (ISP) is or is not the telecommunication company
app	Category (#38)	The accessed resource (*e.g.,* Mail)
fastLocationChange	Boolean (0,1)	Successive connections from two countries in a short time or not
authenticationMethod	Category (#3)	The used authentication method (*e.g.,* password)
country	Category (#136)	The country that the authentication attempt originates from
robot	Boolean (0,1)	Regularity of successive connections is or is not detected
changingSim	Boolean (0,1)	The SIM card has been changed or not
knownUser	Boolean (0,1)	The user is known (has been previously seen) or is connecting for the first time
changingLocation	Boolean (0,1)	The location is known or unknown from the user's history

Table 5.2 – Description of the Used Contextual Features.

5.3.2 Method

Based on [48], I have constructed a statistical estimation of the risk. For every authentication event, I calculate the logarithmic probability that it is a legitimate event and an imposter event. The actual **risk score** describes the difference between these two log probabilities.

$$s_a = log(p(X_a, u, I)) - log(p(X_a, u, G)) \tag{5.4}$$

I choose a threshold λ for the risk score to label the events as **genuine and imposter events**.

First, I calculate some basic **descriptive statistics** to summarize the central tendencies, and to analyze how the values of the contextual features are spread off.

Then, I split the authentication event data between a **training set**

(80%) and a test set (20%), using random sampling without replacement. I then get 24,000 training samples and 6,000 test samples.

On these samples, I run a **Logic Regression**, a **Random Forest Classifier**, a **Decision Tree Classifier**, and a ***Support Vector Machines* (SVC) Classifier**. To obtain Y_a, the estimated risk probability is classified into "genuine" (G) or "imposter" (I), depending on whether the threshold is passed or not. For a given threshold T, one can then count the frequency of the **possible outputs**: *False Positives* (FP): authentication events predicted to imposter, that are genuine; *False Negatives* (FN): authentication events predicted to genuine, which are imposter; *True Positives* (TP): authentication events predicted as imposter, which are imposter; *True Negatives* (TN): authentication events predicted as genuine, which are genuine. The **misclassification rate** of a model can be calculated as

$$\frac{FP + FN}{TP + TN + FP + FN} \tag{5.5}$$

and it characterizes the proportion of wrong predictions among the total number of predictions. FPR and *True Positive Rate* (TPR) are then calculated as follows:

$$\frac{FP}{FP + TN} \tag{5.6}$$

$$\frac{TP}{TP + FN} \tag{5.7}$$

Further, this study analyzes the ***Receiver Operating Characteristic* (ROC) curves** of the four classifiers. They plot the FPR on the Y axis against the TPR on the X axis for a range of threshold values. The ideal ROC curve coincides with the Y axis, a situation which cannot be realistically achieved. The best model will be the one closest to it. The ROC curve is usually summarized with the *Area Under The Curve* (AUC), a number between 0 and 1. The higher the AUC, the better the model. Next, I calculate the **Shapley value explanations** of the authentication event logs in the test set, using the values of their explanatory contextual features. In particular, I use the **Tree*SHapley Additive exPlanations***

(SHAP) method in combination with Random Forest. Tree SHAP is a fast and exact method to estimate Shapley values for tree models and ensembles of trees [84]. I calculate the local Shapley values for the 6,000 authentication events of the test sample. I get 6,000 arrays consisting of two sub-arrays. In the first sub-array, I get the Shapley values for the first class (**imposter authentication events**). In the second sub-array, I get the Shapley values for the second class (**genuine authentication events**). The last part of the analysis involves using the Shapley value vectors that correspond to each authentication event, and look for the presence of **clustering structures** that group together **similar risky authentication events**. To this aim, I employ a **K-means** clustering algorithm [1]. I cluster the Shapley values calculated for the authentication events of the test sample to find patterns that can lead to appropriate authentication methods. I am using the elbow method [2] to decide how many clusters are a good fit for the data. Next, I fit the K-Means model to the Shapley values for the test sample with four as the number of clusters. I then map for each authentication event (data point) which cluster was assigned to it based on its training and look for the presence of clustering structures that group together similar authentication events.

5.3.3 Results

Figure 5.3 displays exemplary the distribution of the “changingIP" feature regarding the risk score. I observe that the medium risk score is higher if the “changingIP" feature takes the value 1 (unknown IP) than if the value is 0 (known IP).

Figure 5.4 shows that all classifiers outperform the SVC classifier. Indeed the comparison of the **Area Under the ROC curve (AUC)** for the four classifiers indicates an increase from 0.90 (SVC) to 0.94 (Random Forest, Decision Tree). For further analysis I choose the **Random Forest**

1. A method of vector quantization that aims to partition n observations into k clusters in which each observation belongs to the cluster with the nearest mean

2. Heuristic used in determining the number of clusters in a data set consisting of plotting the explained variation as a function of the number of clusters, and picking the elbow of the curve as the number of clusters to use

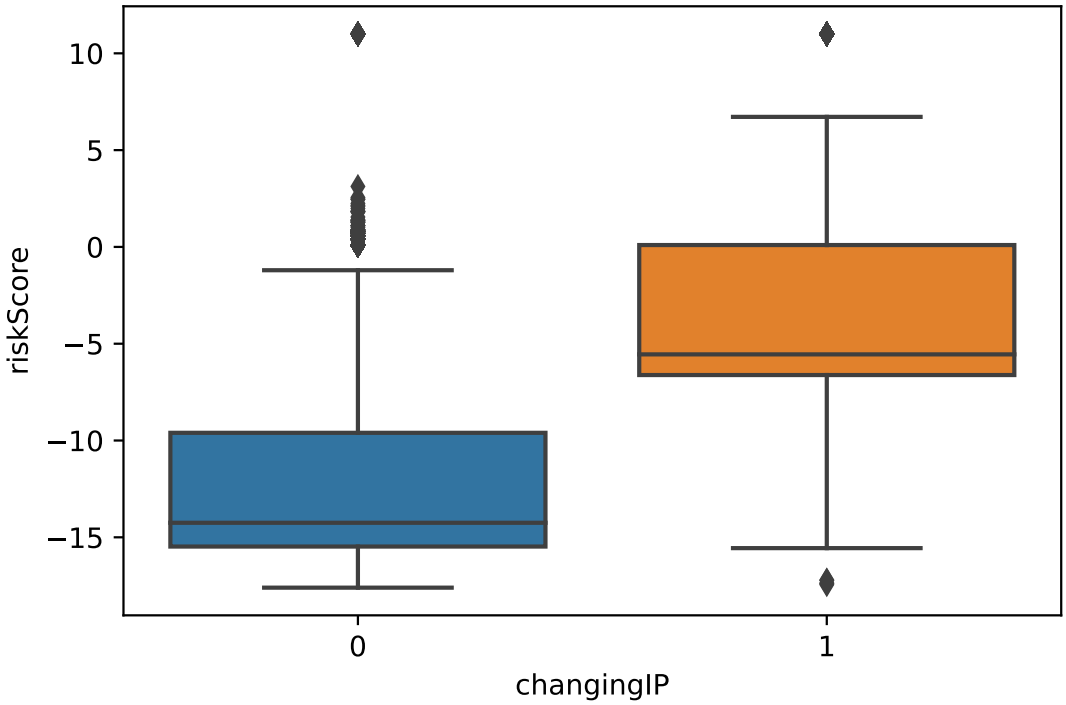

Figure 5.3 – Boxplot Displaying the Distribution of the "changingIP" Feature Regarding the Risk Score.

Classifier because it outperforms the Decision Tree Classifier in terms of accuracy (92.1 versus 90.8).

For single authentication events, I can visualize the explanations as illustrated in Figure 5.5 for an imposter authentication event. Features that **push the risk score higher** (to the right) are shown in red, and those **pushing the prediction lower** are in blue. The **output value** is the prediction for that authentication event (0.92). The **base value** is the value that would be predicted if I did not know any features for the current authentication event. In other words, it is the mean risk prediction. The base value is 0.1843. This is because the mean of the risk scores in the test sample is 0.1843. In the exemplary authentication event at risk (see Figure 5.5), the contextual features that drive the score up the most are *changingDevice*, *changingIP* and *gatewayOwner*.

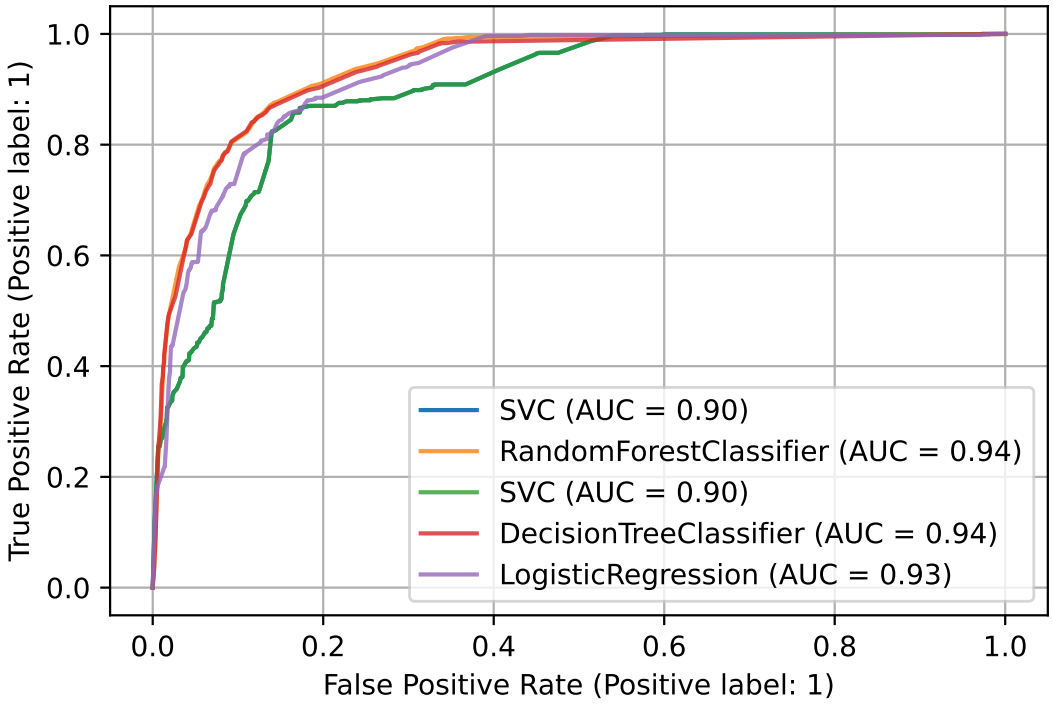

Figure 5.4 – Receiver Operating Characteristic (ROC) curves for the Logic Regression, the Random Forest Classifier, the Decision Tree Classifier, and the SVC Classifier.

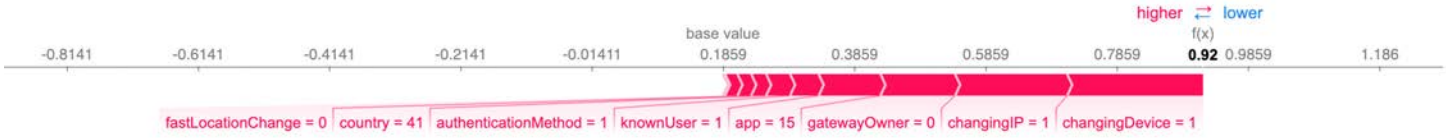

Figure 5.5 – Local Explanations of an Authentication Event at Risk.

Rather than referring to the risk score as a black box to choose the appropriate authentication method(s) for a high-risk authentication event, the **explanations** can be used. These explain the contextual background of the risk, which is necessary to reason on the appropriateness of authentication methods.

According to the elbow method, I choose 4 as number of clusters for the k-means clustering (Figure 5.6). In Figure 5.7, I plot the scatterplot of

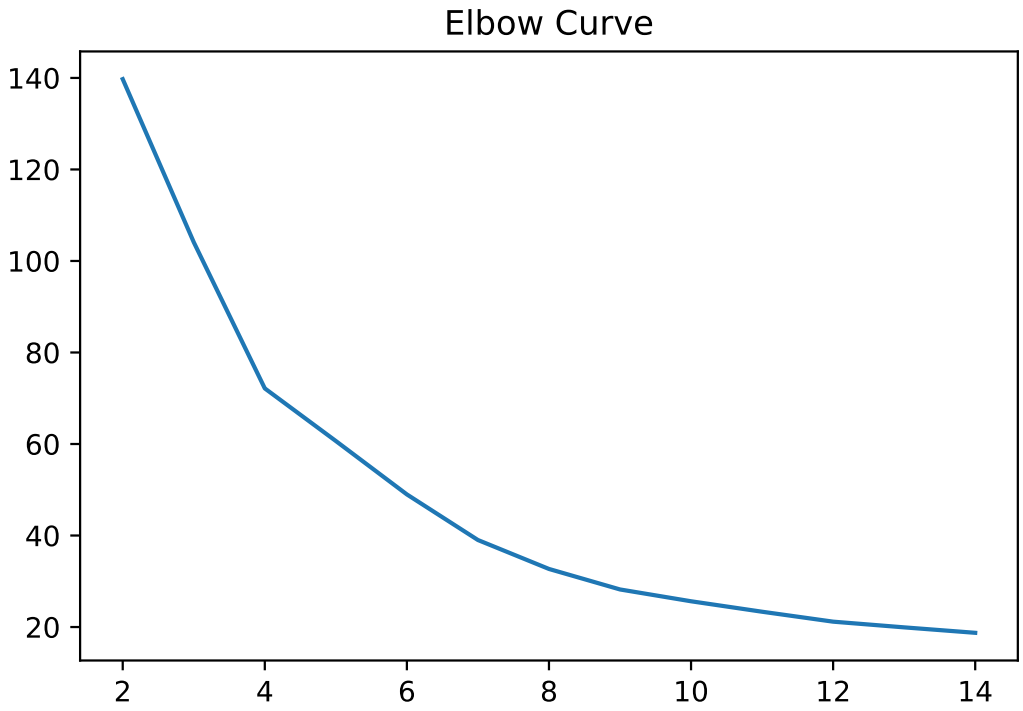

Figure 5.6 – Elbow Curve to Choose the Right Number of Clusters (4).

the first two principal components of the Shapley values, attributing each authentication event to one of the four clusters. The obtained clusters are clearly differentiated and balanced, confirming the advantage of using the proposed method. Furthermore, I take a closer look at the authentication events of the four clusters. For most of the authentication events which have been assigned to **cluster 0** the user is not behind his or her own line and the

ISP is not the telecommunication company. For most of the authentication events which have been assigned to **cluster 1**, the IP address is unknown and the device is unknown. For most of the authentication events which have been assigned to **cluster 2**, the IP address and the geolocation are unknown. For most of the authentication events which have been assigned to **cluster 3**, the user is connecting for the first time. I can see, that the different cluster represent different contextual situations.

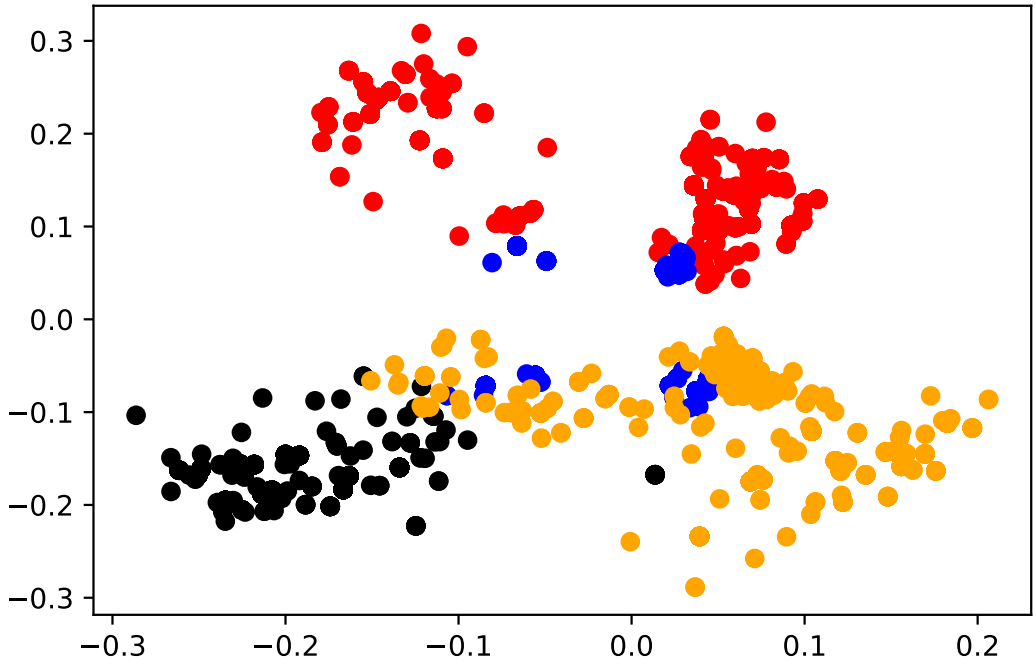

Figure 5.7 – Scatterplot of the First Two Principal Components of the Shapley Values.

5.4 Using Explanations to Differentiate Between Different Risk-Based Authenticatioon Attack Types

The contextual explanations of the risk can help authentication engineers to understand the suspiciousness of a high-risk authentication event in terms of the type of risk (attack type), which is behind the risk. Hence,

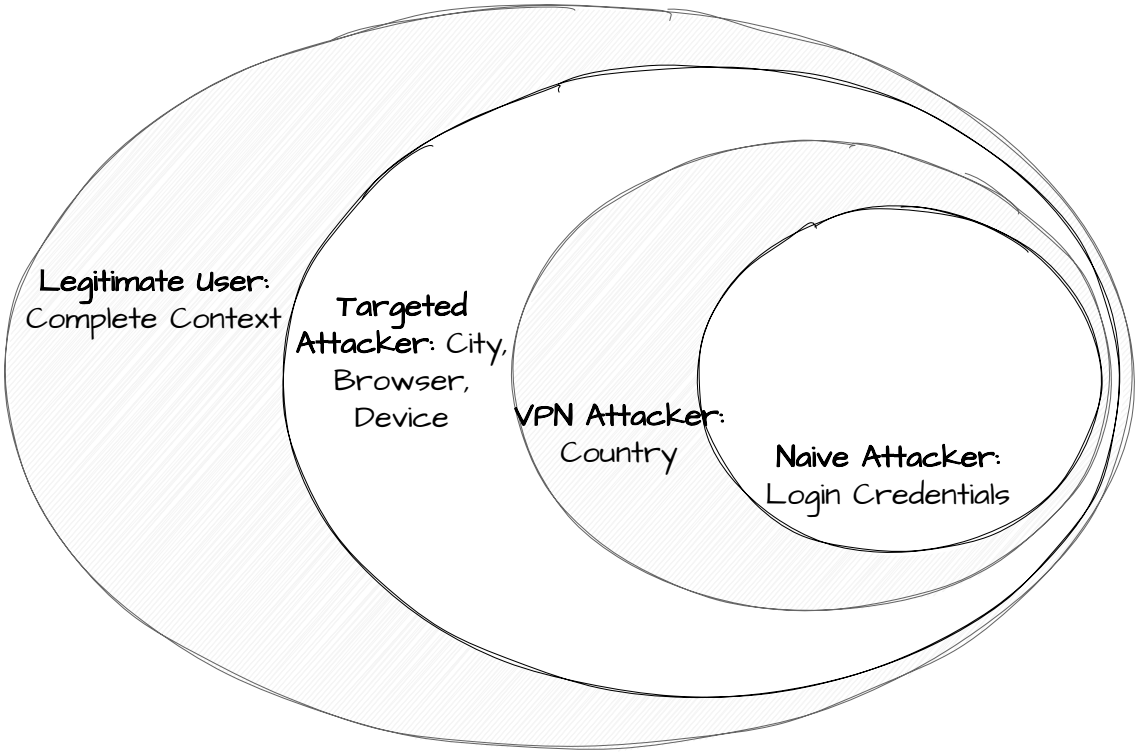

Figure 5.8 – Overview of the Attack Types that Can be Distinguished based on Contextual Explanations of the Risk Score [127].

they can choose authentication methods that are appropriate for the attack type with the help of CoFrA. I take three **attack types** based on known ones in the RBA context presented in [127]. All attackers possess the victim's login credentials, none of the attackers possesses the complete context of the legitimate user (see Figure 5.8).

Wiefling et al. [127] describe the attack types. I here analyze them further regarding six exemplary contextual features. I can see in Table 5.3 that the values that the contextual features take depend on the attack type. This illustrates that contextual explanations of the risk score can help to choose an authentication method that is appropriate for the attack type. Common risk factors of the attack types (*e.g., fastLocationChange*) are evident from the explanations but not from a risk score itself.

Contextual Feature	Naive Attacker	VPN Attacker	Targeted Attacker
IP address	Randomly located	Victim's country	Victim's city
Browser	Random popular browser	Random popular Browser	The victim's browser
Device	Random popular device	Random popular Device	The victim's device
Keystrokes	Unknown	Unknown	Unknown
ChangingLocation	1	1	0
FastLocationChange	1	0	0

Table 5.3 – Contextual Characterization of RBA Attack Models.

Figure 5.9 shows how the Shapley values in Figure 5.5 can be used to create a CoFrA model. I observed that the high risk in this example is manly driven by the features "changingDevice", "changingIP", and "gatewayHolder", "app", "knownuser", 'authenticationMethod", "country", and "fastLocationChange" also play a role. In the corresponding CoFrA model this translates into four threat situations ('changingDevice", "changingIP", "knownUser_notBehindBox", "mediumLocationChangeSpeed"). After the identification of the threat situations, context-threat-algorithms need to be identified and defined allowing to detect the threats from required context information. Then, a threat-risk-algorithm needs to be defined which classifies the threats according to risk types. Here, I classified the threats into the risk type "StolenPassword". Last, the authentication methods to be used need to be identified. I assume in this example that mobile-based authentication can be used, as the risk concerns the knowledge factor and not the possession factor. A biometric authentication method can also be applied here. This is an example how the Shapley values can be used to create a CoFrA model. I do not claim to propose the perfect model here. The aim of this example is to show how the explanations can be used by experts to identify threats and classify risks and choose the appropriate authentication methods.

5.5 Summary

In order to improve the understanding of risks, and to allow a fine-grained mapping of context information and authentication methods, I

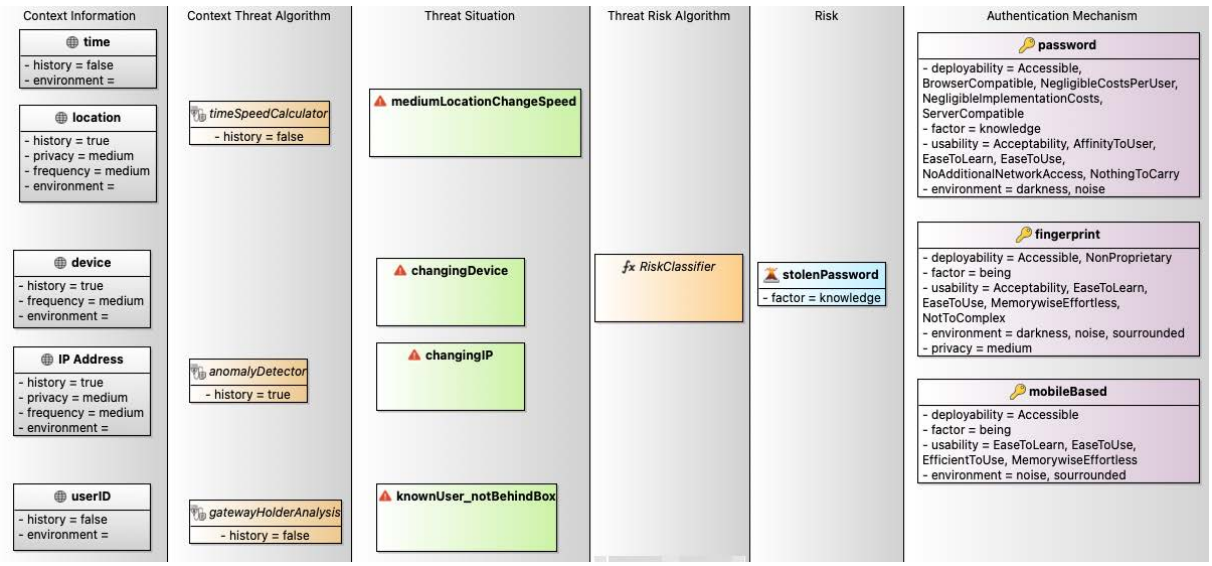

Figure 5.9 – Exemplary Use of the Shapley Values from Fig. 5.5 to Build a CoFrA Model.

propose a novel methodology that can be embedded within an authentication service. Authentication services which are currently based on RBA approaches can use the proposed methodology to reason about types of risks behind the score and create a CoFrA model. Hence, this methodology supports the transition from RBA to AA. The methodology, which is based on a model agnostic interpretability tool (Shapley Values), leads to a powerful segmentation of authentication events. A case study shows that the approach brings several advantages and, in particular, the ability to perform segmentation that is based on the risk similarity between authentication events. A case study on 30,000 real world authentication events shows that risky and non-risky events can be grouped according to similar contextual features, which can explain the risk differently and specifically

for each authentication event. This research suggests that explainable machine learning models can effectively improve our understanding of risks and can enhance the usage of CoFrA. This work shows that a reasoning about risk types (authentication attacks) with the help of contextual information is possible and can help to choose the appropriate authentication methods in case of a high risk. However, the identified explanations (Shapley values) are not sufficient for this purpose. It is necessary that they are efficiently used with the help of CoFrA.

Chapter 6

Tooled Approach for the Definition of the Most Well-Suited Authentication Models

This chapter presents the fourth contribution of this thesis, the tooled approach for the definition of the most well-suited authentication model for a given system. While CoFrA defines the valid structure of an AA model, this contribution allows to compare and evaluate authentication models (e.g., CoFrA models, RBA models). Figure 6.1 highlights this fourth contribution in the global vision of this thesis. First, I recall the need to evaluate and compare authentication models. Second, I detail the main concepts of the approach. Third, I explain the usage of the approach over the whole life-cycle of the authentication system. Last, I present the evaluation of the approach.

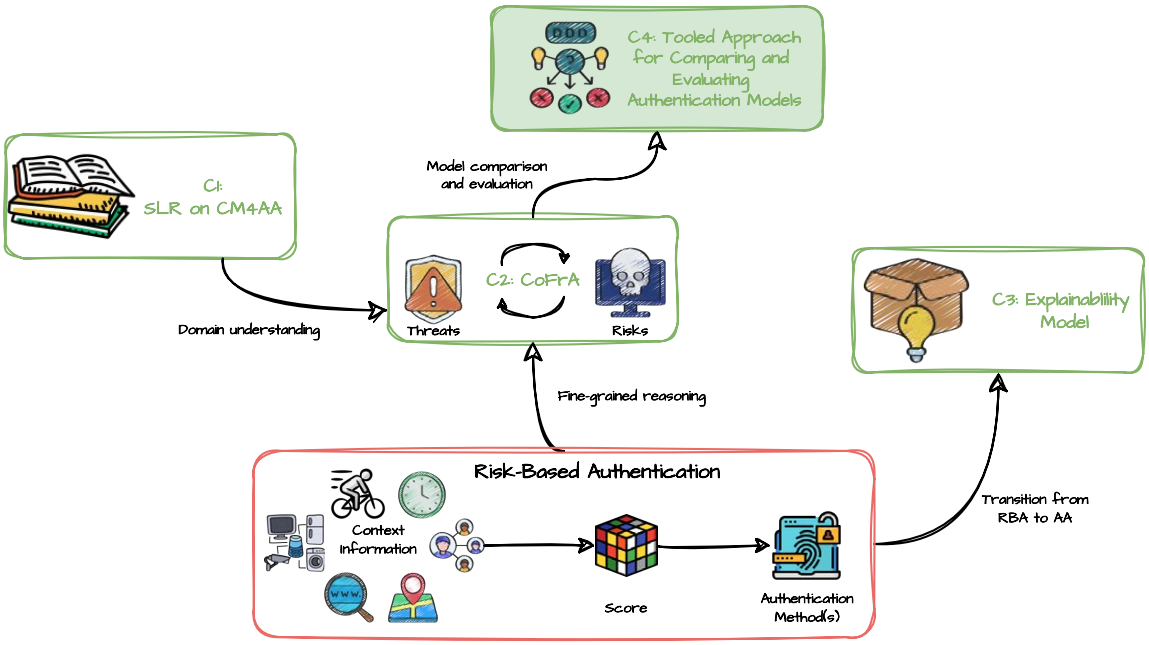

Figure 6.1 – Contribution 4: Approach for Comparing and Evaluating Authentication Models.

Contents

6.1 Need to Evaluate and Compare Authentication Models

The CoFrA metamodel defines the structure and constraints of a statically valid Adaptive Authentication (AA) Model. CoFrA is the first language that sets an approach for creating AA models. Advances in prediction techniques and sensing open up numerous alternative approaches for AA [135]. Hence, for a given system, different valid instances of CoFrA exist (metamodel-model relationship introduced in Section 2.2). Evaluating and comparing different models are crucial to determine which model best fits the needs of a particular authentication system and its stakeholders. Also, comparing CoFrA models with other authentication models (e.g., RBA models basic password-authentication models) is important to define the most well-suited authentication model for a give system. Authentication models need to be tailored carefully to each online service, as even

small configuration adjustments can significantly impact security and usability [127]. It is hence essential to have a way to compare and evaluate different adaptive authentication models based on multiple criteria (e.g., security, usability, deployability, privacy). These evaluation criteria may sometimes conflict, involve various stakeholders with different interests, and may change over time. Current evaluation approaches for authentication solutions mostly focus on the evaluation of individual authentication methods. Nevertheless, a holistic view of the user's path is essential when evaluating the performance of the overall authentication model, rather than just considering individual authentication methods in isolation. To assess not only individual methods, but authentication models that dynamically select methods in the user paths, more research is needed. This assessment requires considering the dynamic nature of the user's context and interactions between multiple authentication methods. Evaluation metrics must account for changes in the user's context and their impact on the appropriateness of authentication methods used.

In this chapter, I present an extensible tooled [1] approach for the definition of the most well-suited authentication models for a given system. I aim to guide the evaluation and comparing process of authentication models on user paths to select and tailor models for specific systems. I create an approach to not only compare individual authentication methods but to evaluate authentication models on user paths and hence in concrete contexts. Also, I am the first to propose a multi-dimensional (security, usability, deployability, privacy) trade-off analysis between different quality criteria instead of a one-dimensional evaluation metric. The approach proposes a framework to apply an authentication model on a user path and to evaluate its performance. In this way, multiple authentication models can be compared to define the most well-suited model for a given system.

The novel contributions of the approach compared to the state-of-the-art on evaluating authentication solutions are the following:

— First, I propose a **conceptual model** to apply authentication models on user paths.

1. A tool prototype is proposed to help using the approach.

— I formalize a **user path** as a sequence of successive authentication events [2].
— I formalize the interpretation process of an authentication model on a user path: the **authentication model** takes as input a user path and gives a sequence of successive predictions of authentication methods, *i.e.,* an authentication path.
— I formalize an **authentication path** as a sequence of successive authentication events each associated with an authentication method.

— Second, I propose a **customizable trade-off analysis of the quality criteria** of an authentication model together with a **standard library of well-known quality criteria** proposed in the literature to date.

I evaluate the contributions with a set of authentication models based on real-world use cases and cases from the literature. This allows to analyze the approach's **feasibility**, **time and structural simplicity**, **usefulness**, and **effect**. I conclude that all the authentication models can be interpreted and evaluated with the help of the approach which covers all domain concepts and provides clear evaluation results (feasibility). The authentication engineers appreciate the decision support in comparing authentication models and consider the approach as useful in conceptualizing and comparing authentication models. They confirm the time and structural simplicity and the effect of the approach.

The remaining of this chapter is organized as follows. The approach, its concepts, and relationships are presented in Section 6.2. In Section 6.3, I explain the usage of the approach during the entire life-cycle of an authentication system. The validation is described in Section 6.4. I summarize the contribution in Section 6.5.

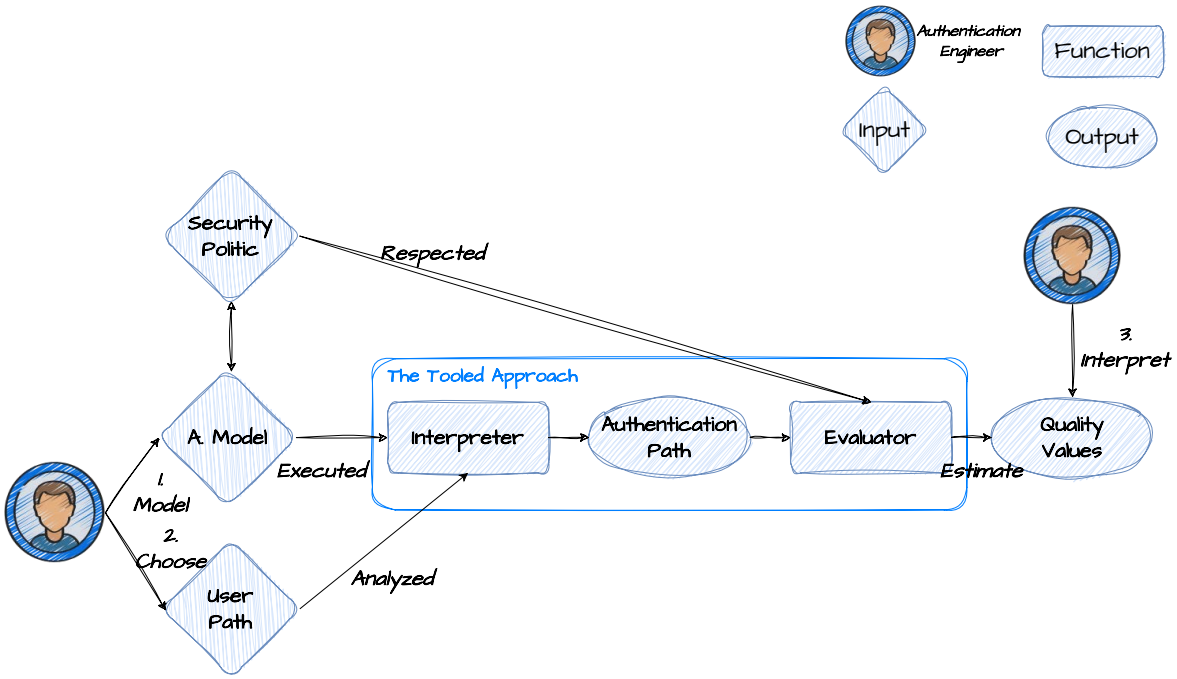

Figure 6.2 – The Approach.

6.2 Main Concepts of the Approach

Figure 6.2 shows the proposed **approach** for the definition of the most well-suited authentication models for a given system. It consists of two main functions: the **interpreter** and the **evaluator**. The **interpreter** can interpret authentication models on a **user path** returning an **authentication path**. The **evaluator** estimates **quality values** reflecting the quality of the authentication model with respect to the **security politic**, a set of rules and information to consider when evaluating an authentication model. I introduce each of the approach's components in the following.

6.2.1 User Path

I define a **user path** as a sequence of successive authentication events. I define an **authentication event** as an access attempt of a user to a

2. I define an authentication event as an access attempt of a user to a resource that takes place in a specific context and time (Chapter 2).

resource that takes place in a specific context and time. I use $y = (t, r, C)$ to denote an authentication event where $t \in T$ is its time, $r \in R$ the resource and C a n-tuple of context information: $C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$.

For example, an authentication event's context C can contain information about the location, the IP address, the browser, the battery status, the light, and the device of the user [8]:

$$y = (07h13, mail, C = \begin{bmatrix} location : work \\ IP : 123.456.789.101 \\ device : smartphone \\ browser + version : Safari\_v4 \\ battery : high \\ light : bright \end{bmatrix}).$$

Wiefling et al. [131] published login feature data of over 33 million access attempts and over 3.3 million users on a large-scale online service in Norway. [3] The data was collected between February 2020 and February 2021. I collected the user paths with a significant number of login attempts. Also, I simulated specific user paths where the login attempts come from different well-known types of attackers: naive attackers, targeted attackers, very targeted attackers, and VPN attackers [131]. This provides an extensive library of user paths on which authentication models can be evaluated and compared. [4]

6.2.2 Authentication Model

An **Authentication model** M suggests using no, one, or multiple authentication methods for each authentication event in a user path. The structure of an authentication model is specified by CoFrA. In summary, the model M consists of multiple functions (algorithms): one to determine

3. https://zenodo.org/record/6782156

4. The totality of user paths is available on my companion website (https://github.com/BumillerAnne/CoFrA-Studio/tree/main/UserPaths).

threat situations from the context (*e.g.,* a derivation from the user's habits), one which is identifying the risk type behind the threat (*e.g.,* a password theft or a device theft) and one to map the risk type and the adapted authentication method (*e.g.,* in the risk of a stolen password, no password authentication should be asked.). When an authentication model is applied on a user path, it gives successive predictions of authentication methods for each event in the user path. For each event, the authentication model requires inputs that indicate the adapted authentication method, called event indicators, that is a subset $S \subseteq C$ ($M(S) = [\text{“}methods\text{”}]$).

6.2.3 Security Politic

The **security politic** is a file consisting of rules and information to consider when evaluating an authentication model. I stated earlier that in the literature to date, individual authentication methods have been evaluated according to different criteria. I propose a security politic file that is based on these evaluations. In the literature, I identified four required concerns: *security*, *usability*, *deployability*, and *privacy*. I hence, propose a security politic based on these four concerns.

I propose a security matrix (m × s) containing the information on whether the m authentication methods (a_1, ...,a_m) provide the s security properties (sb_1, ...,sb_s) given in the literature to date:

$S=$

$$\begin{array}{c} \begin{array}{ccccc} a_1 & a_2 & a_3 & \dots & a_m \end{array} \\ \begin{pmatrix} ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... \end{pmatrix} \end{array} \begin{array}{l} sb_1 \\ sb_2 \\ sb_3 \\ \\ sb_s \end{array}$$

In the same way, I propose a usability matrix (m × u) containing the information on whether the m authentication methods provide the u usability properties (ub_1, ...,ub_u); a deployability matrix ($m \times d$), containing the information on whether the m authentication methods provide the d

deployability properties (db_1, ..., db_d); and a privacy matrix ($m \times p$), containing the information on whether the m authentication methods provide the p privacy properties (pb_1, ...,pb_p).

Users of the approach can customize the security politic by adding or removing some of the criteria depending on their individual needs. Therefore they can use standard library introduced in Chapter 4 and detailed in Chapter 7 which provides a set of common values. Based on the criteria in the standard library, I report on the evaluation of a large set of authentication methods based on existing evaluatiins in the literature (0: property not respected, 0.5: property partially respected, 1: property respected). For example, for the usability criteria ‘**“memory-wise effortless”**, I evaluated the following authentication methods as follows [5]:

— “mobileConnect”: 1,
— “app_OTP”: 0.5
— “sms_OTP”: 0.5,
— ‘backupEmail_OTP”: 0.5
— “backupNumberSMS_OTP”: 0.5
— “password”: 0
— “security_question”: 0
— “knownPhoneNumber”: 0,
— “known_email”: 0,
— “lastLoginLocation”: 0,
— “accountCreationDate”: 0,
— “printedBackupCode”: 0.5,
— “securityKey”: 0, “federatedSSO”: 0,
— “fingerprint”: 1,
— “face”: 1,
— “CAPTCHA”: 1,
— “OTP_anyPhone”: 0.5,
— “OTP_anyEmail”: 0.5

Although the focus of this contribution is not on the content of the secu-

5. The values for other criteria are available on my companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/blob/main/security_politics.json).

rity politic, this evaluation is an essential aid for authentication engineers. Furthermore, the security politic remains extendable and the users of the approach can adapt the security politic to their individual concerns and requirements.

6.2.4 Interpreter

I propose an **interpreter** I able to interpret heterogeneous authentication models implemented by the user of the approach while respecting the specifications or this approach. The interpreter can analyze and execute the program of the authentication model M on an input user path P. That means that for each event in P, M predicts a set of authentication methods ($M(S) = [\text{“}methods\text{”}]$). For the whole user path, we hence obtain a sequence of suggested authentication methods: $I : (M, U) - > [[\text{“}methods\text{”}], [\text{“}methods\text{”}], ..., [\text{“}methods\text{”}]]$.

6.2.5 Authentication Path

An **authentication path** A is a sequence of suggested authentication methods (*e.g.,* [[“ ”], [“password”, “SMS_OTP”], [“fingerprint”]])

6.2.6 Evaluator

The **evaluator** E is the function that evaluates authentication models. The function takes the predicted authentication path as input and gives quality values for each defined evaluation criteria (*e.g.,* security, usability, deployability, privacy): $E(A) = [\text{“}se\_value\text{”}, \text{“}us\_value\text{”}, \text{“}de\_value\text{”}, \text{“}pr\_value\text{”}]$. I propose a standard interface of the *Evaluator* describing multiple evaluation metrics for the criteria security, usability, deployability and privacy, and for which an implementation is available to the user of the approach in Python code. Hence, the user can implement other evaluation metrics that conform to the specifications. I further explain the implementation of the evaluator function in Chapter 7.

6.2.7 Quality Values

With the help of the approach, an authentication model can be evaluated according to multi-criteria optimizations of the required concerns as identified in the literature review and interviews with authentication engineers: security, usability, deployability, and privacy (Chapter 2)

— Quality of Security (QoS)
— Quality of Usability (QoU)
— Quality of Deployability (QoD)
— Quality of Privacy (QoP)

For each criterion, I provide standard methods to derive the quality values based on the security politic. For example, one method counts each criterion's desired properties and computes the authentication path's mean, maximum, and minimum values. For the usability criteria, another standard method is to calculate the number of login attempts and the proportion of those that require authentication (*number authentications/ number of login attempts*). Also, the number of required authentications in a time window (*e.g.,* during one day) can be interesting.

Once the approach (described in Figure 6.2) is fixed, the authentication engineer can choose an authentication model to be evaluated on a user path and with respect to a security politic. To compare two authentication models, the authentication engineer only varies the authentication model and evaluates it on the same user path and with respect to the same security politic. Figure 6.3 illustrates the evaluation of two authentication models (two *simulations*) with the help of the approach. The interpreter and the evaluation functions are specified and fixed. A user path has been chosen. The only varying input is the model. The approach is then applied to the two models and quality values are determined for each of them. An authentication engineer can then use these values to compare, select and tailor the models for a given system.

It may be interesting to develop an automated evaluation pipeline to test multiple authentication models by systematically applying the evaluation approach to each model. After evaluating all the models, the pipeline

could rank them based on their quality values. The authentication engineer can set a threshold or weighting of criteria to automatically select the best-performing models. While automation can streamline the evaluation process, it's essential to be cautious about fully replacing the human aspect for selecting high-quality models. The aim of the evaluation approach presented in this thesis to facilitate the discussion and exchange of evaluation metrics and results among stakeholders. By adopting a manual evaluation process, I aim to involve human experts in the decision-making process to ensure a comprehensive understanding of the authentication models' performance.

6.3 Usage of the Approach

Evaluating the quality of authentication models remains an issue over the entire life-cycle of the authentication system (Planning & Analysis, Design, Implementation, Maintenance (Figure 6.4)). With the approach, I would like to enable both tailoring and selecting of authentication models. By tailoring, I mean editing a model to be suitable for a particular system. By selecting, I mean choosing the most well-suited model from a set of models. In the following, I detail how authentication models can be selected and tailored with the help of the approach during the different life-cycle stages of the authentication system.

Planning and Analysis. In this first phase, engineers can use the standard library to get a comprehensive picture of the state of the art in evaluating authentication models. Then, a reconciliation of objectives must occur, whereby the authentication engineer's objectives are matched with the standard library. The standard library can be adapted and extended by the authentication engineer (*e.g.,* adding new authentication methods, extension by a quality criterion). The metrics for determining the quality values can also be adapted and extended at this stage.

Design. During the design phase, different model variations can be tried out, and quality checks carried out. This phase is the heart of the tailoring process. The authentication engineer can test different designs for quality. For example, he can run tests with different authentication methods and test the models against different types of user paths. At the end of this phase, the authentication engineer selects the tailored model for the implementation. As mentioned before, an amortisation of this task may be interesting.

Implementation. During the implementation stage of the authentication system based on the selected and tailored authentication model, additional needs may arise that require the design to be reconsidered (*e.g.,* non-availability of some context information at runtime). Then, the authentication engineer can take a step back in the design process and test whether the limited version of the model still meets the quality requirements.

Maintenance. As long as the authentication system is in use, it must be maintained. Therefore, engineers should carry out regular quality checks with the approach (*e.g.,* check whether quality thresholds are still fulfilled). In this way, the system can be continuously monitored, and compliance with quality restrictions can be ensured.

6.4 Evaluation of the Approach

This section evaluates the approach's **feasibility** (ability to compare authentication models), **temporal and structural complexity** (time required, the rigor and the complexity of the evaluation), **usefulness** (helpfulness for authentication engineers), and **effect** (influence on authentication engineers). I first formulate the research questions, and then present the protocol and datatset before I discuss the results.

6.4.1 Research Questions

I formulate the following research questions:

RQ1 With the approach, can an authentication engineer compare different authentication models according to multiple criteria? This aims to investigate the **feasibility** of the approach.

RQ2 With the approach, can the **temporal and structural complexity** of evaluating and comparing authentication models according to multiple criteria be reduced? This aims to estimate the time required, the rigor and the complexity of the manual evaluation process, to assess the difficulties faced by authentication engineers, and to provide insight into the challenges of manual evaluation.

RQ3 To what extent is the approach helpful for authentication engineers? This aims to assess the approach's **usefulness**.

RQ4 To what extent does the use of the approach influence authentication engineers when comparing authentication models? This aims to determine the **effect** of the approach and whether authentication engineers behave differently when evaluation guidance is available and when it is not.

6.4.2 Evaluation Protocol and Dataset

The evaluation of the approach consists of two parts.

First, I assess the feasibility (RQ1) of the approach on six authentication models based on real-world use cases and use cases from the literature.

Second, I further assess the approach with the **survey and interview method**. Hereby I answer RQ2 (**temporal and structural simplicity**), RQ3 (**usefulness**), and RQ4 (**effect**).

6.4.2.1 Case Study Method: RQ1 - Feasibility

The approach aims to provide constructs to evaluate and compare authentication models. To validate the relevance of the abstraction provided, I propose to discuss the approach's ability to handle concrete example models correctly and evaluate them clearly (**feasibility**).

Table 6.1 – Example Models.

Authentication Model	Prediction Parameters	Authentication methods
Anomaly Detection Model	Location, device	Password/ SMS OTP/ both
IP History Model	IP address	Face recognition/ SMS OTP/ password
Robot Suspected Model	Time	CAPTCHA
Fast Location Change Model	Location, time	Email OTP, password, security question
Risk Score Model	Risk score	Fingerprint, app OTP, password
Session Based Model	Time	Password

I therefore created six authentication models based on use cases from the literature, and real-world use cases (Table 6.1). I evaluate and compare them with the approach.

Below, I will explain the real-world use cases and the literature-based use cases on which the example models are founded.

Real-world Use Cases. Some of the authentication models are inspired by a company's project towards user notifications (IAlerting). The project's origins come from the need to notify the user in the case of changes in the device or the country. The notifications are created based on successful access attempts containing the context information date (time), the IP address (country), and the user agent (device). Based on this information, threat situations and risks are predicted (new IP address, new location, new device, fast location change, and robot suspicion).

Use Cases From the Literature. Some of the authentication models are inspired by an approach from Freeman et al. [48]. It is an RBA approach, which is a statistical prediction to measure risks. I selected this approach from the literature since other works showed good performance [129]. Also, this RBA approach is known to be widely used, *e.g.,* by popular online services like Amazon, Google, and LinkedIn [128, 129].

In Subsection 6.4.3, I discuss each of the six models that I created based on these cases in detail.

6.4.2.2 Survey and Interview Method: RQ2, RQ3, RQ4 - Temporal and Structural Complexity, Usefulness, Effect

Objectives. I aim to study the temporal and structural complexity of the approach. Therefore, this study analyzes the time required, the complexity, and the rigor of an evaluation guided by the approach compared to a manual evaluation of authentication models (RQ2). Also, this study analyzes the usefulness of the approach (RQ3) and the effect on the authentication engineers' behavior (RQ4). Therefore, I design an authentication engineer survey. [6]

Experiment Design. The panel consists of eleven authentication engineers working on identity management, authentication, and system security. They come from different departments of a multinational telecommunications corporation (Orange™) and have all at least five years of experience in the domain. I targeted people who deal with authentication in everyday life. However, it is not possible to identify and survey this entire population. Hence, I have chosen engineers from my professional network. All of them are authentication engineers, and therefore, potential users of the approach. Table 6.2 shows the job titles of the authentication engineers.

I contacted the authentication engineers and did a one-hour face-to-face meeting with each of them. In the first stage, I presented two authentication models (Solution A, Solution B) to the authentication engineer. [7] Solution A is inspired by the current approach of many online services where only the duration of the session is taken into account to decide about the authentication method(s) to require. After a certain time, the user session expires and the user gets re-authenticated. Solution B takes into account different context information to calculate a confidence level (RBA inspired).

Then, the authentication engineers answered eleven questions during

6. The totality of the questions and anonymous answers are available on my companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/tree/main/ExpertSurvey).

7. The descriptions of the two solutions are available on my companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/tree/main/ExpertSurvey).

Table 6.2 – Job Titles of the Experts Participating in the Evaluation Survey of the Approach for the Definition of the Most Well-Suited Authentication Models for a Given System.

	Job Title
Auth. Eng. 1	Project Manager: Identity Anticipation and Research
Auth. Eng. 2	Identity Domain Architect
Auth. Eng. 3	Direction of the IT Services and Access Management Program
Auth. Eng. 4	Project Manager: Access Management Solutions
Auth. Eng. 5	System Architect for Digital Identity
Auth. Eng. 6	Functional Architect (Digital Identity)
Auth. Eng. 7	Architect for Projects for Identity Anticipation and Research
Auth. Eng. 8	Head Of Identity and Access Management for Users
Auth. Eng. 9	Cloud and Security Architect
Auth. Eng. 10	Data Security Manager
Auth. Eng. 11	Authentication Product Owner

the interview. [8] I discuss the questions and answers concerning RQ2, RQ3 and RQ4 in Subsection 6.4.3.

6.4.3 Results

In this section, I present the result of (1) the case study, and (2) the survey and interview method.

6.4.3.1 Case Study Method: RQ1 - Feasibility

The **Anomaly Detection Model** (Figure 6.5 [9]) is a model inspired by IAlerting. The location and the device are context features typically used for AA [8], and it is prevalent to use anomaly detection algorithms for the prediction. So, in the anomaly detection model, I predict the authentication method(s) based on two parameters, the location and the device. If the user's location is unusual, then she needs to authenticate with a password;

8. The questions are available on my companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/tree/main/ExpertSurvey).

9. Graphical representations of all other example use cases are available on my companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/tree/main/ExampleAAModelCases).

if the device is unusual for the user, then she needs to authenticate with an SMS OTP; if the device and the location are unknown; then she needs to authenticate with a password and SMS OTP. I also evaluate this model with a variation where I use app OTP instead of SMS OTP. With such an example, an engineer can check the differences between using two authentication methods in terms of usability, security, privacy, and deployability.

The **IP history model** is a model inspired by IAlerting. The IP address is also a frequently used parameter to predict authentication methods [8]. So in this model, I use the IP address. If the IP address has never been seen in the user's history before she gets authenticated with face recognition; if the IP address has not been seen during the last twenty logins, then the user gets authenticated with SMS OTP. Otherwise, she gets authenticated with a password.

The **robot suspected model** is inspired by IAlerting. Robot patterns are predicted with the help of the time of the access attempt. If the variance of the time difference between successive access attempts is equal or close to zero, then a robot is suspected to be behind the access attempt. A CAPTCHA is then required as an authentication method.

The **fast location change model**, inspired by a real-world authentication system (IAlerting), calculates the user's speed with the help of the time and space difference between successive access attempts. When the location change is very speedy, the user is authenticated with email OTP; if it is speedy with a password, and if the speed is average, then she is asked a security question.

The **risk score model** is based on Freeman et al.'s [48] statistical approach to measure the risk, and depending on the risk value, the user gets authenticated with fingerprint in case of high risk, with app OTP in case of medium risk and password in case of low risk.

The **session-based model** is a standard model still often used by online services. Based on the time, the model decides whether the session is expired (*e.g.,* after 15 minutes, after one hour, after six months). If the session expires, the user is authenticated with a password. An engineer can compare different variations of this model with the help of the approach

(*e.g.,* different time thresholds, different authentication methods).

I was able to interpret and evaluate all the models with the help of the approach. I hence conclude that the approach covers all domain concepts (sufficiency) without specifying unnecessary, too many details (necessity), and provides clear evaluation results, highlighting the **feasibility** of the approach. [10] I am intentionally not presenting the results of the evaluation here. I will introduce in Chapter 7 an example of evaluation results to explain how they can be used and interpreted by authentication engineers. The focus of this contribution is on the methodology. I do not make any claims about the exclusiveness of these evaluation metrics used but present a methodology that can be adapted by authentication engineers. Accordingly, the actual results of the evaluation are not relevant here.

6.4.3.2 Survey and Interview Method: RQ2, RQ3, RQ4 - Temporal and Structural Complexity, Usefulness, Effect

RQ2 - Temporal and Structural Complexity. With the help of the authentication engineer survey, I estimate the time required, the complexity, and the rigor of a manual evaluation of two authentication models without the guidance of the approach. More precisely, I estimate the time required, the complexity and the rigor of four tasks:

— Making a global comparison of two authentication models,
— Defining desirable criteria for the evaluation,
— Formalizing desirable criteria, and
— Making a criteria-specific comparison of two authentication models.

The first task is for the engineers to decide which of the two presented authentication models, A or B, is better. I measure the time the authentication engineers take to make their decisions. On average, the authentication engineers took 43 seconds to choose A or B. I observe significant time differences between the authentication engineers. Some decide in less than ten seconds, while others need more than two minutes. Accordingly, the **global evaluation** of two simple models can already take a long time

10. All implementations are available on a companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/tree/main/AAModelImplementations).

and, moreover, the time differences show that the experts have different decision-making processes. Models A and B are simple examples where differences are clear. As the models become more complex and difficult to distinguish, such an assessment can become even more time consuming.

In the second question, I asked the authentication engineers why they preferred this solution and according to which criteria they did compare the solutions. Hence, this task concerns the definition of desirable criteria to evaluate authentication systems. On average, the authentication engineers took 96 seconds to **define the desirable criteria**. They all took a minimum of 37 seconds and a maximum of 169 seconds. I present here the list of the criteria mentioned by the engineers:

— *"simplicity of the authentication method"*
— *"familiarity of the user with the authentication method"*
— *"number of different authentication methods"*
— *"number of authentications in a path"*
— *"availability of the authentication methods"*
— *"universality of the authentication methods (adapted to ecosystem)"*
— *"sensitivity of the service"*
— *"implementation costs"*
— *"durability of the authentication methods"*
— *"environment aspects"*
— *"battery usage"*
— *"quality of support for the use of the authentication method"*
— *"time performance"*
— *"maintainability"*

This list is a relevant complement to the standard library of quality values obtained from the literature. The heterogeneity of the mentioned criteria also points out to the usefullness of the extensibility of the approach.

Afterwards, I ask the authentication engineers which solution is better in terms of usability, security, privacy, and deployability. I measure the time needed to decide on each criterion. On average, the authentication engineers took 99 seconds, which indicates the average time it takes to make a **criteria-specific comparison of two systems**. As for the global

evaluation, the time required varies from expert to expert pointing out the need for systematization of the evaluation process.

I present to the authentication engineers an example authentication path and ask them to describe the security and usability of this path (*e.g., number of authentications, appropriateness of the authentication methods*).[11] I measure the time it takes the authentication engineers to describe the security and usability of the example path and take this as an indicator of the time to **formalize desirable criteria**. On average, the authentication engineers took 147 seconds to describe what security and usability means. All authentication engineers took more than one minute. I observe significant differences in the description of the authentication engineers. This indicates a lack of rigor in the manual evaluation without the guidance and formalization of the approach.

I ask the authentication engineers to which extent they find it challenging to compare the two solutions A and B and why (from 1 being not challenging at all to 5 very challenging). On average, they found it difficult (4). The fact that authentication engineers find it challenging to carry out such an evaluation is an essential indication of the complexity of a manual evaluation of authentication models without the guidance of the approach.

RQ3 - Usefulness. The fact that authentication engineers find it difficult (4) to compare solutions is an essential indication that authentication engineers need **guidance to define the most well-suited authentication models**. I ask the authentication engineers to what extent they agree that usability, security, privacy, and deployability are crucial for evaluating the systems (from 1 being not crucial at all to 5 very crucial). On average, all criteria are considered at least 4. This underlines the meaningfulness of the approach and the importance of the proposed **standard library** of quality criteria. I observe differences in the pondering of the importance of the four criteria. For example, some authentication engineers find security more important than usability, and others, vice versa. This means that it is

11. I describe the path on my companion webpage (https://github.com/BumillerAnne/CoFrA-Studio/blob/main/ExpertSurvey, in the PDF).

beneficial to give the authentication engineers the possibility to **formalize their own weighted trade-off**. I also ask the authentication engineers which other criteria they consider essential for evaluating the systems. The fact that other aspects are considered necessary by the authentication engineers means that the **extensibility** of the approach is important.

After the tasks described in the previous paragraphs, I show the authentication engineers the approach. Then, I explain to them the main functionality and do a demonstration on the models they were asked to evaluate manually before (Solution A and Solution B). I ask the authentication engineers whether such an automated evaluation process is helpful and why. The authentication engineers highlight, in particular, the usefulness of the decision support to compare authentication models. The authentication engineers all say that they like the variety of indicators. They think that the approach can support the discussion between stakeholders with heterogeneous interests and can be used to convince them. This points out the advantage of the proposal compared to proposals that calculate one-dimensional quality metrics for individual authentication methods. The authentication engineers find it helpful that changing criteria can be considered. Some mention that they like the scientific standard library of desired criteria. According to the authentication engineers, the approach can help to conceptualize authentication systems and to compare already established systems.

RQ4 - Effect. This study analyzes the influence of the guidance in evaluating authentication systems on authentication engineers. The discussion of the effect is important in the context of this work, because I do not propose a one-dimensional quality value. Hence, the user cannot only choose the model with the highest quality value, but needs to take the approach as a decision support for a multi-criteria quality analysis. I ask the authentication engineers whether such an automated evaluation would influence their decisions regarding integrating new authentication solutions and how. All authentication engineers think that the approach would influence their decision. However, most authentication engineers mention that the approach

can be one of many decision bases. That is why this semi-atomized approach is a good way to provide automated decision support while still considering the human factor.

With the authentication engineers survey, I estimate the temporal and structural complexity, and rigor of manual evaluation of two authentication models without the guidance of the approach. The tasks include making a global comparison, defining desirable criteria, formalizing desirable criteria, and making a criteria-specific comparison. The results show that making a global decision between two models and making criteria-specific decisions can be very time consuming for experts even for the simple models A and B. The authentication engineers find it challenging to carry out such evaluations without guidance, with an average difficulty score of 4. The authentication engineers agree that usability, security, privacy, and deployability are crucial criteria for evaluating systems and consider these criteria important, with some prioritizing security over usability and vice versa. The authentication engineers also find the approach useful and helpful, proposing a variety of quality indicators, extensibility, and individual optimization capabilities. They appreciate the decision support in comparing authentication models and consider the approach useful in conceptualizing authentication systems.

6.4.4 Automated Comparison With the Approach

I will not make a direct comparison of the time required for manual evaluation and an evaluation with the tool supported approach. Such a comparison would be error-prone because there are many factors that may vary (*e.g.,* whether the user is already familiarized with the tool, whether the authentication models are already implemented). Instead, I discuss here in general terms the time performance, the complexity and the rigour of an automated evaluation with the approach. I have shown in Subsection 6.4.3 that comparing and evaluating authentication systems manually is even for authentication engineers a time-consuming and complex task. The analysis of the interviews shows that there is often a lack of rigour

in manual evaluation. Authentication engineers mix different criteria and weight the criteria differently along the evaluation process. The approach provides important guidance towards a less time-consuming, less complex and more rigorous evaluation. Nevertheless, the process as a whole must be considered. Authentication engineers must first familiarize themselves with the approach. If authentication engineers want to implement new models and use different evaluation methods, this is also a further time-consuming task. With the guidance of the approach, however, the authentication engineers are well supported and once they have implemented their model, they can quickly and practically use the evaluation over the entire life cycle of the authentication system.

6.5 Summary

This contribution aims to cover an existing gap in the literature: the lack of a method for comparing and evaluating authentication models according to multiple quality criteria. I propose an approach to realize this, which covers the shortcomings of existing works based on the evaluation of individual authentication methods. Both the knowledge from literature and the experience from industry were gathered through this work to learn the needs of both sides and obtain an added value to the proposals given by this contribution. The approach's feasibility is ascertained through six case studies. The main contribution is creating an extensible approach for the definition of the most well-suited authentication models for a given system based on the academy and the industry, which allows authentication engineers to choose and evaluate the model during the entire life-cycle of the authentication system.

The four contributions of this thesis thus produce the overall vision of this thesis. To use the context information efficiently and to reason on the appropriateness of authentication methods beyond risks scores, I made efforts to find out which models are suitable for the field of context modeling for AA with the help of the structured review of the literature (Chapter 3). I propose the first modeling framework CoFrA for AA which enables

complex mappings between context information, risks, and authentication methods (Chapter 4). I propose a support for a smooth transition from RBA to AA with the help of an explainability model allowing organizations to gradually incorporate AA solutions. I propose a way to compare and evaluate authentication systems, to be able to determine which systems perform better than others under different conditions and which models are more suitable for specific systems (Chapter 6). This research hence helps designing, evaluating, and comparing authentication models and supports the transition from RBA to AA.

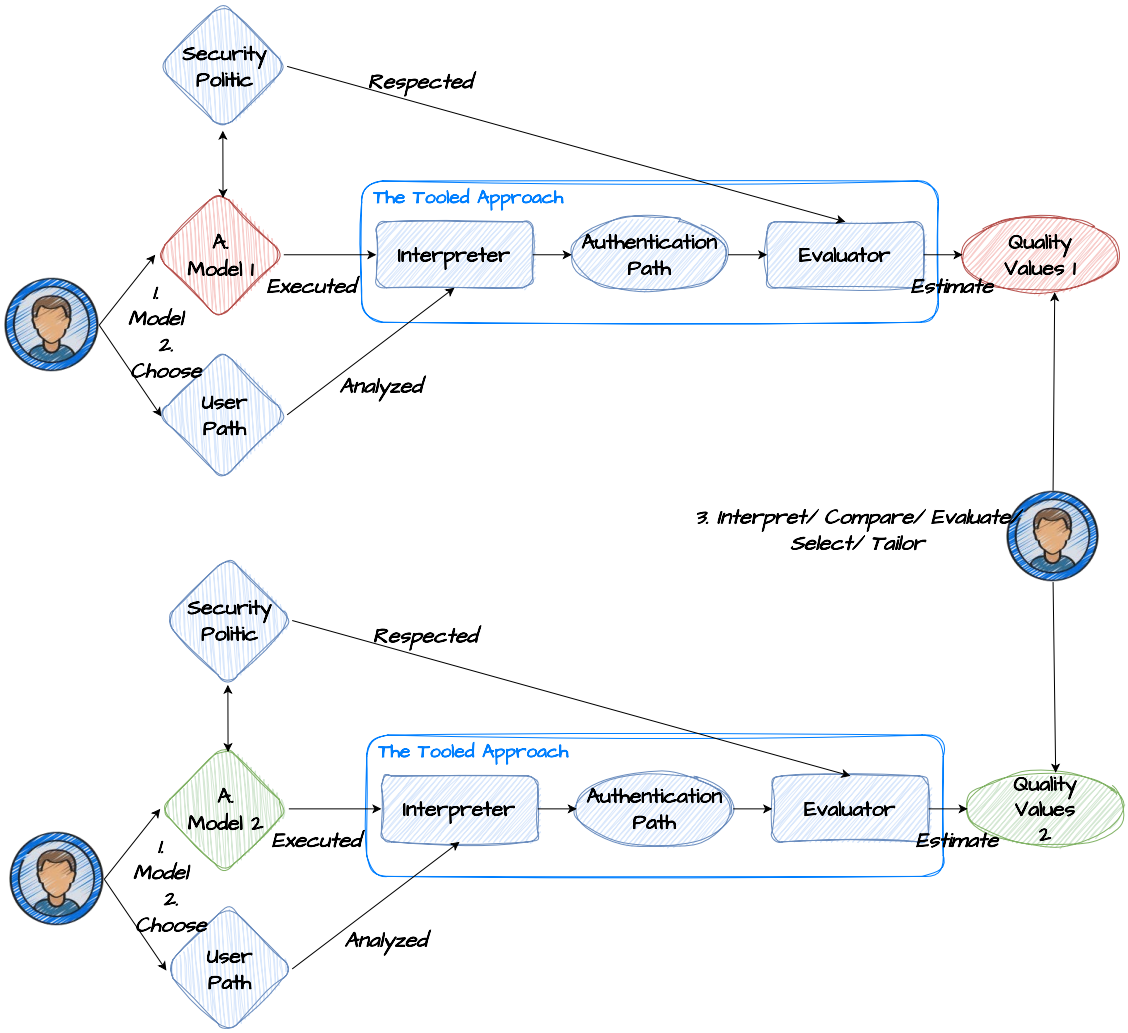

Figure 6.3 – Approach for Comparing Two AA Models.

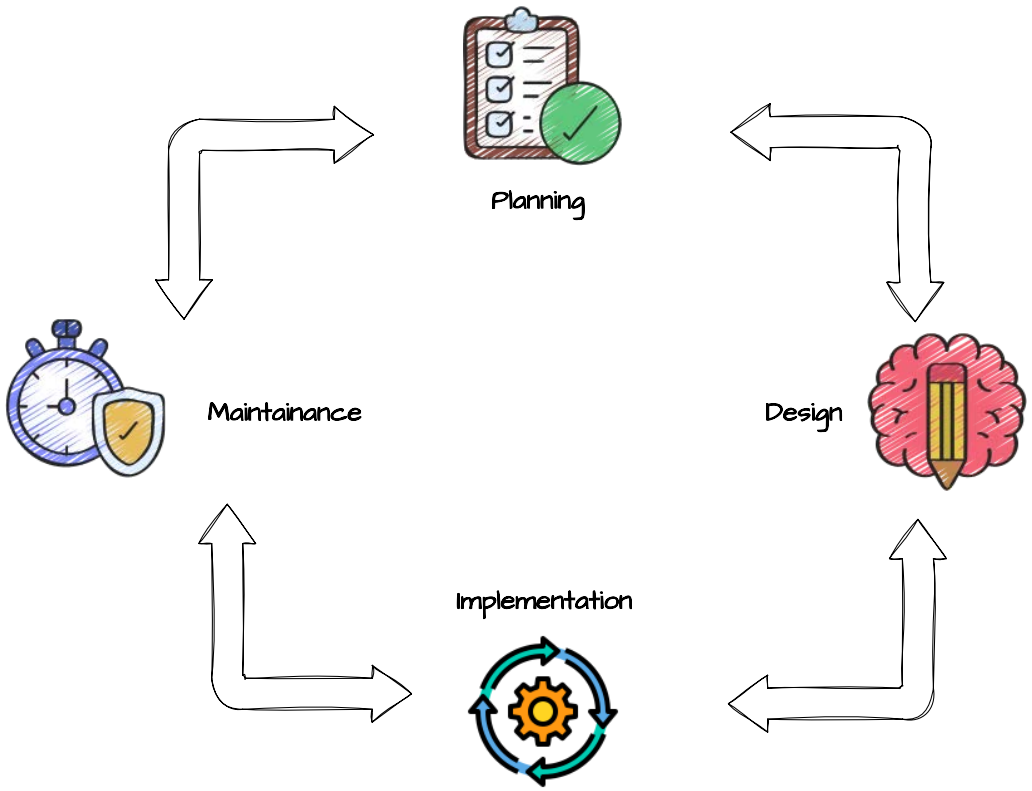

Figure 6.4 – Usage of the Approach Over the Entire Life-cycle of the Authentication System.

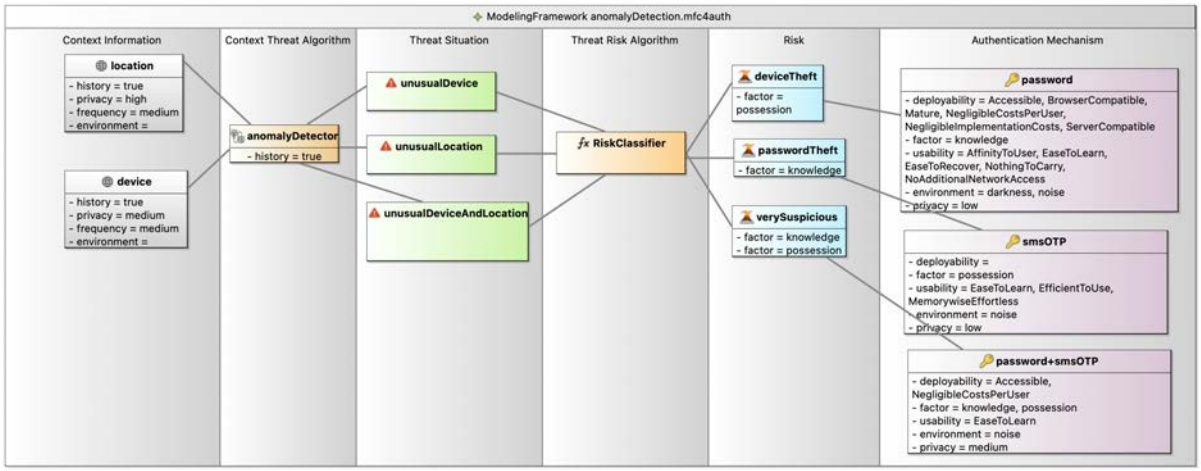

Figure 6.5 – Anomaly Detection Model.

Chapter 7

Implementation in Industrial Setting and Software Prototypes

This chapter presents the implementation of my research work in the industrial setting of Orange™ and the provided software prototypes. The aim is to outline the technology transfers to integrate the ideas from this thesis into the Orange™ authentication setting. I first present the authentication environment of Orange™ France. I explain how I improved their existing Risk-Based Authentication implementation and how I implemented an Adaptive Authentication (AA) model based on CoFrA. I also outline implementation challenges. Then, I introduce the provided prototypes which help to further support the implementation of the ideas defended in this thesis.

Contents

The work presented in this thesis builds on the needs expressed within the identity and trust research project of Orange™ to meet the requirements for AA. Working with Orange™ also provides the perfect environment to implement the approaches proposed in this thesis in order to couple existing authentication solutions with smarter and context-aware functionalities. The technology transfers presented in this chapter are the

result of a strong desire to integrate the ideas from this thesis into the Orange™ authentication setting. This work could not have taken place without the support of the project engineers. It is also the result of the technological efforts made by a trainee to propose prototypes to support our reflections. I would particularly like to acknowledge the work of:

— Didier Vojtisek, Benoit Hérard, and Erwan Diverrez for their prototype developments,
— Nicolas Aillery for his expertise in the domain and his support,
— and Ryan Yue Chun for his reflections and implementations during his internship.

7.1 The Authentication Environment of Orange™ France

Similar to many organizations, Orange™ France has already implemented a RBA model named *IAlerting*. The transition to AA is a gradual process. Hence, I first contributed to enhancing the risk estimation models for the current RBA implementation, which involved using advanced statistical approaches from the state of the art to estimate impersonation risks and detect anomalies in authentication attempts (Subsection 7.1.1). Then, I used the explainability model (Chapter 5) to help the transition to AA. This led to the implementation of an AA algorithm, the *Authentication Selector*, which is a valid CoFrA model (Subsection 7.1.2).

7.1.1 Enhancement of the Current Risk-Based Authentication Implementation

The *IAlerting* system is a RBA system which monitors contextual features during password entry such as device or geolocation information, and notifies the user if a certain risk level is detected.

Figure 7.1 shows the architecture of the IAlerting system, used in addition to password-based authentication. The system logs contextual features for each successful login attempt and compares them to the previously observed feature values (Login History). The user gets notified if the login

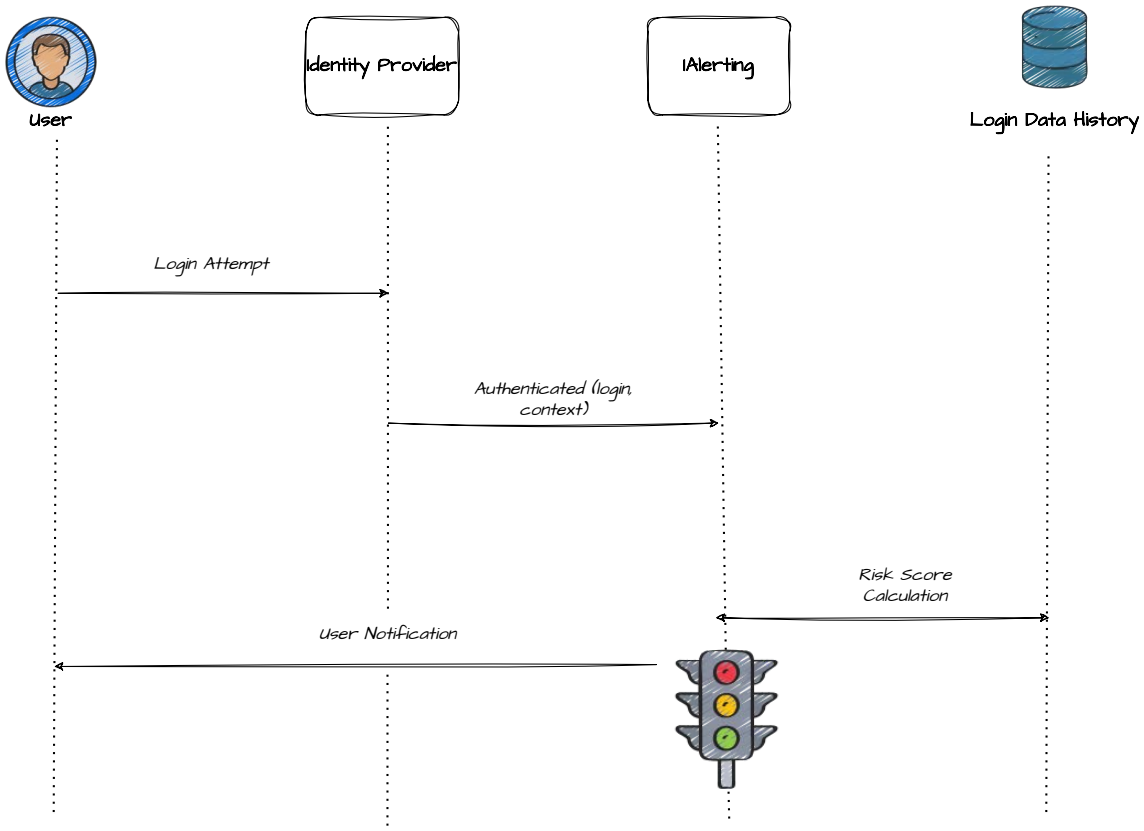

Figure 7.1 – Overview of the IAlerting System.

context is too different from the previously observed ones (*e.g.*, via an email informing about a suspicious account activity). This comparison of the current login context with a recorded history of login contexts is done by calculating a risk score. The score is a number indicating the deviation from the expected values.

IAlerting makes use of statistical models to determine the risk level associated with a user's login attempt, based on domain rules. The need for more sophisticated statistical approaches arises from the need to improve the accuracy of the risk assessment and anomaly detection. In the literature, I identified advanced statistical approaches that can be used for RBA to estimate the risk beyond domain rules (*e.g.*, [113, 122, 3]). Based on these works, I helped upgrading the current RBA implementation with enhanced state-of-the art statistical methods. For coding the algorithms

I used Python. Kafka is used to send and receive messages. It ensures that authentication events are processed in real-time. For the storage of user authentication data, such as user credentials, access tokens, and login information, Cassandra and MongoDB are used.

7.1.2 Proposal of an Adaptive Authentication Implementation

To go beyond RBA and to further integrate an AA component in the Orange™ authentication setting, I introduced the *Authentication Selector* approach. It dynamically adjusts the authentication method(s) required based on the current context and risk factors. It is build based on CoFrA. The *Authentication Selector* evaluates the contextual information to determine the risk type and hence, to determine the appropriate authentication method(s).

Figure 7.2 shows the architecture of the *Authentication Selector* system. If *IAlerting* detects a certain risk level, the user not only gets notified, but *IAlerting* sends the login and the corresponding context to the *Authentication Selector*. The *Authentication Selector* then compares the current risk level with the target level requested by the service and proposes the appropriate authentication methods for achieving the target level based on a CoFrA model. This architecture hence incorporates both, a score based approach (IAlerting) triggering the need for choosing an appropriate authentication method and an AA approach to reason on the appropriateness of the different authentication methods. The *Authentication Selector* could also be a stand alone solution and determine the appropriate authentication methods required for each login attempt and not only if *IAlerting* detects a suspicious attempt. While this implementation integrates the *IAlerting* risk assessment with the *Authentication Selector*, it is possible to expand the *Authentication Selector*'s functionality to independently determine authentication methods at each login attempt.

Figure 7.3 visualizes the transition process from (1) *IAlerting* to (2) the enhanced version of IAlerting, and to (3) the *Authentication Selector*, the first AA implementation. The basic *IAlerting* system (1) calculates the risk

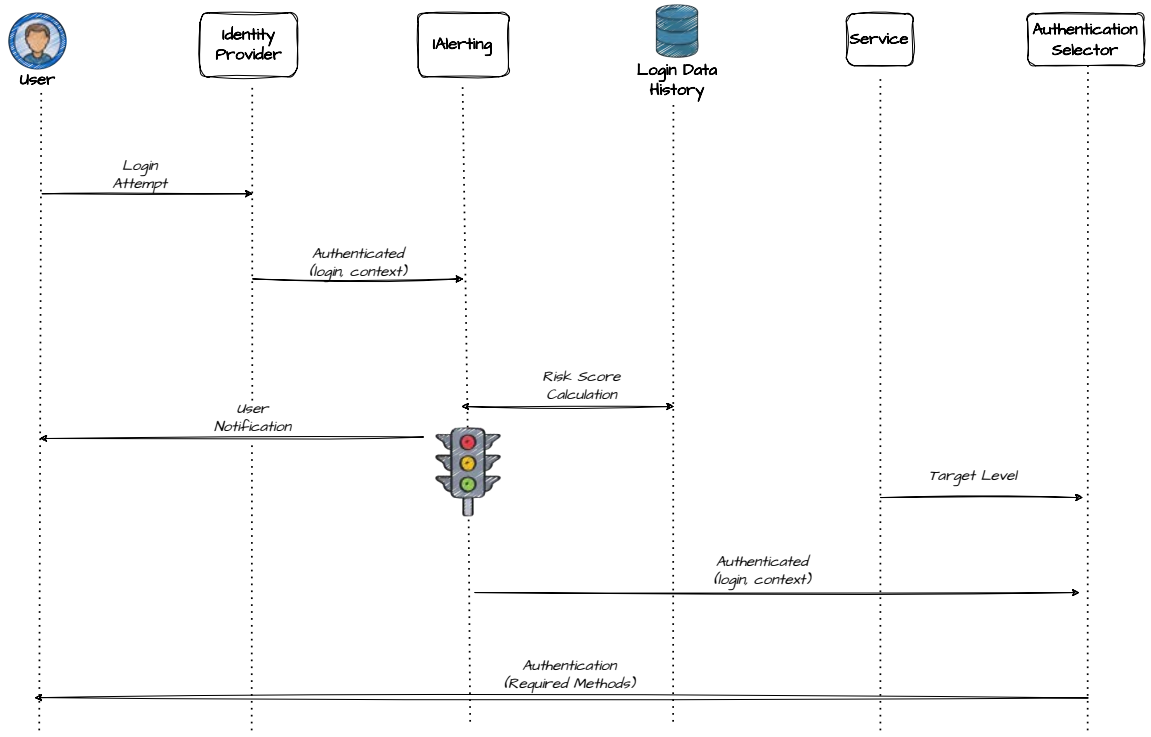

Figure 7.2 – Overview of the Authentication Selector System.

score based on simple statistical methods and domain rules. The enhanced *IAlerting* system (2) calculates the risk score based on enhanced state-of-the-art statistical methods. The *Authentication Selector* (3) proposes not only a risk score, but also the appropriate authentication methods.

Starting with this basic version of AA, the prototypes I describe in the following help to further improve and advance the implementation of AA.

7.1.3 Architectural Integration of Adaptive Authentication

The authentication system architecture is not the primary focus of my work. Nevertheless, I want to ensure that the solutions proposed in this thesis are aligned with existing industry practices and that AA can be integrated with existing systems. Hence, I outline, in this section, the ba-

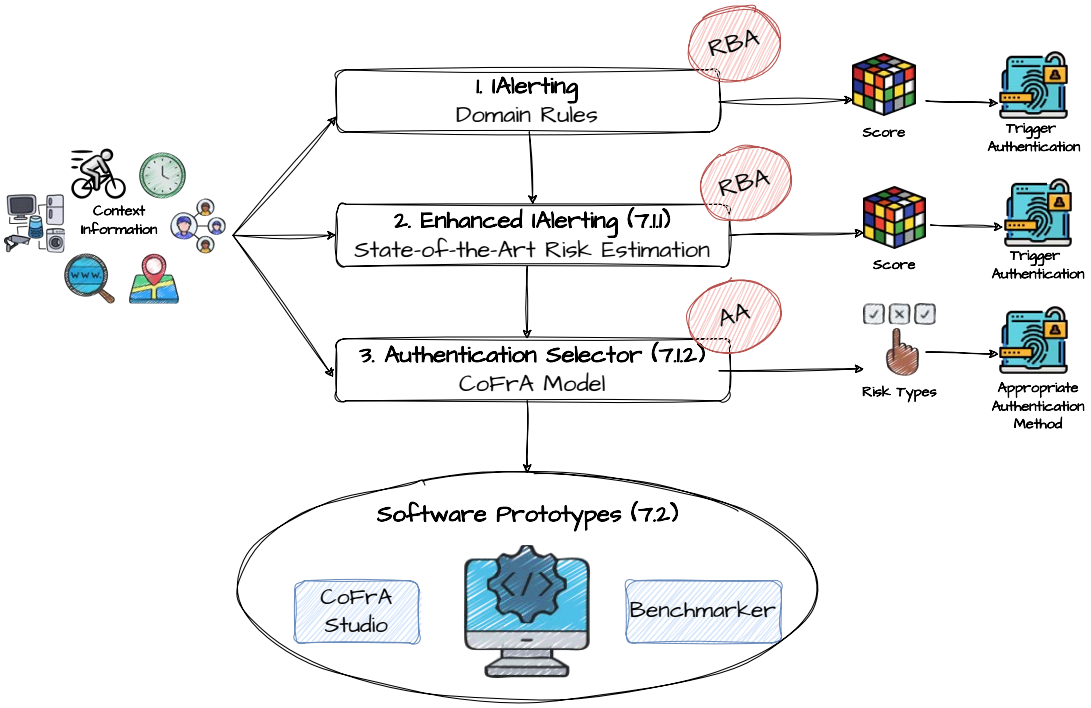

Figure 7.3 – The Authentication Environment of Orange™ France: From *IAlerting* to *Authentication Selector*.

sic components of an authentication system (e.g., the Orange™ France authentication system), and I describe the necessary changes to integrate AA.

Basic Authentication System Architecture. The basic architecture of the Orange™ France authentication system (Figure 7.4) consists of a user interface, a reverse proxy, and an identity provider (IdP). The user interface serves as the entry point for users to interact with the authentication system. It can be a web-based login page, a mobile app, or any other form of interface. Users provide their credentials through the user interface to initiate the authentication process. The reverse proxy acts as an intermediary between the user interface and the server hosting the protected resources.

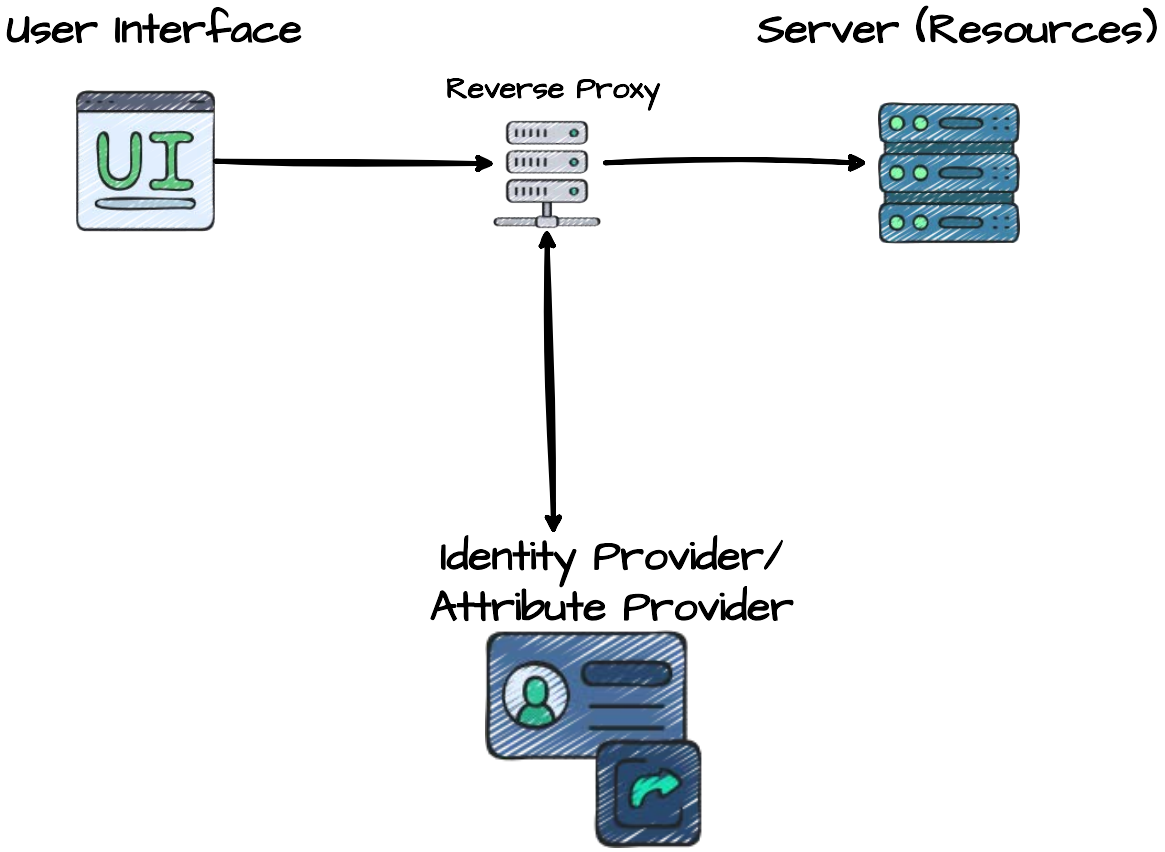

Figure 7.4 – Basic Authentication System Architecture.

Its primary function is to handle incoming requests from the user interface and forward them to the server. The IdP is responsible for managing user identities and authentication processes. It acts as a centralized service that validates user credentials and provides authentication assertions to grant access to protected resources. In the basic architecture, the IdP offers two authentication methods, namely password-based authentication and SMS OTP. When a user initiates the authentication process, the IdP prompts the user to perform password authentication or SMS OTP depending on the given preferences of the user. If the user uses password-based authentication, the user interface collects the password provided by the user and sends it to the IdP. If the user uses SMS OTP, the authentication process

may involve redirecting the user to a SMS OTP authentication service, which authenticates the user through their mobile device. Once authenticated, the SMS OTP authentication service returns an authentication token or assertion to the reverse proxy. When a user initiates the authentication process by entering their credentials through the user interface, the user interface sends the authentication request to the reverse proxy. The reverse proxy receives the authentication request from the user interface and forwards it to the IdP. The IdP communicates via the reverse proxy with the user and prompts him to provide a form of credentials. Then, the IdP validates the user's credentials received from the reverse proxy. It checks the provided credentials against the user database. If the credentials are valid, the IdP generates an authentication token or assertion. The IdP sends the authentication token or assertion back to the reverse proxy, which acts as an intermediary. The server verifies the token or assertion with the reverse proxy to ensure the user's authenticated session and grants access to the requested resources accordingly.

Adaptive Authentication System Architecture. When AA is integrated in this architecture (Figure 7.5), the IdP incorporates a SELECT component, which is responsible for dynamically selecting the authentication method based on the user's context. The SELECT component communicates with the CoFrA system. The CoFrA system analyzes contextual information and evaluates this information to choose the appropriate authentication method. Kafka [1], an event streaming platform, is utilized to facilitate communication between the SELECT component and the CoFrA system. The SELECT component can publish authentication-related events, such as user context data, to Kafka topics, and the CoFrA system can subscribe to these topics to receive and process the events. The SELECT component receives the user's authentication request from the reverse proxy and communicates with the CoFrA system via Kafka to obtain the user's contextual information, the assessment results, and the most appropriate authentication method. The SELECT component then proceeds with the

1. https://kafka.apache.org/

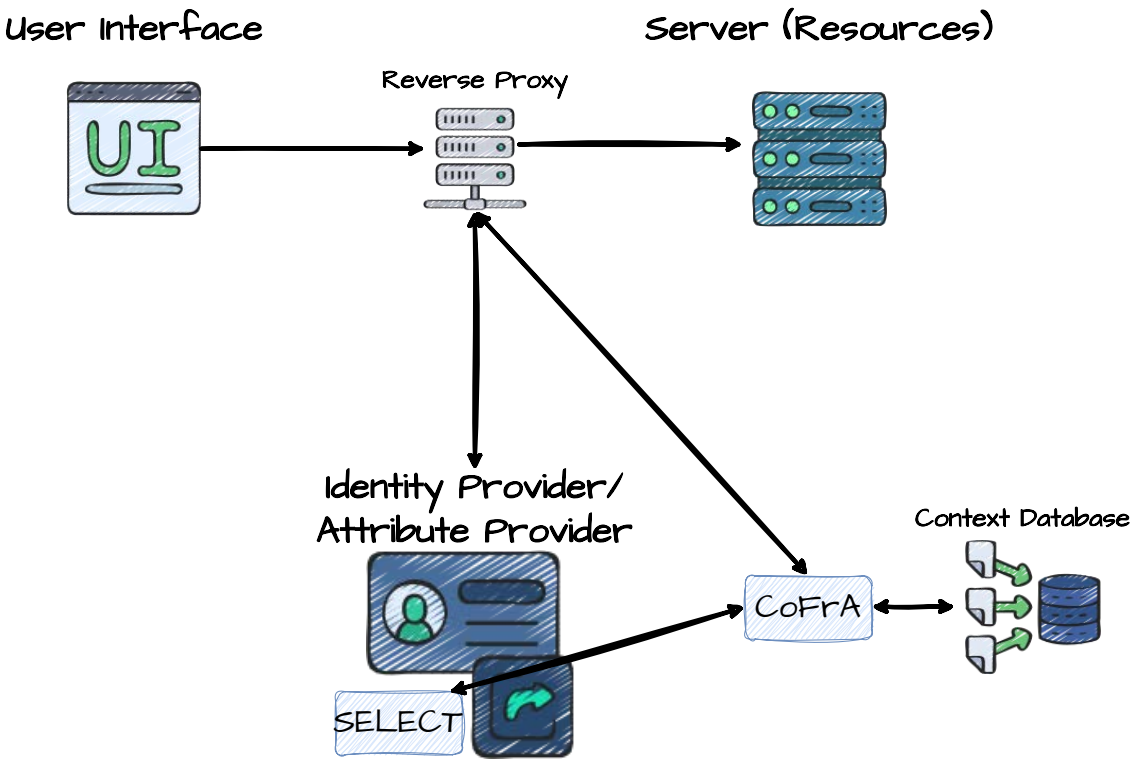

Figure 7.5 – Adaptive Authentication System Architecture.

authentication process based on the selected method, which can involve password-based, or SMS OTP authentication, or any other available methods. The reverse proxy transmits the necessary credentials or tokens to the IdP for validation and token generation, similar to the previous architecture.

AA introduces additional complexity compared to a static authentication system. It requires the development and integration of the SELECT and CoFrA components. The expertise gained from this thesis helps implementing these components. Integrating the SELECT component and the CoFrA system into the existing architecture requires careful planning and integration efforts. AA relies on gathering and analyzing contextual data to make informed decisions. This may involve collecting information from various sources, such as user devices, network logs, and behavioral

patterns. Proper data collection, storage, and processing mechanisms need to be implemented, taking into account privacy regulations and security considerations. Ensuring the accuracy and reliability of the collected data is crucial for effective AA. AA systems may require additional computational resources and infrastructure to handle the increased processing demands. Real-time analysis of contextual data and decision-making might impose higher performance requirements on the system. Scaling the infrastructure, optimizing the algorithms, and ensuring efficient data processing impact the costs and the complexity of the implementation.

7.2 Software Prototypes

The need for software prototypes arises from the desire to bridge the gap between the abstract concepts defended in this thesis and tangible implementations. The contributions of this thesis involve exploring new ideas about AA, testing hypotheses, and evaluating the feasibility of proposed solutions. The software prototypes presented in this chapter allow to bring the concepts to life and to demonstrate their practicality in a tangible form. By creating these prototypes, I was able to better understand how the concepts and theories translate into real-world implementations, what helped me to identify issues, refine the solutions and validate my ideas. The concrete representation of the solutions with the help of the prototypes also helped me to communicate my ideas to stakeholders, especially to potential users (*e.g.,* authentication engineers from Orange™). In this section, I first introduce the CoFrA Studio, which is a graphical modeling workbench for creating, editing and visualizing AA models. Then, I introduce the AA Benchmarker, which enables evaluating and comparing AA models as explained in Chapter 6.

7.2.1 CoFrA Studio - Graphical Modeling Workbench

With the help of Sirius, an Eclipse project, I created a graphical modeling workbench by leveraging the Eclipse Modeling technologies, including

Eclipse Modeling Framework (EMF). The modeling workbench is composed of a set of Eclipse editors (diagrams, tables and trees) which allow the users to create, edit and visualize CoFrA models.

Hence, I propose a modeling tool which natively supports the vocabulary to create a CoFrA model according to CoFrA. Users do not have to learn concepts which are external to the authentication domain. They just have to learn the views provided by the tool and how to navigate between them. Having this graphical modeling workbench for creating, editing and visualizing CoFrA models provides a visual representation of a complex model, making it easier to understand and communicate about it. It also facilitates the collaboration between different stakeholders, as the models can be easily shared and discussed. Furthermore, it enables simulation and testing of various models, allowing for the exploration of different authentication solutions before implementation.

Figure 7.6 shows the CoFrA studio palette showing all the necessary concepts to create an AA model conform to CoFrA.

Figure 7.7 shows the creation of the example model of Bob, the traveler (Chapter 1) with the CoFrA modeling workbench. The model consists of four ContextInformation instances, three ThreatSituation instances, one Risk instance, and three AuthenticationMethod instances. The CoFrA studio allows the creation of these instances with all necessary attributes (*e.g.,* history, privacy, frequency, quality, and environment for ContextInformation).

Standard Library. I explained in Chapter 4 that I also provide a standard library of common values of instances and attributes for the concepts of the CoFrA metamodel. This library is available in the CoFrA studio. Hence, authentication engineers can use the library as a support for modeling an AA system. For each concept of CoFrA (ContextInformation, ContextThreatAlgo, ThreatSituation, ThreatRiskAlgo, Risk, AuthenticationMechanism (Chapter 4)), I provide a common set of instances and attribute values. Also for the enumeration classes, I provide a common set of values. Authentication engineers can customize the li-

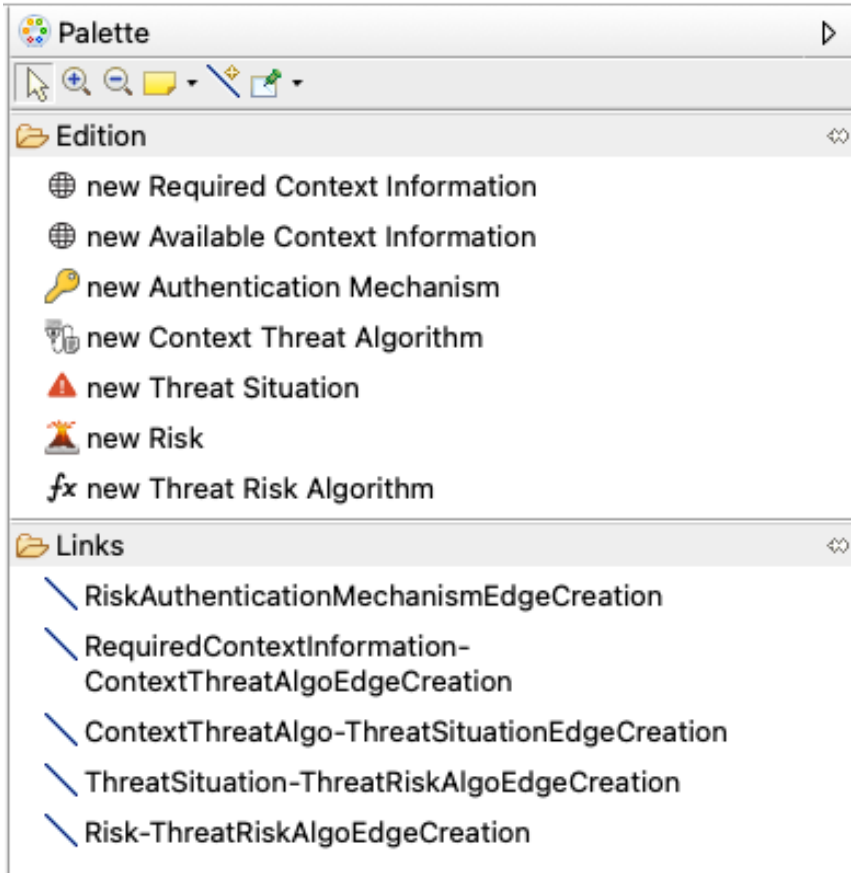

Figure 7.6 – The CoFrA Studio Palette.

brary included in the CoFrA studio by adding or removing some of these common values.

These properties may not directly align with real-world authentication protocols as they are theoretical and are hence typically used to discuss authentication protocols among researchers. There are still several benefits considering them in the evaluation process. By incorporating properties that have been widely discussed and used in research, I establish a connection between academic research and industry practice promoting a more holistic understanding of authentication solutions. Including these properties in the evaluation also encourages authentication engineers to engage with and critically analyze these academic properties.

When users of the CoFrA studio instantiate concepts, they can directly add attributes from the library. For example, Figure 7.8 shows the creation

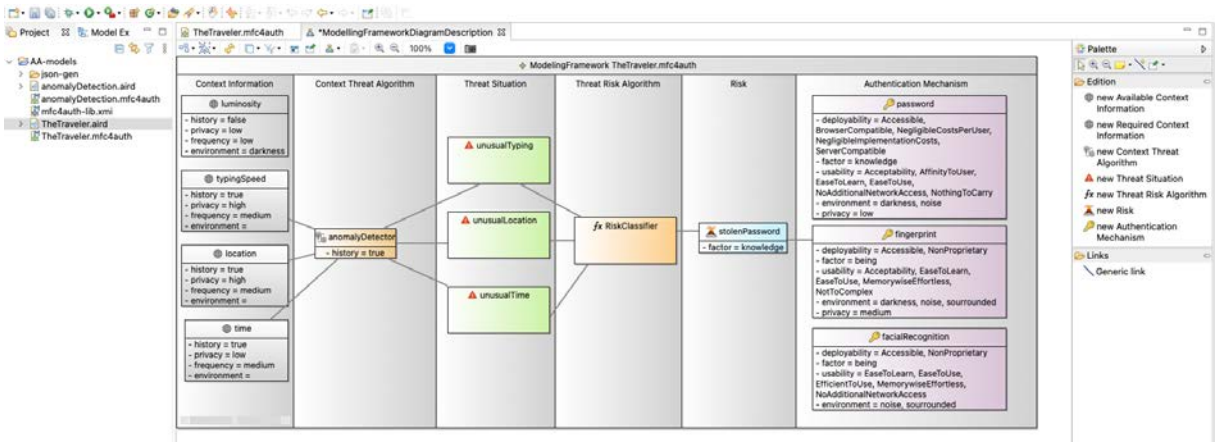

Figure 7.7 – Creation of the Traveler Model with the CoFrA Studio.

of an authentication method instance (password-based) and the pop-up window allowing to choose values for the usability attribute from the standard library. To choose the usability values for an authentication method, the user can take the evaluations (security politic file) as an inspiration, but can also add or remove some values according to their own knowledge. For example, I evaluated the SMS_OTP authentication method as "easy to use". But it is possible that for some user groups (*e.g.*, users of exclusively non-mobile equipment) this authentication method may be hard to use. Hence, an authentication engineer would not allocate the "easy to use" property to the authentication method SMS_OTP in his model.

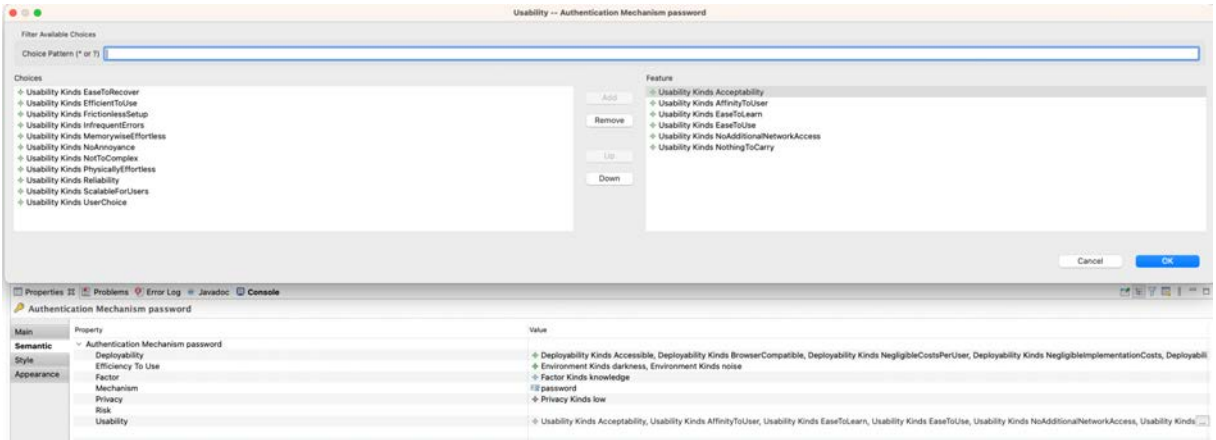

Figure 7.8 – Creation of an Authentication Method Instance - Password.

7.2.2 Authentication Model Benchmarker

I also developed a software tool to prototype the evaluation methodology for authentication models described in Chapter 6. The tool is designed to be used in conjunction with the CoFrA studio and allows the user to evaluate different models on various user paths. The tool takes as input the model files extracted using the CoFrA studio. The CoFrA studio allows extracting the created models in JavaScript Object Notation (JSON) format. The interface provided by the tool then includes drop-down lists for the user to choose the model to be evaluated, the user path, and the security politic file. As explained in Chapter 6, I provide a set of user paths based on the data set from Wiefling et al. [2].The model files have been extracted from the CoFrA studio and the user can choose from a set of models. The same holds for the security politic file. There are also five buttons provided for evaluating the usability, the security, the deployability, and the privacy of the authentication model on the chosen user path. The "General Evaluation" button evaluates the number of authentications requested and calculates the ratio of authentication attempts for which an authentication method is requested with the path length. The interface is shown in Figure 7.9.

For each of the criteria, the tool applies evaluation metrics to assess the model's performance. The evaluation metrics are based on a Python code that counts each criterion's desired properties from the standard library in the path and computes the authentication path's mean value. While this is a simple approach, it provides a baseline for evaluating authentication models according to required properties identified in the literature. However, it is important to note that the evaluation metrics can be extended and customized according to the specific needs of the authentication engineer. For example, for usability evaluation, the number of authentication methods that the user is asked to provide during a day can be taken into account instead of just counting the usability properties of the authentication methods. This allows for a more nuanced evaluation of the authentication

2. https://zenodo.org/record/6782156

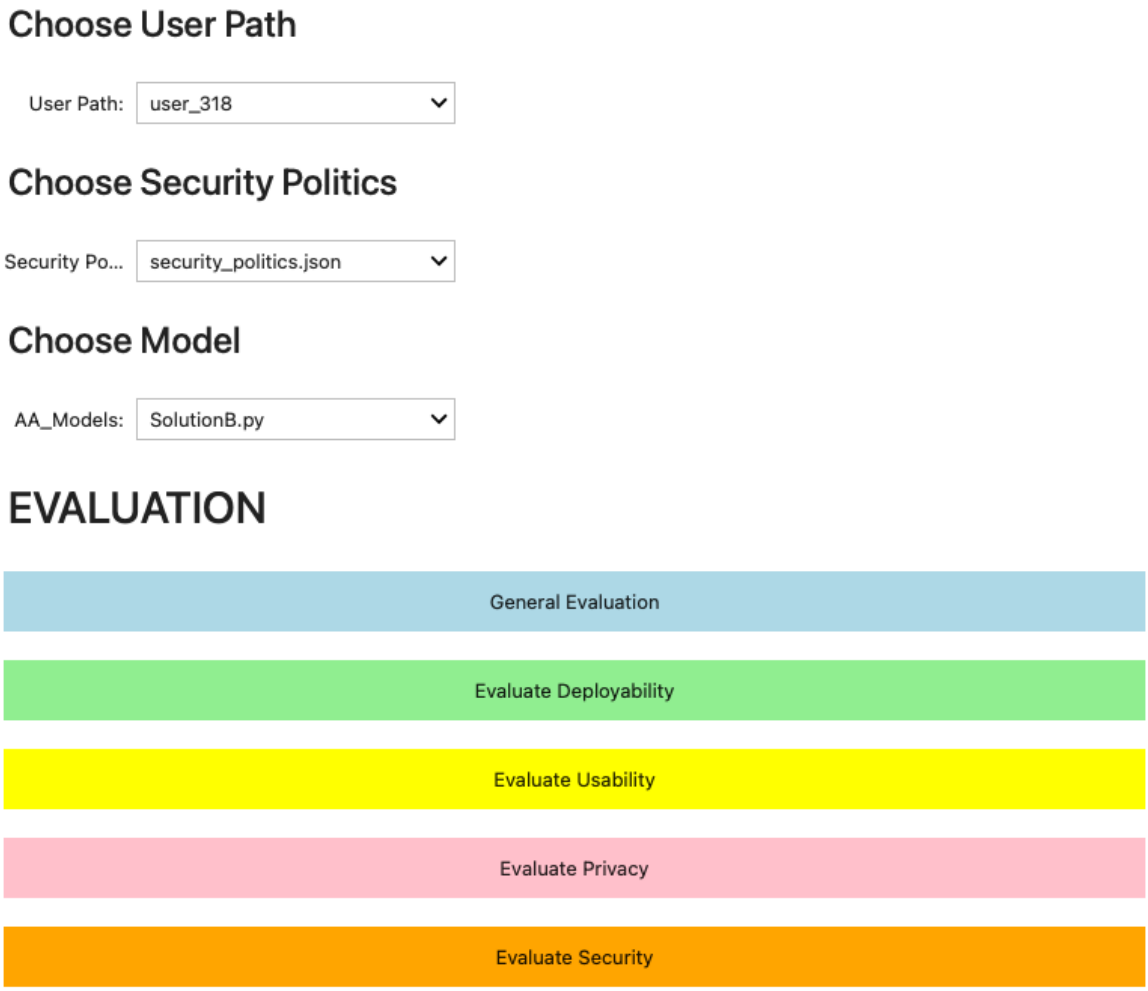

Figure 7.9 – User Interface for Evaluating an Authentication Model on a User Path.

models based on the requirements of the specific authentication system being evaluated. The results of the evaluations are stored in *csv* files in a folder, and the user can access this folder to compare the model performance according to all the evaluation metrics. Overall, the tool provides a user-friendly interface to prototype the evaluation methodology described in Chapter 6 and offers customization options for evaluation metrics.

To further explain the tool, I describe in the following a use case scenario. I created the models *OrangeStandard* and *OrangeV1* with the CoFrA studio. [3] The *OrangeStandard* model is inspired by the current authenti-

3. For confidentiality reasons I do not show the models here. I have already included other figures

cation system of Orange™ mainly based on the contextual feature *time* and the notion of expired sessions. The *OrangeV1* model is inspired by the authentication solution with the *Authentication Selector* and hence takes into account multiple contextual features to choose between diverse authentication methods. I then generated the corresponding JSON files (*OrangeStandard.json*, *OrangeV1.json*) I copied the two files in the *models/instances/* folder of the benchmark workspace (Figure 7.10).

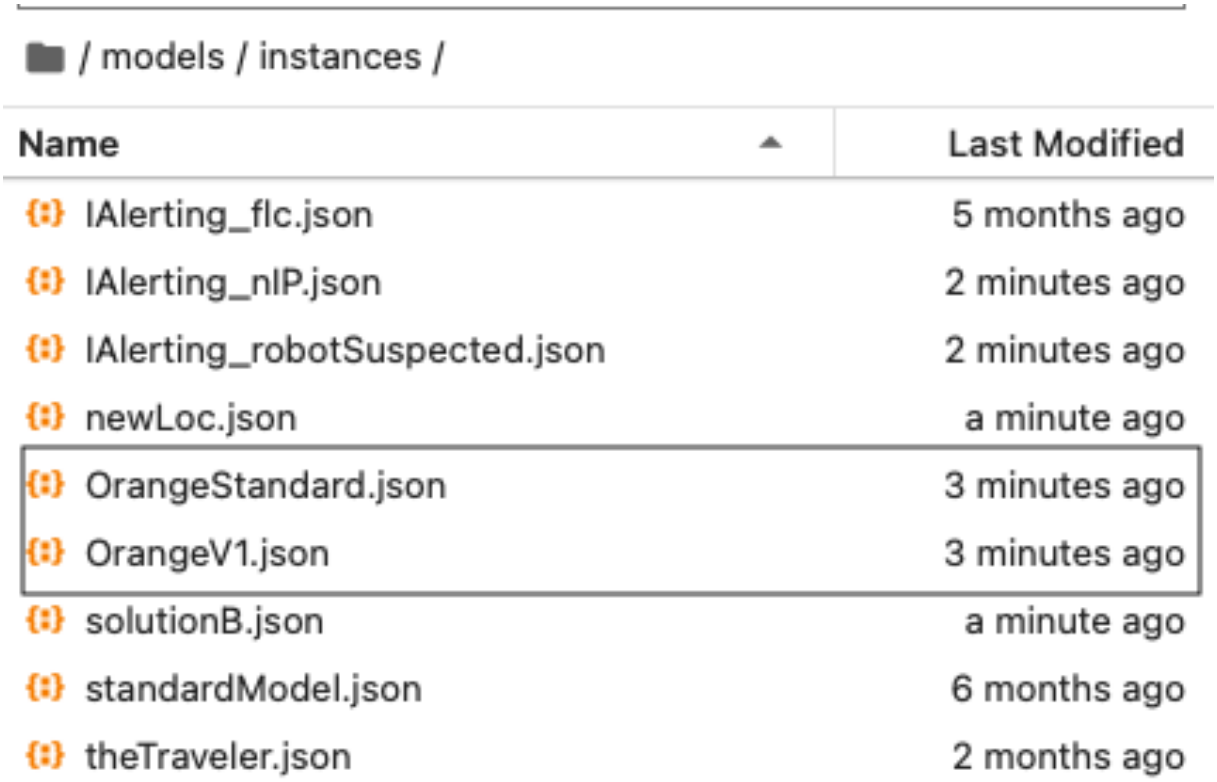

Figure 7.10 – Copy JSON Files in Benchmark Workspace - *OrangeStandard*, *OrangeV1*.

Then, I evaluate the two models (Figure 7.11).

Clicking on the evaluation buttons for these two models generates two *csv* files containing the results of the evaluation (Figure 7.12, Figure 7.13).

The first time a model is evaluated, a *csv* file is generated. Then, for each evaluation (on another user path, for another metric) a line is added to this file.

illustrating the creation of an AA model with the CoFrA studio (*e.g.*, Figure 6.5).

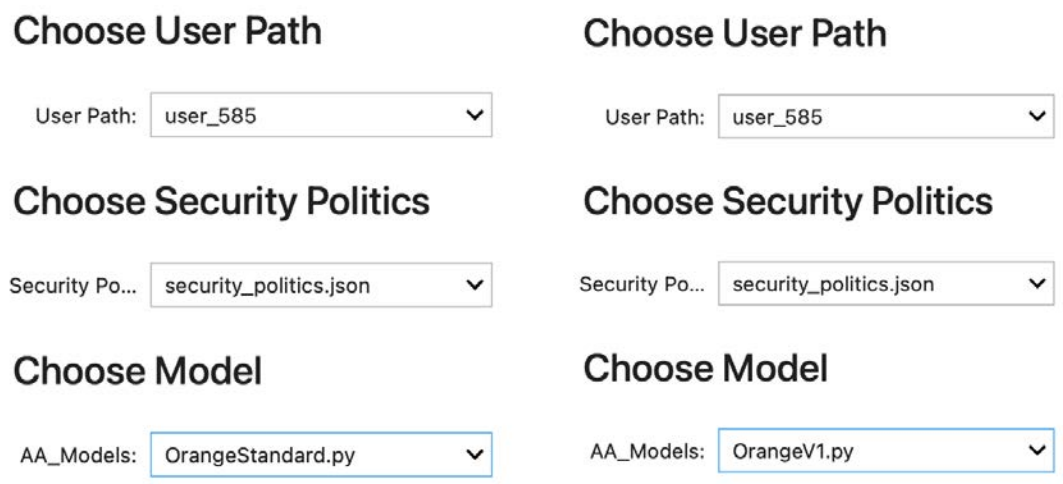

Figure 7.11 – Evaluation of the *OrangeStandard*, and the *OrangeV1* Models.

For the two example models, I evaluated the security, the deployability, the usability and the privacy according to the properties of the authentication methods as explained in Chapter 6. We can see that the *OrangeV1* model only requires 45 authentication challenges while the standard model requires 91 for a user path length of 678 authentication attempts. This means that based only on time, authentications are requested from the user even if there is no risk according to a CoFrA model (context analysis). One can consider the *OrangeV1* model more usable for this reason. The deployability and privacy values are decreasing when the *OrangeV1* model is used, while the usability value is maintained and the security value increases. Hence, in this example deployability and privacy issues need to be discussed and the *OrangeV1* model can be suitable for an application that requires a high level of security. This example illustrates how the results of the benchmark tool can be used for discussion support by authentication engineers. I note here that the benchmark does not provide a universally valid decision between two models. Rather, it helps to discuss different criteria and understand their evolution. The evaluation results are

bench_config.ipynb | <function OrangeStandard

Delimiter: ,

	AA_Model	security_politics	user_path	metric	value
1	OrangeStandard.py	security_politics.json	user_585	nb_authentications	91
2	OrangeStandard.py	security_politics.json	user_585	mean_sequence_deployability	7.0
3	OrangeStandard.py	security_politics.json	user_585	mean_sequence_usability	3.0
4	OrangeStandard.py	security_politics.json	user_585	mean_sequence_privacy	4.0
5	OrangeStandard.py	security_politics.json	user_585	mean_sequence_security	1.0

Figure 7.12 – Evaluation results: *OrangeStandard*.

bench_config.ipynb | <function OrangeV1 at 0x11

Delimiter: ,

	AA_Model	security_politics	user_path	metric	value
1	OrangeV1.py	security_politics.json	user_585	nb_authentications	45
2	OrangeV1.py	security_politics.json	user_585	mean_sequence_deployability	1.0
3	OrangeV1.py	security_politics.json	user_585	mean_sequence_usability	3.0
4	OrangeV1.py	security_politics.json	user_585	mean_sequence_privacy	2.0
5	OrangeV1.py	security_politics.json	user_585	mean_sequence_security	5.0

Figure 7.13 – Evaluation results: *OrangeV1*.

here only examples to illustrate their use.

7.3 Summary

This chapter describes the gradual transition from RBA to AA at Orange™ France. I explain how I improved the risk estimation models for the RBA implementation, and how I implemented the *Authentication Selector*, which adjusts the authentication method(s) based on current context and risk factors based on CoFrA. The chapter also introduces prototypes, including the CoFrA Studio for creating and visualizing AA models and the authentication model Benchmarker for evaluating and comparing authentication models. Overall, the chapter aims to bridge the gap between

abstract concepts and tangible implementations of AA, allowing for better understanding, refinement, and validation of my ideas.

Chapter 8

Conclusion and Perspectives

This last chapter summarizes the main content of this thesis and discusses future research lines. I summarize the scientific and industrial context of Adaptive Authentication (AA), and my contributions. Then, I state ongoing work, research perspectives and industrial perspectives to extend this research.

Contents

8.1 Background

This thesis presents a comprehensive investigation into AA with a focus on using context information to dynamically select appropriate authentication method(s). I highlight the interdisciplinary nature of the research field, encompassing security & privacy, machine learning, identity management and adaptive systems, with the challenges it presents. Specifically, I explore the challenges of black-box risk score calculations, evolving identity standards, and sensitive context information. I emphasize the importance of context modeling for security applications like AA, stressing the need for standardized and practical solutions to enhance authentication systems. Also, I discuss the ongoing quest to replace passwords and emerging authentication trends. My thesis includes an analysis of the state-

of-the-practice, an identification of commercial AA solutions using AI technologies for risk assessment based on contextual factors, and insights from experts in the field. Additionally, my research dives into RBA approaches, highlighting their potential for secure authentication with good usability while outlining their limitations. I argue that assessing the appropriateness of authentication methods requires a more fine-grained approach beyond relying solely on risk scores.

8.2 Contribution

This thesis has four main contributions. The first contribution is a **systematic literature review** that provides a structured review of the literature on Context Modeling for Adaptive Authentication (CM4AA). The review aims to understand the current body of knowledge about CM4AA by analyzing the context information that determines the context of AA systems, how it is modeled, and for which phase of the authentication system life-cycle the model is used. Desired properties of the context information model and its use for AA systems are also identified. This contribution enhances the understanding of the current body of knowledge about CM4AA and provides a systematization of knowledge.

The second contribution is a **Context-driven modeling Framework for dynamic Authentication decisions (CoFrA)**. The framework leverages context information to reason on the appropriateness of authentication methods beyond the calculation of risk scores. It is based on a precise metamodel that reveals framework abstractions and a set of constraints that specify their meaning. The framework supports authentication engineers in the complex trade-off between context information, risks, and authentication methods, according to usability, deployability, security, and privacy properties. It provides a domain-specific language for AA. The proposed framework is validated through case studies and extensive exchanges with authentication and modeling experts. This contribution abstracts the domain knowledge about context modeling for AA and provides a language to determine the appropriate authentication method(s) in a given context.

The third contribution is an **explainability model that uses Shapley values to obtain contextual explanations of risk scores** estimated with RBA approaches. The model proposes an explanation of the risk scores of authentication events and can be used to integrate a more fine-grained reasoning about the appropriateness of authentication methods into CoFrA models. This supports the transition from RBA approaches to AA. The contextual explanations of the risk score can help authentication engineers attempting to provide the appropriate authentication method(s), to understand the suspiciousness of an authentication event and the attack type, and hence to choose the appropriate authentication method(s).

The fourth contribution is **a tool-supported approach for the definition of the most well-suited authentication model for a given system**. The approach enables the evaluation of the quality of authentication models (*e.g.,* CoFrA models, RBA models, static models). It proposes components to apply an authentication model on a user path and to evaluate its performance. Multiple authentication models can be compared to select and tailor models for specific systems. This is the first evaluation approach to allow a multi-dimensional trade-off analysis between different quality criteria instead of a one-dimensional evaluation metric. This evaluation allows authentication engineers to choose the most well-suited model for a given authentication system.

In summary, the first contribution enhances the understanding of the current body of knowledge about CM4AA. The second contribution abstracts the domain knowledge about context modeling for AA and provides a language to determine the appropriate authentication method(s) in a given context. The third contribution provides an explainability model that helps to understand the suspiciousness of an authentication event and supports the transition from RBA to AA. The fourth contribution enables the evaluation of the quality of authentication models and helps authentication engineers to choose the most well-suited model for a given authentication system. Together, these four contributions support the **design, deployment and evaluation of AA systems** by handling the complex

navigation between context information, threats, risks and authentication methods.

8.3 Ongoing Work and Perspectives

In this thesis, I presented my work that covers the needs of precisely modeling context for AA and to reason on it to provide the appropriate authentication method(s). However, there is still a lot of work that can be done to advance research in the field. In this section, I thus discuss some ongoing work and perspectives that should be considered in the continuation of my research work. I also present industrial perspectives to outline the impact of my research for Orange™ , and other companies.

8.3.1 Ongoing Work

In this section, I present work that I am currently conducting and that extends my Ph.D. research project in the short term.

Community-Driven Benchmark. The absence of standardized evaluation metrics and benchmarks for authentication models can be attributed to the lack of open discussions within the community. Hence, in addition to the tooled approach for the definition of the most well-suited authentication model presented in Chapter 6, I aim to leverage my knowledge gained in industry and academia to propose a comprehensive set of authentication models. The objective is to gather information about existing authentication models from a variety of sources and to evaluate their performance using the tooled approach. Then, I will analyze and publish the results.By publishing the results, the goal is to initiate discussions within the community. Various stakeholders can participate in discussions concerning the quality of different authentication models and discuss evaluation metrics. The end goal is to foster a collaborative effort within the community to establish a benchmark for authentication models and hence contribute to the

development of better authentication models and methods for evaluating their performance.

Explanations of Additional RBA Models. The proposed explainability methodology (Chapter 5) needs to be extended to other datasets and risk score estimation models. Initially, there was a limitation as no publicly available dataset was accessible during the development of the methodology. However, a recent publication by Unsel et al. [121] has provided a synthesized login feature dataset comprising over 33 million login attempts and 3.3 million users from a large-scale online service in Norway. Additionally, the authors have made available the first open-source Risk-Based Authentication (RBA) implementation. The objective is to apply the explainability model developed in Chapter 5 to the newly available dataset and open-source RBA implementation. Hence, the observed risk clusters will be subjected to further investigation on another dataset to identify different types of attacks. Corresponding CoFrA models will be constructed based on the findings from the investigation to better reflect the risks.

Expert Evaluation of CoFrA and CoFrA Studio. To show the usability of the CoFrA studio, an evaluation by experts using the studio is missing. Hence, I plan to demonstrate the usability of the CoFrA studio through a structured evaluation conducted by experts. Therefore, I am currently working on a fully functional tool which includes the CoFrA modeling studio and the benchmarker prototype. I aim to conduct these evaluations with the experts I already contacted for the surveys. They are familiar with the domain and can provide valuable feedback on the usability of the tool. Their feedback will also help identify potential issues or areas for improvement that may not have been apparent otherwise. Demonstrating the effectiveness of the tool through this experimentation can help build confidence and further push its use. This will also help the validation of the fourth contribution of this thesis, as a direct comparison can then be made between manual evaluation of authentication models and a tool-based evaluation.

Automated Generation of CoFrA Models. In this thesis, I introduce concepts and a language that facilitates the design of CoFrA models. However, the current process of designing a CoFrA model relies on manual efforts from authentication engineers. This proces can be time-consuming, particularly as systems become more complex and new risks and threats emerge. To further enhance the efficiency of this process, I aim to explore ways to automate the generation of CoFrA models using techniques like threat and risk clustering models. The challenge therefore lies in finding methods to gather relevant data related to threats, risks, and contextual information, and then using this data to automatically generate coherent CoFrA models. By automating the process of CoFrA model generation, I seek to reduce the time and effort required for design contributing to a more efficient and effective approach to CoFrA model design.

Model For Context Information Acquirement. The acquisition of context information and sensor technologies are out of scope of this thesis. I shed light on the fact that the contextual relationships between different entities often are omitted when context information for AA is modeled. In the literature review (Chapter 3), I observe that most contributions for context modeling for AA systems do not only rely on raw sensor data but consider context information on a transformed level. I also found that the works are often based on context information acquired from mobile devices. Those are therefore crucial for data acquisition in the research area of CM4AA. Non-mobile devices are often disregarded.

I defined context information as a triplet (informing entity, contextual feature, assigned entity) in Chapter 3 to enable a detailed analysis of the entities and their situations in an AA system. Hence, this notion of a triplet may be incorporated into the CoFrA model and may build the basis for proposing a model-driven approach for the acquisition of context-information. Within this research, I aim to improve the distinction between raw sensor information and information at a transformed level to enable keeping track on the transformations. By proposing a context acquirement model, I also aim to enable taking into account contextual relationships

between different entities and tacking into account non-mobile devices.

8.3.2 Research Perspectives

In the following subsection, I discuss new areas for future research for the broader field of study.

Figure 8.1 shows four problems triggering four research perspectives. I arrange them in the MAPE-K loop for AA systems introduced in Chapter 1 according to the areas they concern. The problem of incorrect context information due to the use of Virtual Private Network (VPN)s and proxies or stolen fingerprints concerns **Monitoring (M)** and motivates perspective 1. The difficulty to take into account user preferences on authentication methods concerns **Analysis (A)** and motivates perspective 2. The lack of a formal validation of the security of an AA system concerns **Plan (P)** and motivates perspective 3. The limited privacy of IF systems that increase the availability of AA concerns **Execution (E)** and motivates perspective 4. In the following, I detail the four perspectives.

(M) Incorrect Context Information. I discussed in Chapter 2 the evolving attack landscape and explain that as authentication systems get more sophisticated attackers also find new ways to bypass them. For AA, falsified context information plays a crucial role in these attacks. Lin et. al [69] explain how phishing attackers use browser fingerprints to bypass context-aware authentication systems. Other works identify ways to falsify context information to bypass context-aware authentication (*e.g.,* [7, 28]). Proxy servers and VPNs are also commonly used tools that allow users to access online content anonymously and bypass geographical restrictions. However, these tools can also be used for malicious activities, such as cyber attacks, and data breaches. Therefore, it is essential to identify traffic coming from proxies and VPNs to assess the associated level of risk. These tools can mask the true identity and location of the user and can lead to a false sense of security when relying on Internet Protocol (IP) address, geolocation or other location-based context information. For example, if a user is

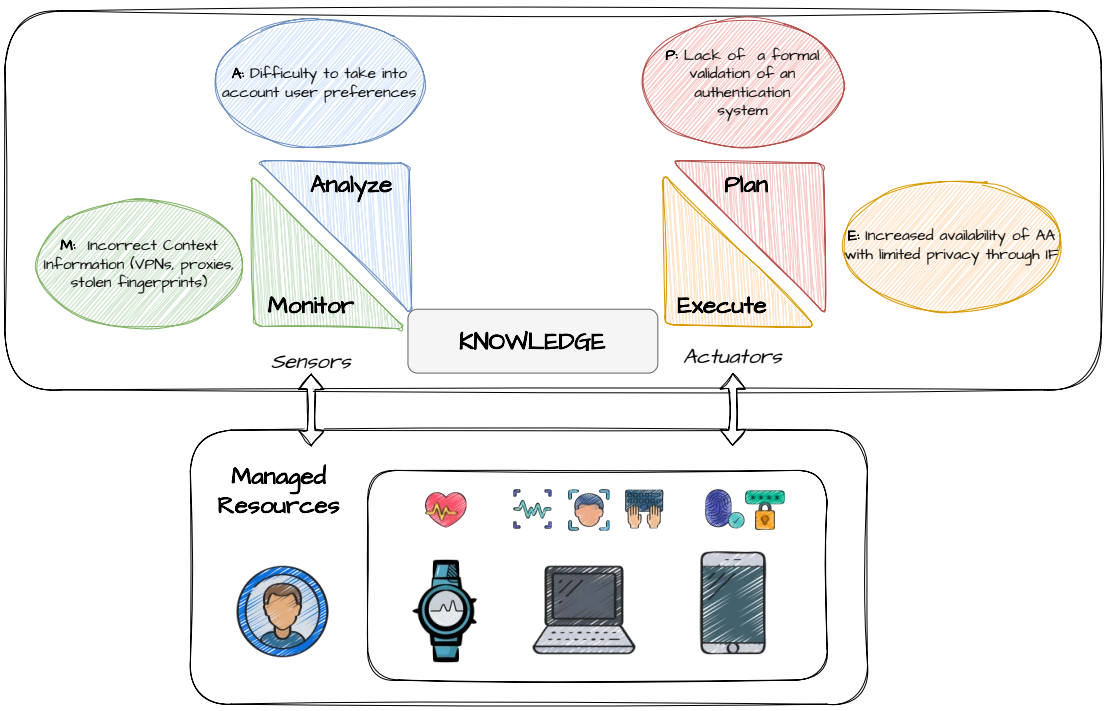

Figure 8.1 – Main Problems Triggering Future Research Perspectives.

logging in from a different country than their usual location, it may trigger a risk for the authentication system and lead to the authentication attempt flagged as suspicious. Malicious actors can use proxies and VPNs to obfuscate their true location and carry out attacks from different locations around the world, making it difficult to track and identify them. However, this could be a legitimate use of a VPN or proxy by a user who is traveling or working remotely. I showed in Chapter 3 that anomaly detection plays a crucial role for AA. These algorithms suffer particularly from falsified contextual information.

This future research will investigate how we can accurately identify falsified context information (*e.g.,* traffic coming from proxies and VPNs, and falsified browser fingerprints). The aim is to provide a framework for attributing a specific level of correctness to the context information.

(A) Hierarchical Management of Authentication Methods Beyond Authentication Factors: Incorporating User Preferences and Context. CoFrA al-

lows choosing authentication methods according to the context, identified threats and risks. To guarantee the resilience against different risk types, authentication methods are differentiated according to the factors they rely on: Something You Know, Something You Have, Something You Are (Chapter 2). The context in which the authentication takes place is also taken into account. CoFrA ensures the usability of the authentication methods in the environment (*e.g.,* no face recognition in the dark). Additionally, CoFrA allows different desired properties to be assigned to the authentication methods (*e.g.,* usability, deployability, privacy and security properties). Moreover, users often have different preferences and choices for their authentication methods. Based on these aspects, the properties of the methods may vary. Therefore, there is a need for a hierarchical management approach for authentication methods that can incorporate user preferences and choices, in addition to the context and authentication factors. The research will be based on my literature review and the identified state-of-the-art authentication methods. User studies and surveys may be helpful to collect data on user preferences and choices for these authentication methods. A hierarchical management approach for authentication methods will enable the user having more control and flexibility over the authentication methods. This can also help to look at different user groups in different ways. I have already mentioned that, for example, usability values can vary from user group to user group. Also, users may have different preferences regarding privacy. Some may want to disclose more in order to have a more secure authentication, while others may want to share less information.

(P) Model Validation Framework for AA Systems. With the help of CoFrA, AA systems can be designed. This thesis also provides a tool-supported approach to evaluate and compare AA models (Chapter 6). I provide a methodology for evaluating the quality of the models. The approach helps authentication engineers to define the most well-suited authentication model for a given system. However, when a new authentication system is implemented, there remains a need to formally ensure that the solution

provides adequate security. Hence, this future research focuses on the development of a model validation framework for authentication systems to not only evaluate and compare systems, but to validate the system's security formally. Hence this involves developing a formal specification of a secure authentication process. I proposed in Chapter 6 a formal description of an authentication path. The added value of this research is the formal specification of the path in a formal language to enable reasoning about its security (*e.g.,* with formal model-checking methods). A formal specification of an (adaptive) authentication system and the corresponding authentication path, and a formal specification of the security requirements are necessary. The model validation framework can be developed based on a thorough literature review of security requirements for authentication processes and an investigation of how they can be formalized and proved.

(E) Towards Privacy-Enhanced Identity Federation (IF). IF is increasingly used in both private and public sectors, including cloud computing platforms, private organizations, and global markets [63]. In addition to allowing users to access web applications seamlessly, IF increases the availability of AA [49].

IF enables the sharing of digital identities across multiple services, allowing users to access resources across various domains managed by different services. To achieve this, services agree on standards and protocols, forming a federation. The IF system architecture typically includes users, IdPs/ AtPs, and SPs. The user's credentials and attributes are stored with the IdP, eliminating the need to have credentials for each SP. Instead, the IdP validates the user's credentials through a dialog and protocol exchange with the user and the SP.

IF also enables SPs to request access to additional user data stored with the IdP/ AtP. Major IdPs like Facebook, Google, and Microsoft offer web Application Programming Interface (API)s that allow SPs access to user data stored on their platforms. Conversely, also the IdP can gain information about the user's behavior and track them.

This is specifically important when the IdPs propose AA, because that

means that the IdPs require context information and may share it with SPs. Gavazzi et al. [49] found that nearly all IF providers that support MFA and RBA are major third-party trackers and say that more work needs to be done to make MFA and RBA more widely available in IFs and privacy-preserving.

In a non federated two-party AA protocol, there are two involved parties: the authenticating party (*e.g.,* the service) as well as an authenticated party (*e.g.,* the user). The authenticating party is in charge of the adaptation and hence controls the user context data. In a federated AA protocol, there is a third party involved in the process as some protocol steps are delegated from the service itself as authenticating party to an IdP taking the role of an authenticating party and controlling user context data. The involvement of a third party in a IF AA protocol can give rise to privacy issues due for example to increased data sharing, the centralization of user data, the possible lack of control over data handling for the user, and the possibilities of user activity tracking for the IdP.

There are many existing works on privacy shortcomings of current IF standards like Open ID Connect (OIDC) or Security Assertion Markup Language (SAML) (*e.g.,* [85, 115, 67, 126]).

Legal requirements require organizations to use privacy-preserving technologies. Nevertheless, IF solutions often lack compliance with legal requirements for informed consent and Privacy by Default [60, 11]. In addition to legal requirements, there have been many academic initiatives for proposing privacy-preserving IF solutions (*e.g.,* [81, 134, 52]).

Hence, the privacy problems of IF can be (partly) mitigated by applying these techniques. Nevertheless, AA itself raises problems about privacy, because sensitive user context information is used. In [8], the authors identify issues related to privacy that derive from the need to comply with privacy regulations like the GDPR. They mention the following issues: the privacy of data used for AA, the privacy of contextual data, which can reveal very sensitive information about the user, such as location or activity, and the incorporation of user consent for authentication-related transactions without decreasing the overall usability. Wiefling et al. [130]

outline that context-aware authentication may expose potentially sensitive personal data, which conflicts with user privacy rights.

Some privacy properties for IF also need to be looked at from a different perspective when AA is used. For example, when identity providers propose AA, the principles of minimal attribute disclosure and purpose limitation are still relevant but may be implemented differently to accommodate the contextual factors involved. The principle of minimal attribute disclosure states that only the necessary attributes or information should be shared during the authentication process. Context-aware authentication takes into account various contextual factors, such as user behavior, location, and device information, to assess the risk level and make informed authentication decisions. The principle of purpose limitation states that personal data should only be collected and used for specific, legitimate purposes that are disclosed to the user. Context-aware authentication may require the collection and analysis of additional data points to establish the user's context accurately. However, the purpose limitation principle remains important to ensure that the collected data is used solely for authentication purposes and not for other unrelated activities.

I aim to analyse if there are limitations that prevent us from designing an "ideal" privacy-preserving IF systems that satisfies all the desirable privacy goals and allows for AA. The question is whether identity federation and especially AA always involves a privacy trade-off or whether there is a "ideal" solution. I hence aim to shed light over the most common privacy requirements, and to shed light over the most common techniques to enhance the privacy of IF solutions and their usage. I then aim to analyze the alignment of privacy-preserving IF solutions with AA.

8.3.3 Industrial Perspectives

Orange™ handles sensitive customer information and provides multiple services. Proper identity verification ensures that these services are accessed by the intended individuals, and prevent fraudulent activities. Identity and authentication are vital in mitigating security threats such as identity theft

due to data breaches and fraud. By implementing robust authentication solutions, Orange™ can significantly reduce the risk of these threats. Identity and authentication measures also play an important role in building and maintaining customer trust. When customers trust that their identities are securely verified and their accounts are protected, they are more likely to engage with services provided by Orange™ . This trust leads to improved customer satisfaction, loyalty, and a positive reputation for Orange™ . AA, which I promote in this thesis, allows balancing the pros (such as enhanced security) with the cons (such as added user burden) of authentication methods according to multiple criteria. This enables Orange™ to make smart authentication decisions without just searching for password replacements and changing the authentication processes on a whim. AA involves dynamically adjusting authentication method(s). Research in this area is essential for Orange™ , as it enables enhancing security while maintaining s seamless user experience, privacy, and deployability properties. I explain in the previous chapter how I implemented the authentication selector, a first AA solution. In this section, I will discuss the ideal vision of the authentication landscape and how the ideas presented in this thesis align with that vision. The authentication landscape refers to the overall framework and strategies used for authentication. More precisely, I explain how the concepts of Password Based Authentication (PBA), Multi-Factor Authentication (MFA), Risk-Based Authentication (RBA), and Adaptive Authentication (AA) work together in the overall authentication landscape and its evolution. I have chosen these terms and especially the distinction between RBA and AA based on the specific focus of my research. By using these terms according to the definitions given in Section 2.1, I provide clarity and specificity to the concepts I am discussing in this thesis. However, I would like to point out here that in the literature and in the practice these terms are not always used in this way and concepts are often mixed up.

I also experienced in industry that the term “adaptive” is understood in multiple ways. Assuming that non-adaptive authentication means that the user enters its username and password at each authentication event, requiring the password only once in a while and not at each event is a kind

of adaptation. Requiring the user to enter a second factor from time to time (depending on session duration, service sensibility and other factors) is also commonly understood and experienced as "adaptation". Requiring the second factor depending on the risk level (RBA) is also a way of "adaptation". Requiring the appropriate authentication method(s), where appropriateness depends on the desired properties of the authentication method(s) in a context (my definition of AA) is a sophisticated way of "adaptation".

By outlining in this section how PBA, MFA, RBA, and AA work together according to my definitions and vision and contribute to the authentication landscape's overall evolution in industry, I demonstrate the interconnections between these concepts and emphasize the relevance and significance of my research for Orange™ 's authentication landscape.

Figure 8.2 shows the evolution process from PBA [1] to AA with advantages (in green) and disadvantages (in red) for each method.

The evolution from PBA to AA is not only driven by technological advancements but also by social factors, user willingness, acceptance, and customer characteristics. Understanding and addressing these factors is essential for promoting the adoption and successful implementation of AA solutions across different user segments and industries. The topic needs to be embedded in the overall context. Especially privacy issues need to be considered in more detail so that the solutions can be widely accepted.

To implement an AA system, several values have to be considered (*e.g.,* laws, regulation, corporate values). The European Commission is currently working on a European e-identity. Every EU citizen and resident in the Union will be able to use a personal digital wallet to identify themselves or provide confirmation of certain personal information. The debates and concerns surrounding the European Wallet project reveal that society is still grappling with the issue of privacy and identity. We are still far from achieving a consensus on how to balance the convenience offered by digital authentication solutions with the protection of individuals' privacy rights.

In this thesis, it has been confirmed that Adaptive Authentication (AA) has the potential to enhance the authentication landscape without searching for replacing passwords.

1. I define here PBA as an authentication model requiring systematically a password at each login request.

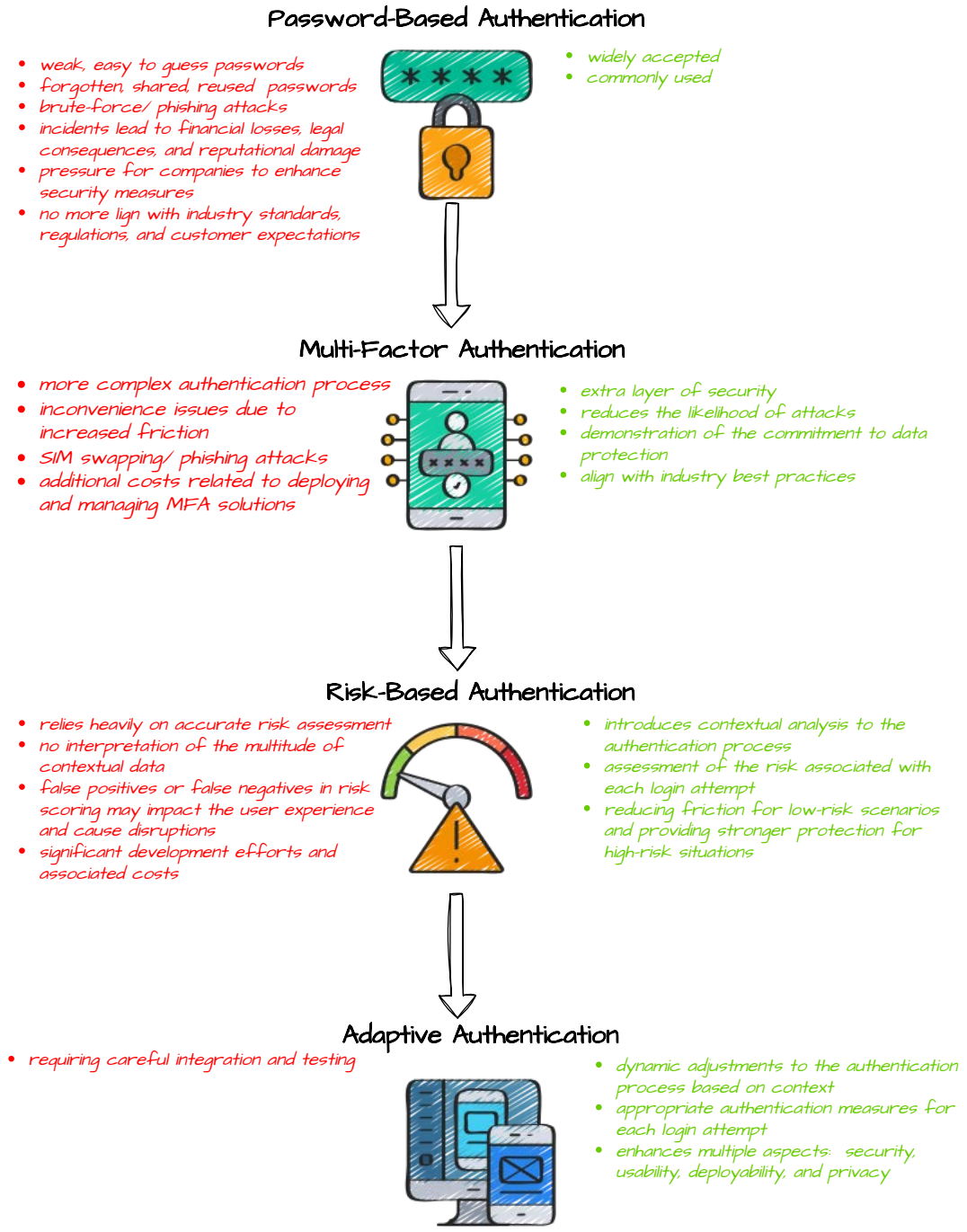

Figure 8.2 – Industrial Perspectives.

BIBLIOGRAPHY

[1] « A semantic model for authentication protocols », *in*: *Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, IEEE, 1993, pp. 178–194 (cit. on p. 22).

[2] Achilleas P Achilleos, Georgia M Kapitsaki, and George A Papadopoulos, « A framework for dynamic validation of context-aware applications », *in*: *2012 IEEE 15th International Conference on Computational Science and Engineering*, IEEE, 2012, pp. 532–539 (cit. on p. 65).

[3] Idan Achituve, Sarit Kraus, and Jacob Goldberger, « Interpretable online banking fraud detection based on hierarchical attention mechanism », *in*: *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)*, IEEE, 2019, pp. 1–6 (cit. on pp. 47, 178).

[4] Anne Adams and Martina Angela Sasse, « Users are not the enemy », *in*: *Communications of the ACM* 42.*12* (1999), pp. 40–46 (cit. on p. 1).

[5] Furkan Alaca and Paul C Van Oorschot, « Comparative analysis and framework evaluating web single sign-on systems », *in*: *ACM Computing Surveys (CSUR)* 53.*5* (2020), pp. 1–34 (cit. on p. 3).

[6] Md Zahangir Alom and Tarek M Taha, « Network intrusion detection for cyber security using unsupervised deep learning approaches », *in*: *2017 IEEE national aerospace and electronics conference (NAECON)*, IEEE, 2017, pp. 63–69 (cit. on p. 49).

[7] Patricia Arias-Cabarcos and Christian Krupitzer, « On the Design of Distributed Adaptive Authentication Systems », *in*: *Open Access Media* 5 (2017), pp. 12–14 (cit. on pp. 86, 88, 93–96, 201).

[8] Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker, « A survey on Adaptive Authentication », *in*: *ACM Computing Surveys (CSUR)* 52.*4* (2019), pp. 1–30 (cit. on pp. 2, 7, 23, 27, 36, 47, 48, 52, 53, 55, 61, 65, 155, 165, 166, 205).

[9] Colin Atkinson and Thomas Kuhne, « Model-driven development: a metamodeling foundation », *in*: *IEEE software* 20.*5* (2003), pp. 36–41 (cit. on pp. 30, 31).

[10] Khairul Azmi Abu Bakar and Galoh Rashidah Haron, « Adaptive Authentication: Issues and challenges », *in*: *2013 World Congress on Computer and Information Technology (WCCIT)*, Dhaka, Bangladesh: IEEE, 2013, pp. 1–6 (cit. on p. 26).

[11] Lujo Bauer et al., « A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality », *in*: *Proceedings of the 2013 ACM workshop on Digital identity management*, 2013, pp. 25–36 (cit. on pp. 54, 205).

[12] Nelly Bencomo, Sebastian Götz, and Hui Song, « Models@ run. time: a guided tour of the state of the art and research challenges », *in*: *Software & Systems Modeling* 18 (2019), pp. 3049–3082 (cit. on pp. 82, 89).

[13] Nelly Bencomo et al., « Genie: Supporting the model driven development of reflective, component-based adaptive systems », *in*: *Proceedings of the 30th international conference on Software engineering*, 2008, pp. 811–814 (cit. on p. 52).

[14] Emmanuel Bertin et al., « Access control in the Internet of Things: a survey of existing approaches and open research questions », *in*: *Annals of telecommunications* 74 (2019), pp. 375–388 (cit. on p. 60).

[15] Joseph Bonneau et al., « Passwords and the evolution of imperfect authentication », *in*: *Communications of the ACM* 58.7 (2015), pp. 78–87 (cit. on p. 2).

[16] Joseph Bonneau et al., « The quest to replace passwords: A framework for comparative evaluation of web authentication schemes », *in*: *2012 IEEE Symposium on Security and Privacy*, IEEE, 2012, pp. 553–567 (cit. on pp. 3, 33, 113).

[17] Tim J Boonen, Anja De Waegenaere, and Henk Norde, « A generalization of the Aumann–Shapley value for risk capital allocation problems », *in*: *European Journal of Operational Research* 282.1 (2020), pp. 277–287 (cit. on p. 133).

[18] John Brainard et al., « Fourth-factor authentication: somebody you know », *in*: *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 168–178 (cit. on p. 25).

[19] Nicolas Broders et al., « A generic multimodels-based approach for the analysis of usability and security of authentication mechanisms », *in*: *Human-Centered Software Engineering: 8th IFIP WG 13.2 International Working Conference, HCSE 2020, Eindhoven, The Netherlands, November 30–December 2, 2020, Proceedings 8*, Springer, 2020, pp. 61–83 (cit. on p. 3).

[20] Andy Brown et al., « Recurrent neural network attention mechanisms for interpretable system log anomaly detection », *in*: *Proceedings of the First Workshop on Machine Learning for Computing Systems*, 2018, pp. 1–8 (cit. on p. 48).

[21] Peter J Brown, John D Bovey, and Xian Chen, « Context-aware applications: from the laboratory to the marketplace », *in*: *IEEE personal communications* 4.5 (1997), pp. 58–64 (cit. on p. 2).

[22] Anne Bumiller et al., « A Context-Driven Modelling Framework for Dynamic Authentication Decisions », *in*: *SEAA 2022-Euromicro Conference Series on Software Engineering and Advanced Applications*, 2022, pp. 1–8 (cit. on pp. 18, 106).

[23] Anne Bumiller et al., « On Understanding Context Modelling for Adaptive Authentication Systems », *in*: *ACM Trans. Auton. Adapt. Syst.* (Feb. 2023), Just Accepted, ISSN: 1556-4665, DOI: 10.1145/3582696, URL: https://doi.org/10.1145/3582696 (cit. on pp. 7, 18, 58).

[24] Anne Bumiller et al., « Towards a Better Understanding of Impersonation Risks Anonymous », *in*: *15th IEEE International Conference on Security of Information and Networks (SINCONF 2022)*, 2022 (cit. on pp. 18, 128).

[25] Niklas Bussmann et al., « Explainable machine learning in credit risk management », *in*: *Computational Economics* 57 (2021), pp. 203–216 (cit. on p. 133).

[26] Li-jun Cai, Rui Li, and Ye-qing Yi, « A multiple watermarks algorithm for image content authentication », *in*: *Journal of Central South University* 19.*10* (2012), pp. 2866–2874 (cit. on pp. 88, 93, 94, 96).

[27] Miguel Calvo and Marta Beltrán, « A Model For risk-Based adaptive security controls », *in*: *Computers & Security* 115 (2022), p. 102612, ISSN: 0167-4048, DOI: https://doi.org/10.1016/j.cose.2022.102612, URL: https://www.sciencedirect.com/science/article/pii/S0167404822000116 (cit. on p. 52).

[28] Michele Campobasso and Luca Allodi, « Impersonation-as-a-service: Characterizing the emerging criminal infrastructure for user impersonation at scale », *in*: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 1665–1680 (cit. on pp. 4, 36, 201).

[29] Bing Chen, Chengxiang Tan, and Xiang Zou, « Cloud service platform of electronic identity in cyberspace », *in*: *Cluster Computing* 20 (2017), pp. 413–425 (cit. on p. 1).

[30] Zhe Chen and Aixin Sun, « Anomaly Detection on Dynamic Bipartite Graph with Burstiness », *in*: *2020 IEEE International Conference on Data Mining (ICDM)*, IEEE, 2020, pp. 966–971 (cit. on p. 49).

[31] Elyes Cherfa et al., « On investigating metamodel inaccurate structures », *in*: *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020, pp. 1642–1649 (cit. on p. 110).

[32] Sung Choi and David Zage, « Addressing insider threat using “where you are” as fourth factor authentication », *in*: *2012 IEEE International Carnahan Conference on Security Technology (ICCST)*, IEEE, 2012, pp. 147–153 (cit. on p. 25).

[33] Autonomic Computing et al., « An architectural blueprint for autonomic computing », *in*: *IBM White Paper* 31.*2006* (2006), pp. 1–6 (cit. on p. 26).

[34] James Conners et al., « Let's Authenticate: Automated Certificates for User Authentication », *in*: *Network and Distributed Systems Security (NDSS) Symposium*, 2022 (cit. on p. 21).

[35] Daniel D'Silva and Dayanand D Ambawade, « Building a zero trust architecture using Kubernetes », *in*: *2021 6th international conference for convergence in technology (i2ct)*, IEEE, 2021, pp. 1–8 (cit. on p. 35).

[36] Anupam Das et al., « The tangled web of password reuse. », *in*: *NDSS*, vol. 14, 2014, 2014, pp. 23–26 (cit. on p. 33).

[37] Sanchari Das et al., « Evaluating user perception of multi-factor authentication: A systematic review », *in*: *arXiv preprint arXiv:1908.05901* (2019) (cit. on p. 34).

[38] Nor Izyani Daud, Galoh Rashidah Haron, and Siti Suriyati Syd Othman, « Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor », *in*: *2017 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, IEEE, 2017, pp. 152–156 (cit. on p. 4).

[39] HLSRP De Silva et al., « Authdna: An adaptive authentication service for any identity server », *in*: *2019 International Conference on Advancements in Computing (ICAC)*, IEEE, 2019, pp. 369–375 (cit. on p. 47).

[40] Anind K Dey, « Context-aware computing: The CyberDesk project », *in*: *Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments*, AAAI Press Menlo Park, CA, 1998, pp. 51–54 (cit. on p. 2).

[41] Anind K Dey, « Understanding and Using Context », *in*: *Personal and ubiquitous computing* 5.*1* (2001), pp. 4–7 (cit. on p. 77).

[42] Anind Kumar Dey, *Providing architectural support for building context-aware applications*, Georgia Institute of Technology, 2000 (cit. on p. 3).

[43] Loan Thi Ngoc Dinh, Gour Karmakar, and Joarder Kamruzzaman, « A survey on context awareness in big data analytics for business applications », *in*: *Knowledge and Information Systems* 62 (2020), pp. 3387–3415 (cit. on p. 3).

[44] Periwinkle Doerfler et al., « Evaluating login challenges as a defense against account takeover », *in*: *The World Wide Web Conference*, 2019, pp. 372–382 (cit. on pp. 3, 113, 115).

[45] Ana I Segovia Domingo and Álvaro Martín Enríquez, « Digital Identity: the current state of affairs », *in*: *BBVA Research* 1.*0* (2018), pp. 1–46 (cit. on p. 22).

[46] Claudia Eckert, *IT-Sicherheit: Konzepte-Verfahren-Protokolle*, Germany: Walter de Gruyter, 2013 (cit. on p. 22).

[47] Jean-Marie Favre, Jacky Estublier, and Mireille Blay-Fornarino, *L'ingénierie dirigée par les modèles: au-delà du MDA*, Hermes-Lavoisier, 2006 (cit. on pp. 31, 33).

[48] David Freeman et al., « Who Are You? A Statistical Approach to Measuring User Authenticity. », *in*: *NDSS*, vol. 16, 2016, pp. 21–24 (cit. on pp. 2, 4, 49, 65, 108, 132, 137, 163, 166).

[49] Anthony Gavazzi et al., « A Study of Multi-Factor and Risk-Based Authentication Availability », *in*: *Usenix* (2021) (cit. on pp. 34, 204, 205).

[50] Samyama Gunjal GH and Samarth C Swamy, « A Security Approach to Build a Trustworthy Ubiquitous Learning System », *in*: *2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC)*, Karnataka, India: IEEE, 2020, pp. 1–6 (cit. on pp. 72, 86, 87, 89, 93, 94, 96, 122, 124).

[51] Kashif Habib and Wolfgang Leister, « Context-Aware Authentication for the Internet of Things », *in*: *The Eleventh International Conference on Autonomic and Autonomous Systems*, Rome, Italy: IEEE, 2015, pp. 134–139 (cit. on p. 65).

[52] Sven Hammann, Ralf Sasse, and David Basin, « Privacy-preserving openid connect », *in*: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, pp. 277–289 (cit. on p. 205).

[53] Albert Held, Sven Buchholz, and Alexander Schill, « Modeling of context information for pervasive computing applications », *in*: *Proceedings of SCI* (2002), pp. 167–180 (cit. on p. 2).

[54] Cormac Herley and Stuart E Schechter, « Distinguishing Attacks from Legitimate Authentication Traffic at Scale. », *in*: *NDSS*, 2019 (cit. on p. 4).

[55] Daniel Hintze et al., « CORMORANT: Ubiquitous risk-aware multi-modal biometric authentication across mobile devices », *in*: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3.*3* (2019), pp. 1–23 (cit. on p. 65).

[56] Kexin Hu and Zhenfeng Zhang, « Security analysis of an attractive online authentication standard: FIDO UAF protocol », *in*: *China Communications* 13.*12* (2016), pp. 189–198 (cit. on p. 50).

[57] Adam Hurkała and Jarosław Hurkała, « Architecture of context-risk-aware authentication system for web environments », *in*: *The Third International Conference on Informatics Engineering and Information Science* (2014) (cit. on pp. 4, 52).

[58] Syed Zulkarnain Syed Idrus et al., « A review on authentication methods », *in*: *Australian Journal of Basic and Applied Sciences* 7.*5* (2013), pp. 95–107 (cit. on pp. 22, 23).

[59] Georgios Kaiafas et al., « Detecting malicious authentication events trustfully », *in*: *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2018, pp. 1–6 (cit. on p. 48).

[60] Farzaneh Karegar et al., « Helping john to make informed decisions on using social login », *in*: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018, pp. 1165–1174 (cit. on pp. 54, 205).

[61] Dakshina Ranjan Kisku et al., « Human Identity Verification Using Multispectral Palmprint Fusion », *in*: *Journal of Signal and Information Processing* 3.*2* (2012), pp. 263–273 (cit. on pp. 88, 93–96).

[62] Christian Krupitzer et al., « FESAS IDE: An integrated development environment for autonomic computing », *in*: *2016 IEEE International Conference on Autonomic Computing (ICAC)*, IEEE, 2016, pp. 15–24 (cit. on p. 52).

[63] Katerina Ksystra et al., « Towards a methodology for formally analyzing federated identity management systems », *in*: *Leveraging Applications of Formal Methods, Verification and Validation. Practice: 11th International Symposium, ISoLA 2022, Rhodes, Greece, October 22–30, 2022, Proceedings, Part IV*, Springer, 2022, pp. 382–405 (cit. on p. 204).

[64] Abhilove Kumar and Apoorv Mishra, « Palm print Recognition using 2D Fourier Transformation and Integration Function », *in*: (2021) (cit. on pp. 85, 88, 93–96).

[65] Rajesh Kumar et al., « Continuous User Authentication via Unlabeled Phone Movement Patterns », *in*: *2017 IEEE International Joint Conference on Biometrics (IJCB)*, Denver, CO, USA: IEEE, 2017, pp. 177–184 (cit. on pp. 86, 88, 93, 94, 96, 123, 124).

[66] Nilesh A Lal, Salendra Prasad, and Mohammed Farik, « A review of authentication methods », *in*: *vol* 5 (2016), pp. 246–249 (cit. on p. 74).

[67] Wanpeng Li and Chris J Mitchell, « User access privacy in OAuth 2.0 and OpenID connect », *in*: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2020, pp. 664–6732 (cit. on p. 205).

[68] Joao Carlos D Lima, Cristiano C Rocha, Iara Augustin, et al., « A Context-Aware Recommendation System to Behavioral Based Authentication in Mobile and Pervasive Environments », *in*: *2011 IFIP 9th International Conference on Embedded and Ubiquitous Computing*, Melbourne, Australia: IEEE, 2011, pp. 312–319 (cit. on pp. 85, 86, 88, 89, 93–96, 122, 124).

[69] Xu Lin et al., « Phish in Sheep's Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting », *in*: *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1651–1668 (cit. on pp. 36, 201).

[70] Rolf Lindemann and Davit Baghdasaryan, *System and method for adaptive user authentication*, US Patent 10,706,132, July 2020 (cit. on p. 52).

[71] Meng Liu et al., « Exploring Deep Learning for Joint Audio-Visual Lip Biometrics », *in*: *arXiv preprint arXiv:2104.08510* (2021) (cit. on pp. 87, 93, 94, 96).

[72] Wei Liu, Xue Li, and Daoli Huang, « A survey on context awareness », *in*: *2011 International Conference on Computer Science and Service System (CSSS)*, IEEE, 2011, pp. 144–147 (cit. on p. 2).

[73] Zhan Liu, Riccardo Bonazzi, and Yves Pigneur, « Privacy-based adaptive context-aware authentication system for personal mobile devices », *in*: *Journal of mobile multimedia* (2016), pp. 159–180 (cit. on p. 53).

[74] Sihua Ma et al., « Using Blockchain to Build Decentralized Access Control in a Peer-to-Peer E-Learning Platform », PhD thesis, Saskatchewan: University of Saskatchewan, 2018 (cit. on pp. 72, 86–88, 94, 96).

[75] Eve Maler and Drummond Reed, « The venn of identity: Options and issues in federated identity management », *in*: *IEEE security & privacy* 6.*2* (2008), pp. 16–23 (cit. on p. 2).

[76] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone, *Handbook of applied cryptography*, na: CRC press, 2018 (cit. on p. 22).

[77] Markus Miettinen et al., « Revisiting context-based authentication in IoT », *in*: *Proceedings of the 55th Annual Design Automation Conference*, 2018, pp. 1–6 (cit. on p. 65).

[78] Grzergor Milka, « Anatomy of Account Takeover », *in*: *Enigma 2018 (Enigma 2018)*, Santa Clara, CA: USENIX Association, Jan. 2018, URL: https://www.usenix.org/node/208154 (cit. on p. 44).

[79] Leslie C Milton and Atif Memon, « Intruder Detector: A Continuous Authentication Tool to Model User Behavior », *in*: *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, USA: IEEE, 2016, pp. 286–291 (cit. on pp. 73, 86, 88, 93, 94, 96).

[80] AH Mir, S Rubab, and ZA Jhat, « Biometrics verification: a literature survey », *in*: *International Journal of Computing and ICT Research* 5.*2* (2011), pp. 67–80 (cit. on p. 73).

[81] Omid Mir, Michael Roland, and René Mayrhofer, « Decentralized, privacy-preserving, single sign-on », *in*: *Security and Communication Networks* 2022 (2022), pp. 1–18 (cit. on p. 205).

[82] Moeiz Miraoui and Sherif El-etriby, « A Context-Aware Authentication Approach for Smartphones », *in*: *2019 International Conference on Computer and Information Sciences (ICCIS)*, Aljouf, Kingdom of Saudi Arabia: IEEE, 2019, pp. 1–5 (cit. on pp. 84, 88, 94, 95, 121, 124).

[83] Ian Molloy et al., « Risk-based security decisions under uncertainty », *in*: *Proceedings of the second ACM conference on Data and Application Security and Privacy*, 2012, pp. 157–168 (cit. on p. 4).

[84] Christoph Molnar, *Interpretable machine learning*, Lulu. com, 2020 (cit. on pp. 130–133, 135, 136, 139).

[85] Srivathsan G Morkonda, Sonia Chiasson, and Paul C van Oorschot, « SSOPrivateEye: Timely Disclosure of Single Sign-On Privacy Design Differences », *in*: *arXiv preprint arXiv:2209.04490* (2022) (cit. on p. 205).

[86] Srivathsan G Morkonda, Paul C van Oorschot, and Sonia Chiasson, « Exploring privacy implications in OAuth deployments », *in*: *arXiv preprint arXiv:2103.02579* (2021) (cit. on p. 51).

[87] Robert Morris and Ken Thompson, « Password security: A case history », *in*: *Communications of the ACM* 22.*11* (1979), pp. 594–597 (cit. on pp. 1, 4).

[88] Bruno A Mozzaquatro, Ricardo Jardim-Goncalves, and Carlos Agostinho, « Situation Awareness in the Internet of Things », *in*: *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Madeira Island, Portugal: IEEE, 2017, pp. 982–990 (cit. on pp. 88, 93–95).

[89] Jalal Al-Muhtadi et al., « A lightweight cyber security framework with context-awareness for pervasive computing environments », *in*: *Sustainable Cities and Society* 66 (2021), p. 102610 (cit. on pp. 87, 93–96).

[90] Brahim En-Nasry and Mohamed Dafir Ech-Cherif El Kettani, « Towards an open framework for mobile digital identity management through strong authentication methods », *in*: *FTRA International Conference on Secure and Trust Computing, Data Management, and Application*, Springer, 2011, pp. 56–63 (cit. on pp. 88, 93–96).

[91] Natalia Neverova et al., « Learning Human Identity from Motion Patterns », *in*: *IEEE Access* 4 (2016), pp. 1810–1820 (cit. on pp. 86, 88, 93–96).

[92] Lily Hay Newman, *Facebook Will Force More At-Risk Accounts to Use Two-Factor*, 2021 (cit. on p. 44).

[93] Lawrence O'Gorman, « Comparing passwords, tokens, and biometrics for user authentication », *in*: *Proceedings of the IEEE* 91.*12* (2003), pp. 2021–2040 (cit. on p. 3).

[94] Aleksandr Ometov et al., « Multi-factor authentication: A survey », *in*: *Cryptography* 2.*1* (2018), p. 1 (cit. on p. 34).

[95] Sarah Pearman et al., « Let's go in for a closer look: Observing passwords in their natural habitat », *in*: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 295–310 (cit. on p. 33).

[96] Esther Perumal and Shanmugalakshmi Ramachandran, « A Multimodal Biometric System Based on Palmprint and Finger Knuckle Print Recognition Methods. », *in*: *International Arab Journal of Information Technology (IAJIT)* 12.*2* (2015), pp. 118–128 (cit. on pp. 86, 88, 93–96).

[97] Kai Petersen, Sairam Vakkalanka, and Ludwik Kuzniarz, « Guidelines for conducting systematic mapping studies in software engineering: An update », *in*: *Information and Software Technology* 64 (2015), pp. 1–18 (cit. on pp. 61–63).

[98] Kai Petersen et al., « Systematic mapping studies in software engineering », *in*: *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*, 2008, pp. 1–10 (cit. on p. 70).

[99] Yutthana Pititheeraphab et al., « Vein Pattern Verification and Identification Based on Local Geometric Invariants Constructed from Minutia Points and Augmented with Barcoded Local Feature », *in*: *Applied Sciences* 10.*9* (2020), p. 3192 (cit. on pp. 88, 94–96).

[100] Martin F Porter, « An algorithm for suffix stripping », *in*: *Program* 14.*3* (1980), pp. 130–137 (cit. on p. 70).

[101] Arun Ramakrishnan et al., « PRISM: Policy-Driven Risk-Based Implicit Locking for Improving the security of Mobile End-User Devices », *in*: *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia*, Brussels, Belgium: ACM, 2015, pp. 365–374 (cit. on pp. 86, 88, 89, 93–96).

[102] Oriana Riva et al., « Progressive authentication: deciding when to authenticate on mobile phones », *in*: *21st USENIX Security Symposium (USENIX Security 12)*, 2012, pp. 301–316 (cit. on p. 65).

[103] Martiño Rivera-Dourado et al., « An Analysis of the Current Implementations Based on the WebAuthn and FIDO Authentication Standards », *in*: *Engineering Proceedings* 7.*1* (2021), p. 56 (cit. on p. 50).

[104] Antonio Robles-González, Patricia Arias-Cabarcos, and Javier Parra-Arnau, « Privacy-Centered Authentication: a new Framework and Analysis », *in*: *Computers & Security* (2023), p. 103353 (cit. on p. 3).

[105] Joseph Roth, Xiaoming Liu, and Dimitris Metaxas, « On Continuous User Authentication via Typing Behavior », *in*: *IEEE Transactions on Image Processing* 23.*10* (2014), pp. 4611–4624 (cit. on pp. 86, 88, 93–96).

[106] Shahla Saedi and Nasrollah Moghadam Charkari, « Characterization of palmprint using discrete orthonormal s-transform », *in*: *2011 International Conference on Hand-Based Biometrics*, na: IEEE, 2011, pp. 1–6 (cit. on pp. 88, 94–96).

[107] Daniel Salber, Anind K Dey, and Gregory D Abowd, « The context toolkit: Aiding the development of context-enabled applications », *in*: *Proceedings of the SIGCHI conference on Human factors in computing systems*, 1999, pp. 434–441 (cit. on p. 3).

[108] GH Samyama Gunjal, Pallapa Venkataram, and G Narendra Kumar, « A Context-Based User Authentication Scheme for Ubiquitous Services », *in*: *Proceedings of the World Congress on Engineering and Computer Science*, vol. 1, na: na, 2014, na (cit. on pp. 86, 88, 93, 94, 96).

[109] Bill Schilit, Norman Adams, and Roy Want, « Context-aware computing applications », *in*: *1994 first workshop on mobile computing systems and applications*, IEEE, 1994, pp. 85–90 (cit. on p. 2).

[110] Bill N Schilit and Marvin M Theimer, « Disseminating active map information to mobile hosts », *in*: *IEEE network* 8.*5* (1994), pp. 22–32 (cit. on p. 3).

[111] Edwin Seidewitz, « What models mean », *in*: *IEEE software* 20.*5* (2003), pp. 26–32 (cit. on pp. 30, 31).

[112] David Silver et al., « Password managers: Attacks and defenses », *in*: *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014, pp. 449–464 (cit. on p. 2).

[113] Max Smith-Creasey and Muttukrishnan Rajarajan, « A novel scheme to address the fusion uncertainty in multi-modal continuous authentication schemes on mobile devices », *in*: *2019 International Conference on Biometrics (ICB)*, IEEE, 2019, pp. 1–8 (cit. on p. 178).

[114] Jesus Solano et al., « Risk-based Static Authentication in Web Applications with Behavioral Biometrics and Session Context Analytics », *in*: *International Conference on Applied Cryptography and Network Security*, Bogotá, Colombia: Springer, 2019, pp. 3–23 (cit. on pp. 88, 93–96).

[115] San-Tsai Sun et al., « What makes users refuse web single sign-on? An empirical investigation of OpenID », *in*: *Proceedings of the seventh symposium on usable privacy and security*, 2011, pp. 1–20 (cit. on p. 205).

[116] Nikola Tarashev, Kostas Tsatsaronis, and Claudio Borio, « Risk attribution using the Shapley value: Methodology and policy applications », *in*: *Review of Finance* 20.*3* (2016), pp. 1189–1213 (cit. on pp. 133, 135).

[117] Wafa El-Tarhouni, « Finger Knuckle Print and Palmprint for Efficient Person Recognition », PhD thesis, Northumbria: Northumbria University, 2017 (cit. on pp. 88, 93–96).

[118] Songpon Teerakanok, Tetsutaro Uehara, and Atsuo Inomata, « Migrating to zero trust architecture: Reviews and challenges », *in*: *Security and Communication Networks* 2021 (2021), pp. 1–10 (cit. on p. 35).

[119] Issa Traore et al., « Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments », *in*: *2012 fourth international conference on digital home*, IEEE, 2012, pp. 138–145 (cit. on p. 108).

[120] Javier Troya et al., « Uncertainty representation in software models: a survey », *in*: *Software and Systems Modeling* 20.*4* (2021), pp. 1183–1213 (cit. on pp. 101, 102).

[121] Vincent Unsel et al., « Risk-Based Authentication for OpenStack: A Fully Functional Implementation and Guiding Example », *in*: *arXiv preprint arXiv:2303.12361* (2023) (cit. on p. 199).

[122] José María Jorquera Valero et al., « Machine Learning as an Enabler of Continuous and Adaptive Authentication in Multimedia Mobile Devices », *in*: *Handbook of Research on Multimedia Cyber Security*, IGI Global, 2020, pp. 21–47 (cit. on pp. 48, 178).

[123] Ignacio Velásquez, Angélica Caro, and Alfonso Rodríguez, « Kontun: A Framework for recommendation of authentication schemes and methods », *in*: *Information and Software Technology* 96 (2018), pp. 27–37 (cit. on pp. 3, 113, 115).

[124] Ding Wang et al., « The request for better measurement: A comparative evaluation of two-factor authentication schemes », *in*: *Proceedings of the 11th ACM on Asia conference on computer and communications security*, 2016, pp. 475–486 (cit. on pp. 113, 115).

[125] James E Weber et al., « Weak password security: An empirical study », *in*: *Information Security Journal: A Global Perspective* 17.*1* (2008), pp. 45–54 (cit. on p. 4).

[126] Maximilian Westers et al., « SSO-Monitor: Fully-Automatic Large-Scale Landscape, Security, and Privacy Analyses of Single Sign-On in the Wild », *in*: *arXiv preprint arXiv:2302.01024* (2023) (cit. on p. 205).

[127] Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono, « What's in Score for Website Users: A Data-driven Long-term Study on Risk-based Authentication Characteristics », *in*: *arXiv preprint arXiv:2101.10681* (2021) (cit. on pp. 34, 145, 152).

[128] Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono, « More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication », *in*: *Annual Computer Security Applications Conference*, 2020, pp. 203–218 (cit. on pp. 3, 35, 113, 132, 163).

[129] Stephan Wiefling, Luigi Lo Iacono, and Markus Dürmuth, « Is this really you? An empirical study on risk-based authentication applied in the wild », *in*: *IFIP International Conference on ICT Systems Security and Privacy Protection*, Springer, 2019, pp. 134–148 (cit. on pp. 2, 4, 35, 44, 65, 119, 132, 133, 163).

[130] Stephan Wiefling, Jan Tolsdorf, and Luigi Lo Iacono, « Privacy Considerations for Risk-Based Authentication Systems », *in*: *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2021, pp. 320–327 (cit. on pp. 3, 53, 205).

[131] Stephan Wiefling et al., « Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service », *in*: *ACM Transactions on Privacy and Security* 26.*1* (2022), pp. 1–36 (cit. on pp. 3, 35, 155).

[132] Yvonne Wilson and Abhishek Hingnikar, « OpenID Connect », *in*: *Solving Identity Management in Modern Applications: Demystifying OAuth 2, OpenID Connect, and SAML 2*, Springer, 2022, pp. 103–126 (cit. on p. 51).

[133] Heiko Witte, Christian Rathgeb, and Christoph Busch, « Context-Aware Mobile Biometric Authentication Based on Support Vector machines », *in*: *2013 Fourth International Conference on Emerging Security Technologies*, Cambridge, United Kingdom: IEEE, 2013, pp. 29–32 (cit. on pp. 85, 87, 93, 94, 96).

[134] Zhiyi Zhang et al., « EL PASSO: efficient and lightweight privacy-preserving single sign on », *in*: *Proceedings on Privacy Enhancing Technologies* 2021.*2* (2021), pp. 70–87 (cit. on p. 205).

[135] Liang Zhao, « Event prediction in the big data era: A systematic survey », *in*: *ACM Computing Surveys (CSUR)* 54.*5* (2021), pp. 1–37 (cit. on p. 151).

[136] Verena Zimmermann and Nina Gerber, « The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes », *in*: *International Journal of Human-Computer Studies* 133 (2020), pp. 26–44 (cit. on p. 3).

[137] Verena Zimmermann[1] et al., « The quest to replace passwords revisited–rating authentication schemes », *in*: *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)*, Lulu. com, 2018, p. 38 (cit. on p. 3).

COLLEGE DOCTORAL BRETAGNE
MATHS, TELECOMS
INFORMATIQUE, SIGNAL
SYSTEMES, ELECTRONIQUE

Université de Rennes

Titre : Au-delà des Scores de Risque : Authentification Adaptative Tenant Compte du Contexte

Mot clés : Authentification adaptative, contexte, score de risque, modèles, mots de passe, utilisateur

Résumé : L'***Authentification Adaptative (AA)*** permet à un système de **sélectionner dynamiquement la ou les méthodes les plus appropriées** pour authentifier un utilisateur en fonction d'informations contextuelles, telles que la localisation, et l'adresse IP.

Toutefois, il est difficile de raisonner sur la pertinence de la ou des méthodes d'authentification en fonction des informations contextuelles, lorsque le choix porte sur multiples dimensions telles que la sécurité et l'expérience utilisateur. De nombreuses initiatives universitaires ont été lancées pour remplacer les mots de passe et exploiter les informations contextuelles afin d'adapter la ou les méthodes d'authentification demandées à l'utilisateur. Ces initiatives se concentrent sur l'utilisation des informations contextuelles pour calculer des scores de risque. Des méthodes d'authentification supplémentaires sont alors requises si un certain niveau de risque est détecté. Compte tenu de la diversité des impacts en terme de sécurité, expérience de l'utilisateur, déployabilité, et respect de la vie privée, les scores de risque sont des indicateurs trop simples de l'adéquation des méthodes d'authentification. Le raisonnement sur la pertinence des méthodes d'authentification nécessite une compréhension fine de la situation contextuelle (*e.* type de risque encouru, contraintes d'utilisation dans des environnements spécifiques).

Ma recherche vise ainsi à exploiter les informations contextuelles au-delà du calcul des scores de risque pour fournir un raisonnement plus fin sur l'adéquation des méthodes d'authentification. L'objectif est donc d'améliorer la conception, le déploiement et l'évaluation des systèmes d'authentification adaptatifs.

Dans cette thèse, j'apporte quatre contributions majeures. Premièrement, je propose une **étude de la litérature centré sur la modélisation des informations contextuelles pour les systèmes d'authnetification** afin de modéliser l'ensemble des informations contextuelles. J'analyse la manière dont la modélisation du contexte pour les systèmes d'authentification adaptatifs est effectuée et je détermine les propriétés souhaitées du modèle d'information contextuelle pour les systèmes d'authentification adaptatifs. Je démontre la capacité à capturer un ensemble commun de caractéristiques contextuelles pertinentes pour les systèmes d'authentification adaptatifs indépendamment du domaine d'application, et je souligne que malgré la possibilité d'un cadre unifié, il n'existe pas de norme pour la modélisation du contexte pour les systèmes d'AA.

Deuxièmement, je présente un **framework de modélisation de contexte pour les décisions d'authentification dynamique (CoFrA)**, dans lequel les informations contextuelles spécifient l'adéquation de la (des) méthode(s) d'authentification au-delà du calcul des scores de risque et en ce qui concerne les propriétés de sécurité, d'utilisabilité, de confidentialité et de déployabilité. CoFrA est un métamodèle précis, réutilisable et extensible qui caractérise le domaine de l'AA et fournit un langage permettant de déterminer la ou les méthodes d'authentification appropriées dans un contexte donné.

Troisièmement, je propose un **modèle d'explicabilité basé sur les valeurs de Shapley** qui peut être utilisé pour expliquer les scores de risque qui sont estimés avec des approches basées sur les scores afin de soutenir la transition des approches basées sur les scores vers une approche d'AA plus fine.

Je montre que les risques peuvent être expliqués différemment et spécifiquement pour chaque tentative de connexion de l'utilisateur. Ce modèle d'explicabilité peut donc améliorer efficacement notre compréhension des risques. Les explications générées peuvent être utilisées pour raisonner sur l'adéquation des méthodes d'authentification en fonction de la sécurite, l'éxpérience de l'utilisateur, la deployabilité, et la protection de la vie privée pour chaque tentative de connexion de l'utilisateur, en tenant compte d'autres informations que le seul score de risque. Plus précisément, les explications peuvent être utilisées dans mon cadre CoFrA pour raisonner sur l'adéquation des méthodes d'authentification en utilisant efficacement ces informations.

Quatrièmement, je présente une **approche outillée pour la définition des modèles d'authentification les mieux adaptés**. CoFrA fournit un langage pour déterminer les modèles d'authentification adaptatifs. Pour une application, il peut y avoir plusieurs modèles valides, et la difficulté est de choisir celui qui convient à l'application en fonction de multiples critères de qualité. Ma quatrième contribution soutient ce choix. L'approche d'évaluation que je propose guide les praticiens et les chercheurs en authentification dans le processus d'évaluation et de comparaison des modèles CoFrA afin de définir le modèle le mieux adapté à des applications spécifiques.

Je valide les propositions de cette thèse par des études de cas et sur la base d'échanges approfondis avec des experts en authentification et en modélisation.

Cette thèse aborde les lacunes de l'utilisation exclusive des scores de risque pour déterminer l'adéquation des méthodes d'authentification. Les contributions de cette thèse visent ainsi à améliorer la conception, le déploiement et l'évaluation des systèmes d'authentification adaptatifs via raisonnement fin sur l'adéquation des méthodes d'authentification, au-delà du calcul des scores de risque. Les résultats de cette thèse permettent aux développeurs, aux administrateurs et aux chercheurs de créer des solutions AA efficaces et de soutenir une adoption généralisée dans la pratique.

Title: Beyond Risk Scores: Context-Aware Adaptive Authentication

Keywords: Adaptive Authentication, Context, Risk Score, Risk-Based Authentication, Models, Passwords, User

Abstract: ***Adaptive Authentication (AA)*** allows a system to **dynamically select the appropriate method(s)** for a user depending on contextual information, such as location, IP address, and other attributes. However, reasoning about the appropriateness of authentication method(s) (*e.g.,* for security and usability) according to the contextual information is challenging. In recent years, there have been many academic initiatives to replace passwords, and to leverage context information to adjust the authentication method(s) to request. These initiatives focus on using context information to calculate risk scores. Additional authentication method(s) are then required if a certain risk level is detected. However, given the diversity of concerns (*e.g.,* security, usability, deployability, privacy), risk scores used as proxies of the appropriateness of authentication methods are too simple. Reasoning about the appropriateness of authentication methods requires a fine-grained understanding of the contextual situation (*e.g.,* type of risk faced, usability constraints in specific environments). Motivated by the need to improve the design, deployment, and evaluation of AA systems, my research aims to leverage context information beyond the calculation of risk scores to provide a more fine-grained reasoning about the appropriateness of authentication method(s).

In this dissertation, I provide four major

contributions. First, I propose a **structured review of the literature to date on Context Modeling for Adaptive Authentication systems (CM4AA)**. This review helps to understand the representation of context information with appropriate and well-designed models. I analyze how context modeling for AA systems is performed and determine desired properties of the context information model for AA systems. I demonstrate the ability to capture a common set of contextual features relevant to AA systems independently from the application domain, and I emphasize that despite the possibility of a unified framework, no standard for CM4AA exists.

Second, I present a tool-supported **Context-driven Modeling Framework for dynamic Authentication decisions (CoFrA)**, where the context information specifies the appropriateness of authentication method(s) beyond the calculation of risk scores while considering the security, usability, privacy, and deployability properties. CoFrA is a precise, reusable, and extensible metamodel that characterizes the domain of AA and provides a language to determine the appropriate authentication method(s) in a given context.

Third, I propose an **explainability model based on Shapley values** that can be used to explain risk scores that are estimated with score-based approaches to support the transition from score-based approaches to a more fine-grained AA approach. I show that the risks can be explained differently and specifically for each user login attempt. Hence, this explainability model can effectively improve our understanding of risks. The explanations generated can be used to reason on the appropriateness of authentication methods for each user login attempt while considering more information than just the risk score. More specifically, these explanations can be used within my CoFrA framework to reason on the appropriateness of authentication methods using efficiently this information.

Fourth, I present a **tooled approach for the definition of the most well-suited authentication models**. CoFrA provides a language to determine AA models. For an application, there may be several valid models, and the difficulty is to choose the one that fits the application according to multiple quality criteria. This contribution supports this choice. The evaluation approach that I propose guides authentication practitioners and researchers in the process of evaluating and comparing CoFrA models to define the most well-suited model for specific applications.

All the four contributions of this thesis have been validated rigorously through case studies and extensive exchanges with authentication and modeling experts.

In summary, this dissertation addresses the shortcomings of exclusively using risk scores to determine the appropriateness of authentication methods. The contributions of this thesis aim to improve the design, deployment and evaluation of AA systems by handling a fine-grained reasoning about the appropriateness of authentication methods, beyond the calculation of risk scores. The results of this thesis further enable developers, administrators, and researchers to create efficient AA solutions and support a widespread adoption in practice.