Security in cloud computing

Ahmed Lounis

▶ **To cite this version:**

Ahmed Lounis. Security in cloud computing. Other. Université de Technologie de Compiègne, 2014. English. NNT : 2014COMP1945 . tel-01293631

HAL Id: tel-01293631

https://theses.hal.science/tel-01293631v1

Submitted on 25 Mar 2016

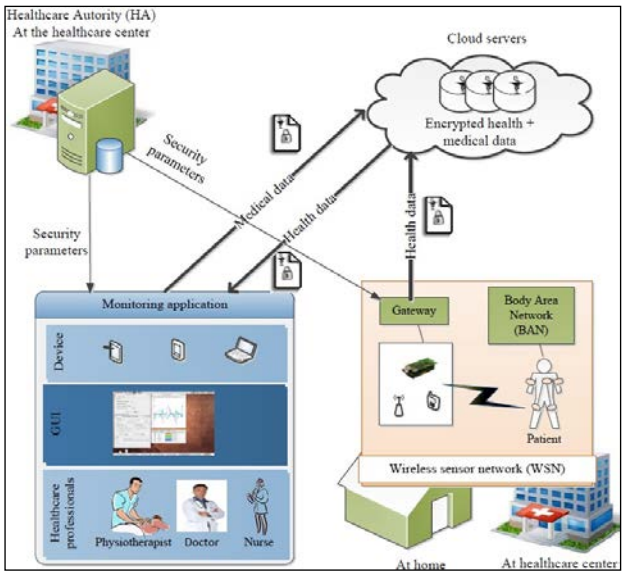
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Par **Ahmed LOUNIS**

Security in cloud computing

Thèse présentée pour l'obtention du grade de Docteur de l'UTC



Soutenue le 03 juillet 2014
Spécialité : Technologies de l'Information et des Systèmes

D1945

Université de Technologie de Compiègne

École doctorale UTC

Security in cloud computing

THÈSE

présentée et soutenue publiquement le **03 Juillet 2014**

pour l'obtention du

Doctorat de l'Université de Technologie de Compiègne

Spécialité : Technologie de l'information et des systèmes

par

Ahmed Lounis

Composition du jury

Président :	Aziz Moukrim	Professeur, UTC
Rapporteurs :	Ahmed Serhrouchni	Professeur, Télécom ParisTech
	Mohammed Naimi	Professeur, Université de Cergy-Pontoise
Examinateurs :	Myoupo Jean Frederic	Professeur, Université de Picardie, Amiens
	Romain Laborde	Maître de conférences, Université Paul Sabatier, Toulouse
	Hani Ragab Hassen	Maître de conférences, Université de Robert Gordon, UK
Directeurs :	Abdelmadjid Bouabdallah	Professeur, UTC
	Yacine Challal	Maître de conférences HDR, UTC

Heudiasyc UMR CNRS 7253, Université de Technologie de Compiègne
Centre de Recherches de Royallieu, BP 20529 - 60205 COMPIEGNE cedex-France

Remerciements

J'adresse du fond du cœur tous mes remerciements à mes deux encadreurs Abdelmadjid Bouabdallah, Professeur à l'Université de Technologie de Compiègne (UTC), et Yacine Challal, maitre de conférences à l'UTC, de m'avoir donné la possibilité de mener à bien cette thèse. Je les remercier notamment pour leurs précieux conseils et encouragements tout au long de ma thèse.

Je remercie Aziz Moukrim, Professeur à l'Université de Technologie de Compiègne, de m'avoir fait l'honneur de présider le jury de thèse.

Je remercie Ahmed Serhrouchni, Professeur à Télécom ParisTech, et Mohammed Naimi, Professeur à l'Université de Cergy-Pontoise, d'avoir accepté d'être rapporteur de ma thèse. Je les remercie également, ainsi que Myoupo Jean Frederic, Professeur à l'Université de Picardie, et Romain Laborde, Maître de conférences à l'Université Paul Sabatier, de m'avoir fait l'honneur de participer au jury de thèse.

Je remercie Hani Ragab Hassen, maitre de conférence à l'Université Robert Gordon UK, pour son aide et ses précieux conseils.

Je voudrais aussi remercier mes collègues de laboratoire HEUDIASYC, qui par leurs conseils et encouragement, ont contribué à l'aboutissement de ce travail. Je remercie Abdelkrim Hadjidj, Marion Souil, Walid Bechkit, Tifenn Rault et Nourhene Maalel.

Mes plus profonds remerciements vont à mes parents. Tout au long de mon cursus, ils m'ont toujours soutenu, encouragé et aidé. Je remercie également toute ma famille pour leur soutien durant cette thèse, et ma fiancée, pour son aide, son écoute et sa patience.

Citation

L'art de la réussite consiste à savoir s'entourer des meilleurs.
John Fitzgerald Kennedy

Abstract

Cloud computing has recently emerged as a new paradigm where resources of the computing infrastructures are provided as services over the Internet. However, this paradigm also brings many new challenges for data security and access control when business or organizations data is outsourced in the cloud, they are not within the same trusted domain as their traditional infrastructures.

This thesis contributes to overcome the data security challenges and issues due to using the cloud for critical applications. Specially, we consider using cloud storage services for medical applications such as Electronic Health Record (EHR) systems and medical Wireless Sensor Networks. First, We discuss the benefits and challenges of using cloud services for healthcare applications. Then, we study security risks of the cloud, and give an overview on existing works. After that, we propose a secure and scalable cloud-based architecture for medical applications. In our solution, we develop a fine-grained access control in order to tackle the challenge of sensitive data security, complex and dynamic access policies. Finally, we propose a secure architecture for emergency management to meet the challenge of emergency access.

Keywords : cloud computing, e-health, wireless sensor networks, sensitive data, security, fine-grained access control, attribute based encryption, confidentiality, privacy

——————————————————————— Liste publications ———————————————————————

Publications list

- Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, Yacine Challal : Secure Medical Architecture on the Cloud Using Wireless Sensor Networks for Emergency Management. BWCCA 2013
- Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, Yacine Challal : Secure and Scalable Cloud-Based Architecture for e-Health Wireless Sensor Networks. ICCCN 2012
- Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, Yacine Challal : Healing on the Cloud : Secure Cloud Architecture for Medical Wireless Sensor Networks. Future Generation Comp. Syst (under review).

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction

1.1 Introduction

Cloud computing has recently emerged as new paradigm for hosting and delivering computing services and data over the Internet. The cloud computing is an on-demand and self-service access to dynamic scalable and pooled computing resources (high computing power, massive storage space, etc.) through communication networks. In addition, the cloud offers the ability to elastically tune resources both up and down as needed without human interaction with. The business and infrastructure benefits of using the cloud for storage and application building/deployment are quite attractive to the vast majority of businesses and organizations. Main advantages of moving to the cloud include cost savings, revenue growth and accessibility (from anywhere and at any time). These advantages are attractive for healthcare providers as well.

Wireless Sensor Networks (WSNs) are promising technologies that has recently significant success in healthcare. Recent advances in WSNs have made it possible to deploy wearable sensors on patient's body in/out hospital. This allows continuous monitoring of physiological signals (such as ECG, blood oxygen levels) and other health related information (such as physical activity levels). The major breakthrough of this technology is the provision of continuous remote patient supervision both in and out of hospital conditions. This reduces healthcare cost and improves the life-quality of patients as well as the treatment efficiency.

Medical WSNs provide great opportunities, but it brings several challenges. Indeed, Medical WSNs require high and continuous sampling rates which results in high volume of data. The data should be collected and sent to the base station in order to be stored and analyzed. Furthermore, this data is typically required to be stored for several years, which requires scalable storage capacity at the base-station. Moreover, medical data could be lifesaving and must be available at any time and from everywhere. For this reason, new innovative solutions are strongly required to meet the great challenges of handling the exponential growth in data generated by sensors. Another challenge we tackle is the confidentiality of collected medical data. Considering social, ethical and legal aspects of medical systems, data collected by sensor networks are highly sensitive and should be managed properly to guarantee patients' privacy. This is why, several countries have defined data protection laws for privacy protection. These laws differ from one country to another, but their primary goal should be to ensure adoption and enforcement of *Fair Information Practices (FIP)* [FIP] that are the basis for privacy protection around the world.

The cloud has become the paradigm of a large-scale data oriented systems which is suitable for medical applications. In addition, when medical data is stored in the cloud, healthcare staff can collect, share and access to this data from anywhere and at anytime. Moreover, the cloud provides complete accessibility with an expanded range of access devices such as PCs, network of computers, smart-phones and network-enabled medical devices. Consequently, These make collaboration easier between healthcare staff in order to provide adequate healthcare services and

avoid unnecessary redundant tasks. In addition, the mobility provided by the cloud enables healtcare providers to ensure fast and appropriate interventions, that have more effect on lifesaving, particularly for emergency interventions.

To take advantages of the cloud, the healthcare providers need to outsource their infrastructures and storage from their environment to a third-party cloud service provider. This lets them focus completely on their real activity, which is providing healthcare services. However, there are several barriers to adopt the cloud for medical applications due to their critical nature. These barriers concern mainly health data security and patients privacy. Since data handled by medical applications is highly sensitive, it may includes information about patient's health state and personal information about patients. Hence, unauthorized disclosure of this information can result in privacy violation, embarrassment and/or illegal exploit of this information. In addition, the cloud is usually considered as untrusted environment (which may be located outside the country that involves others regulations). For this reason, security risk becomes an obstacle for adoption of the cloud by healthcare providers, where confidentiality of medical data and users' privacy are threatened.

Access control is the mechanism used to protect medical data against unauthorized access. In case of Electronic Medical Records (EMR), access to medical data is often governed by complex policies that distinguish between each part of data and each user privileges, these policies are implemented and enforced by healthcare providers. Various techniques have been developed to implement fine-grained access control, which allows flexibility in specifying differential access rights of individual users. Traditional access control rely on a trusted server to mediate access in order to protect files. However, when the centralized server is not enough trusted and/or data stored is highly sensitive, we need a cryptographic access control which relies exclusively on cryptography to provide confidentiality and integrity of data managed by the system. It is particularly designed to operate in untrusted environments where the lack of global knowledge and control are defining characteristics. One critical issue with this approach is how to achieve the desired security goals without introducing a high complexity on key management and data encryption.

1.2 Contributions

This thesis contributes to overcome the data security challenges and issues due to using the cloud for critical applications. Specifically, we consider using the cloud storage for medical applications such as EMR systems and medical Wireless Sensor Networks. Without loss of generality, our proposed solutions for medical applications are also viable for any other critical applications that face the same considered challenges. In what follows, we describe our contributions.

1.2.1 Cloud computing for healthcare : benefits and risks

In our first contribution, we identify the benefits and risks of using the cloud for medical applications (specifically, medical wireless sensor networks) with a key focus on security and privacy issues. We will start by briefly giving cloud definitions and concepts. Then, we present e-health, by giving advantages of communication and technologies in healthcare area. Finally, we give advantages and challenges brought by adopting the cloud for medical applications.

1.2.2 Data security concepts, issues and challenges in cloud computing

As previously explained, security risks are major barriers for adopting the cloud for critical applications. In this contribution, we investigate how to make the cloud more secure for medical applications. First, we present briefly some security concepts related to our work in this thesis. After that, we focus on advanced cryptography methods, especially Attribute Based Encryption (ABE). Recently, this method has been gaining considerable attention as a useful technology for safe and secure storage of data on the cloud. However, ABE needs to be more developed and extended for its successful integration in piratical systems. Then, we study many ABE related

works. We organize our study in several points, each point represents an extension of ABE. Then, we address the challenge of secure data outsourcing in cloud computing. In which, we give some security threats of data outsourcing. Then, we present traditional access control that cannot resolve this problem. After that, we study cryptographic access control and related existing works. Finally, we describe other aspects of data security in the cloud computing.

1.2.3 Cloud-based architecture for medical applications

In this contribution, we address the challenge of data management in wireless sensor networks for patient supervision. We propose a secure and scalable architecture that leverages cloud computing technology to dynamically scale storage resources via on demand provisioning. Furthermore, we propose an innovative security scheme that eliminates potential security threats of medical data outsourcing and guarantees confidentiality, integrity without involving patients or doctors interventions. To implement complex and dynamic security policies necessary to medical application, we develop a fine-grained access control that combines ciphertext-policy attributes based encryption and symmetric cryptography. This combination reduces the management overhead and the encryption/decryption time as we will show by our performance evaluation. Finally, we carry out extensive simulations which shows that our scheme provides an efficient, fine-grained and scalable access control.

1.2.4 Secure medical architecture on the cloud using wireless sensor networks for emergency management

WSNs for medical applications provide useful and real information about patients' health state. This information should be available for healthcare providers to facilitate response and to improve the rescue process of a patient during emergency. In the previous contribution, we have proposed an innovative cloud-based architecture for collecting and accessing large amount of data generated by medical sensor networks. Also, we have integrated CP-ABE for providing a secure fine-grained access control over medical data outsourced on the cloud. However, for emergency

management, integrating CP-ABE creates particular challenges for providing temporary access victims medical data when this is needed. In this contribution we present our architecture for secure emergency management in healthcare area. We address the challenge of ABE integrating for providing temporary access victims medical data in emergency situation. In addition, we use wireless sensor network (WSN) technology to provide early emergency detection.

1.3 Organization of the manuscript

The rest of this thesis is organized as follows. In chapter 2, we highlight benefits and challenges due to use of cloud for medical applications, with a key focus on security challenges. In section 3, we present a study of existing works in the field of data security and confidentiality in untrusted environments in order to identify drawbacks that need to be tackled. In Chapter 4, we propose our secure and scalable storage architecture for medical applications. In chapter 5, we describe our secure cloud-based solution to provide emergency management by using medical wireless sensor networks. In chapter 6, we end-up this work with some concluding remarks and we highlight the main future work directions and open issues.

Chapitre 2

Cloud computing for healthcare : benefits and risks

2.1 Introduction

Cloud computing has recently emerged as a new paradigm for hosting and delivering computing services and data over the Internet. The cloud computing is an on-demand and self-service access to dynamic scalable and pooled computing resources (high computing power, massive storage space, etc.) through communication networks. In addition, the cloud offers the ability to elastically tune resources both up and down as needed without human interaction. The business and infrastructure benefits of using the cloud for storage and application building/deployment are quite attractive to the vast majority of businesses and organizations. Main advantages of moving to the cloud include cost savings, revenue growth and accessibility

(from anywhere and at any time). These advantages are attractive for healthcare providers as well.

Wireless Sensor Networks (WSNs) are promising technologies that has recently significant success in healthcare. Recent advances in WSNs have made it possible to deploy wearable sensors on patient's body in/out hospital. This allows continuous monitoring of physiological signals (such as ECG, blood oxygen levels) and other health related information (such as physical activity levels). The major breakthrough of this technology is the provision of continuous remote patient supervision both in and out of hospital conditions. This reduces healthcare cost and improves the life-quality of patients as well as the treatment efficiency.

Medical WSNs provide great opportunities, but it brings several challenges. Indeed, Medical WSNs require high and continuous sampling rates which results in high volume of data. The data should be collected and sent to the base station in order to be stored and analyzed. Furthermore, this data is typically required to be stored for several years, which requires scalable storage capacity at the base station. Moreover, medical data could be lifesaving and must be available at any time and from everywhere. For this reason, new innovative solutions are strongly required to meet the great challenges of handling the exponential growth in data generated by sensors. Another challenge we tackle is the confidentiality of collected medical data. Considering social, ethical and legal aspects of medical systems, data collected by sensor networks are highly sensitive and should be managed properly to guarantee patients' privacy. This is why, several countries have defined data protection laws for privacy protection. These laws differ from one country to another, but their primary goal should be to ensure adoption and enforcement of *Fair Information Practices (FIP)* [FIP] that are the basis for privacy protection around the world.

The cloud has become the paradigm of a large-scale data oriented systems which is suitable for medical applications. Moreover, the cloud provides a complete accessibility for a wide range of access devices such as PCs, network of computers, smart-phones and network-enabled medical devices. However, using the cloud for medical data storage means moving patients data from a trusted environment (healthcare provider's infrastructure) to an untrusted environment (cloud servers, which may be located outside the country and are under different regulations). Security

threats obstruct the adoption of the cloud by healthcare providers, as medical data confidentiality and users privacy are not guaranteed.

In this chapter, we discuss the benefits and challenges of using cloud services for medical applications (e.g., WSNs for healthcare monitoring). We will first present cloud computing concepts and the cloud architecture. Then, we introduce e-health and show the advantages of using new technologies in healthcare environments. Finally, we review the advantages and challenges of adopting the cloud for medical applications.

2.2 Cloud computing

In this section, we introduce cloud computing concepts and its architecture. First, we define the cloud and we highlight its characteristics and its opportunities. Then, we describe common cloud service models and cloud deployment models.

2.2.1 Definition and characteristics

The National Institute of Standards and Technology (NIST) organization [PT11] defines the cloud computing as "a model enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

According to NIST definition of cloud computing [PT11], there are five essential characteristics :

- **On-demand self-service :** cloud computing enables customers to provision computing resources, such as server time and network storage, as needed in a flexible and simple way, without requiring human interaction with each service provider.

- **Broad network access :** capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

- **Resources pooling :** the cloud computing is a new computing model based on a business model in which computing resources are shared at three levels : network level, host level and application level. Unlike traditional computing model, cloud computing model is multi-tenant model where computing resources are shared between multiple consumers, in other words, computing resources are assigned and reassigned dynamically according to consumer demand.

- **Rapid elasticity :** computing resources can be rapidly increased and decreased as needed. Also, these resources can be completely released for other uses when they are no longer needed. Unlike traditional infrastructure which have fixed and limited capabilities, cloud computing provides the ability to massively scale resources (bandwidth, storage space, servers.

- **Measured service :** the cloud ensures transparency for both the provider and consumer of the utilized service, by providing tools which enable cloud consumers to control and supervise usage of their resources.

The main enabling technology for cloud computing is virtualization. This term, in computing, refers to the abstraction of computer resources (Computing power, storage, memory, network, application stack, database) from the applications and users who use the service [vir14]. The virtualization enables resources pooling in data centers. There exist various forms of virtualization which are : OS virtualization, storage vitualization, database virtualization, application virtualization and hardware virtualization [MKL09].

2.2.2 Service models

In what follows, we present the three principal service models of cloud [PT11] :

- Software as a Service (SaaS) : in this model, user's applications which are traditionally installed and run on the user's desktop or local infrastructure, run on the cloud infrastructure. They are accessible via Internet with thin client interface (web browser) or thick program interface. Users have control on neither the infrastructure resources (network, servers, storage, OS), nor individual application capabilities (with possible exception of limited user-specific application configuration settings).

- Platform as a Service (PaaS) : in this model, the consumer creates the software using programing language, libraries, service and tools from the provider. The consumer also controls software deployment onto cloud infrastructure and configuration settings. Networks, servers, storage, and other services are provided as per consumer's needs.

- Infrastructure as Service (IaaS) : in this model, infrastructure resources including storage and other computing capabilities, are provided as service to consumers via a network. the customer is able to deploy and run operating systems and applications. The consumer does not have any control over cloud infrastructure but could rather possibly have limited control of selected networking components (e.g., host firewalls).

2.2.3 Deployment models

In what follows, we present common deployment models of clouds [Clo13] :

- *Private cloud :* the cloud infrastructure is dedicated to only a single organization. Resources are maintained in-house by an organization, or are allocated exclusively for an organization by a cloud provider on its premises.

- *Community cloud :* the cloud infrastructure is dedicated for exclusive use by a specific community of users from two or more organizations that have shared interests. Resources are maintained in-house, or are allocated exclusively for the community by a cloud provider on its premises.

TABLE 2.1 – Public vs Private

Characteristic	Public cloud	Private cloud
Scalability	Very high	Limited
Elasticity	rapid and greater	rapid , but limited by the capacity of on-premise equipment
Self-On-demand	Very good	Very good
Cost	Very good, pay-as-you-go model and no need for on-premise infrastructure, pay-as-you go	greater installation, upgrade and maintenance cost
Security	The loss of control over protected or sensitive data by organizations	high level of privacy and security of the data and related applications
Reliability	Medium ; depend on Internet connectivity and provider service availability	High, as all equipment is on premise
Equipment quality	The most sophisticated networking equipment on the market	Risk of obsolescence

- *Public cloud :* the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them, on the premises of the cloud provider.

- *Hybrid cloud :* is a cloud infrastructure which is composed of two or more distinct private, community or public cloud infrastructures that remain independent entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [PT11].

2.3 eHealth

Healthcare sector is currently facing many challenges that concern all governments. These challenges include :

- The continuous increase in the elderly population in developed countries [Var07].
- Significant number of medical errors [All13].
- Considerable pressure on healthcare providers affected by the economic crisis(effective staff and infrastructure budgets cuts), resulting in a deterioration of the quality of services provided [Sin02, NKVV13].
- A partial coverage of healthcare services in rural and isolated areas [Var07] ;
- Rising health care costs [Var07].

Using communication technologies [Var07, FPE10, BLL02] in healthcare environment has led to increase accessibility to healthcare services (to anyone from anywhere), improve quality, and reduce cost of healthcare services [FPE10]. Furthermore, communication technologies can be deployed to address healthcare challenges. For example, medical errors which are often due to a lack of information about patient's health, resulting in wrong diagnostic and drug interaction problems. Giving access medical data to healthcare staff, when needed, can reduce medical errors [Var07]. Several solutions are proposed to allow sharing medical data such as electronic healthcare record systems [EHR]. Medical data storage and share over Internet is a solution to increase availability of medical data.Remotely monitoring system can benefit from wireless sensors (see figure 2.2). Indeed. Miniature body wearable sensors can collect medical information about patient's health, and send them to a station where they are stored, processed and visualized by physicians.

2.3.1 Electronic health record

Information technology (IT) has become the principal vehicle that some healthcare specialists believe will reduce medical error [FPE10]. An electronic health record is defined as collection of electronic health-related information on individual patients [NAH08]. This digital format is intended to be shared between different healthcare settings through networks/health information systems. In literature, several terms are given to health record : Electronic Medical Record (EMR), Electronic Health Record (EHR) and Patient Health Record (PHR) [NAH08]. These terms are

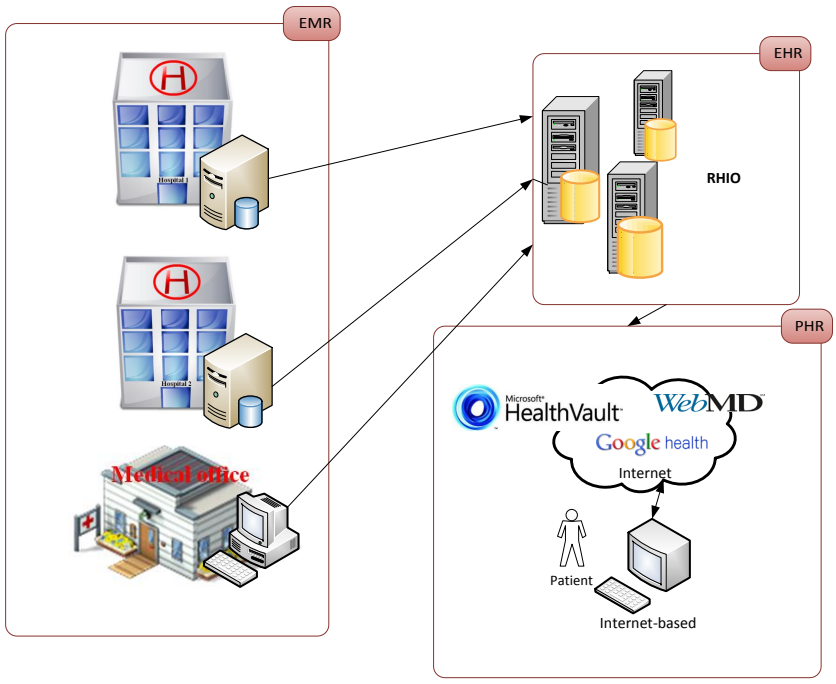


FIGURE 2.1 – Electronic Health Record Diagram

sometimes used interchangeably, they have some differences though ; according to the National Alliance for Health Information Technology (NAHIT) report [NAH08], the definitions of EMR, EHR and PHR are the following (are also described in figure 2.1) :

- **Electronic Medical Record (EMR) :** "is an electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization". For example, medical records (e.g, e-prescribing) are generated and maintained either by healthcare staff of same institution through institution server, or by a doctor in his PC.

- **Electronic Health Record (EHR) :** "is an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization".

- **Personal Health Record (PHR) :** "is an electronic record of health-related

information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual". For example, patient health record systems provided by tier organizations such as Microsoft HealthVault, GoogleHealth (has been permanently discontinued) and others. These platforms allow patients to store and maintain their health and fitness information. In this system, each patient manage himself access authorizations of his medical record.

Health data contains information about patient health status and personal information such as age, address, and sometimes tracking information. This data is considered highly sensitive, and therefore, security of electronic health record is a public priority. Many countries have defined laws of health information protection such as the Health Insurance Portability and Accountability Act (HIPAA) in USA, Data Protection Act of 1978 (revised in 2004) in France, etc.

2.3.2 Wireless sensor networks for health monitoring and rehabilitation

Rates of chronic diseases, including heart disease, lung disorders, cancer and diabetes, continue to increase dramatically in all countries [Org05]. They are leading cause of death and disability in several countries [Org05] such as France with 86%, USA with70%, and Australia. Treatment for these conditions represents a major portion of the healthcare costs in several countries [BLL02]. This situation is further wosen by rapidly increase in the aging population [BLL02]. This resulted in a strong need for developing continuous healthcare monitoring systems. Consequently, healthcare sector has attracted more IT and communications providers to offer means to remote continuous health monitoring technologies in both in and out of hospital environments. Adopting such solutions would give patients back their normal independent lives, and reduce the overall cost of healthcare through efficient use of resources (physician, hospital room,...).

Recent advances in WSN have made possible deployment of wearable sensors

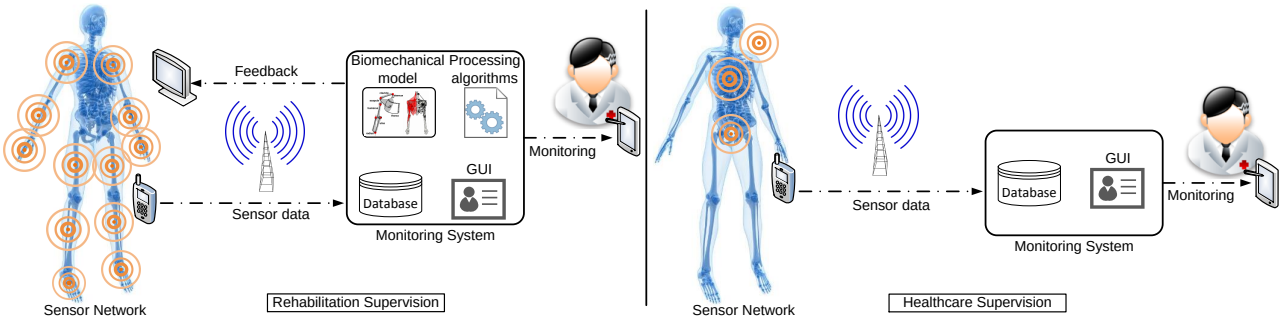


FIGURE 2.2 – WSNs for healthcare monitoring

on the bodies of patients in/out hospital. This allows continuous monitoring of physiological signals (such as ECG, blood oxygen levels) and other health related information (such as physical activity levels). There exist two categories of WSN architectures for healthcare monitoring (see figure 2.2) : (1) architectures for rehabilitation supervision that provide functional re-education and rehabilitation of people who suffered from a health incident/crisis ; (2) healthcare supervision architectures of patients who have critical health status.

These two architecture categories have three components : Body Area Networks (BAN), gateways, and remote monitoring system. (a) The BAN is a set of sensor nodes carried by the patient to collect different health information. A sensor node sends collected data via wireless channel to the gateway. (b) The gateway acts as a relay node to the monitoring system through a backbone network (ADSL, WiFi, 3G or satellite). (c) The remote monitoring system, usually a server hosted by the healthcare provider, is the heart of the architecture at which the collected data is stored, processed and accessed.

The use of WSN in healthcare allows the patients to be able to continue their recovery process while carrying out their normal lives. This leads to cost saving through more efficient use of hospital resources and earlier detection of medical conditions. WSNs provide great opportunities, but also bring several challenges. Scientists and engineers have been working together to tackle research and technical WSN challenges for several years [ASMR11, BFR+06, GCAM08, SNO+08]. However, numerous challenges related to the management of the data collected by these network need to be addressed. Indeed, in WSNs for medical applications, sensor sampling is performed at high frequency, thus they generate a large amount of

sensitive medical data coming from sensors, and that is why healthcare's providers need secure and scalable storage solutions. In addition, health information should be accessible in real time by patient's doctors, at anytime and from anywhere. One of the possible issues is to store the sensed data in the cloud in order to allow medical staff to remotely access this data.

2.4 Using the cloud for medical applications

Various medical applications can rely on the cloud services to take its advantages, including :

- **EHR, EMR and PHR systems :** these systems provide means to share medical information between healthcare professionals, so as to improve of healthcare quality. However, EHR systems present numerous challenges when data are stored in the cloud including infrastructure installation and maintenance costs, and confidentiality of medical records.
- **The healthcare remote monitoring system :** is the base station of medical wireless sensor networks.
- **Emergency intervention systems :** they rely on wireless technology for adequate emergency intervention (by providing early detection and high accessibility to patient's health status information).

2.4.1 Cloud computing advantages for medical applications

The cloud computing provides to healthcare organizations a flexible environment for easily deploying and running medical applications. This allows sharing health information between healthcare professionals and patients. There are several advantages of using cloud computing for medical applications :

- *Collaboration :* in many healthcare cases, healthcare staff need to collabo-

rate to provide adequate healthcare services and avoid unnecessary redundant tasks. This collaboration requires health information sharing. Cloud technologies enable information synchronization and sharing in real-time.

- *Focus on core competencies :* when healthcare professionals outsource their IT infrastructure to the cloud, they can focus on their real business, which is providing healthcare services.

- *Mobility :* by outsourcing health information on the cloud, the healthcare staff and patients will be able to access health information with desired device (such as PCs, smart phones, and network-enabled medical equipment) via Internet or private networks. This increases accessibility of healthcare information by healthcare professional, and improves quality of healthcare services by enabling fast and appropriate interventions.

- *Cost saving :* there is no need for the healthcare institutions and doctors to invest in hardware infrastructure and maintenance because these concerns are already taken care of by the cloud providers.

- *Scalability :* cloud computing can provide an important CPU power as well as memory and storage capabilities that could appear to be unlimited. These capabilities are on-demand and scale dynamically as needed.

2.4.2 Barriers to cloud computing adoption for medical applications

Although there are several benefits of cloud adoption for medical applications, there are also some significant barriers to adoption. The security and confidentiality of health information is the principal barrier that makes healthcare professionals reluctant to adopting the cloud. There are other barriers, but with less impact than the security issues of the cloud. In the following, we give and discus some cloud concerns for medical applications.

2.4.2.1 Security and confidentiality of health information

Moving the storage of health information to clouds raises high security and confidentiality risks that are not acceptable due to the data nature. The European Network and Information Security Agency (ENISA) has established a report "Cloud Computing : Benefits, risks and recommendations for information security" [TH12]. We present in what follows some of the important security risks given in this report.

- **Isolation failure.** This risk category is based on two cloud characteristics, which are multi-tenancy and shared resources. The risk due to an attack (guest-hopping attack) on mechanisms separating(hypervisors) storage, memory, network and reputation between different tenants [TH12]. For example, an attacker will try to identify two virtual machines that are likely to be hosted on the same physical hardware. Assuming the attacker is interested in health information from a virtual machine of healthcare provider (machine A) but is unable to directly penetrate virtual machine "A" because she does not have right access. The attacker will try to penetrate virtual machine "B", and then try to gain access to virtual machine "A". However, this kind of attacks are still rare [TH12] and much more difficult for an attacker to put in practice compared to attacks on traditional operating systems.
- **Loss control over data :** it is difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way.
- **Management interface being hacked :** the cloud provider gives customers the possibility to manage their resources with management interfaces accessible over Internet. Consequently, this raises an increased risk, especially when combined with remote access and web browser vulnerabilities.

These cloud security risks increase the possibility of health information disclosures. This risk is not acceptable in the case of health information. Consequently, the cloud is considered not trusted enough compared to traditional infrastructure The question of how to address these security issues for secure adoption of cloud by medical applications is what we deal with in the rest of this manuscript.

2.4.2.2 Reliability

Medical applications are so critical and must guarantee reliability and availability. For this reason, clouds must provide high availability and mobility support to medical data storage and processing services accessible via Internet. However, these services can become a potential target of security attacks (e.g. denial of service attack), since they are accessible through a simple Internet connection.

2.4.2.3 Independence from cloud providers (so-called lock-in)

Although there are some rules and standards to provide interoperability between cloud providers, they are still insufficient to guarantee data, applications and services portability. Indeed, data structures and services interfaces differ from one cloud provider to another. This can make the migration operation of data, applications and services from one cloud provider to another or back to a local IT environment more difficult. Enabling the migration is expensive, especially if there is a large amount of data stored in the cloud. This results in a dependency on a particular cloud provider for service provision, especially if data portability, as the most fundamental aspect, is not enabled.

2.4.2.4 Loss of governance, legal and regulatory issues

Several governments have defined health information protection laws. Examples include Health Insurance Portability and Accountability Act (HIPAA) in USA, Data Protection Act of 1978 (revised in 2004) in France [PRI], etc. These laws regulate the use and disclosure of health information by healthcare providers, but do not regulate their third-party operations (such cloud providers). Healthcare providers must enter into business association agreement with cloud providers to transfer health information. One this agreement signed the cloud providers become subject to health information regulations that cover the transfer of data from healthcare providers' sites to the cloud providers site. However, the use of this information by the cloud providers is not covered by this agreement. The cloud provider could store

the data outside original country jurisdiction, and these practices might not comply with regulations. Consequently, if healthcare providers choose outsourcing of health information, then they lose control over their data. It is practically impossible to determine how data is used, and when really stored on the cloud [MKL09].

2.5 Conclusion

In This chapter, we have presented the benefits and challenges of using clouds for medical applications. In healthcare, professionals, decision makers and managers are aware that information and communication technologies can reduce costs and improve quality of healthcare services. But, to benefit from sophisticated information and communication technology, healthcare providers face several challenges. These include infrastructure management costs, making storage and processing scalable, accessibility of services in real time. Cloud computing can release healthcare organizations and enterprises from their infrastructure management, and enables them to focus on their core competencies, by providing easy access to dynamically scalable pooling resources, including networks, servers, storage and applications. However, the cloud computing brings several new challenges including confidentiality and privacy of health information. Part of the next chapter will focus on this point.

Chapitre 3

Data security concepts, issues and challenges in cloud computing

'It takes years of hard work to establish trust but only a few seconds of madness to destroy it'

3.1 Introduction

Unauthorized disclosure of medical information can result in privacy violation and embarrassment and/or criminal exploit of information to commit fraud or medical identity theft. As medical information traditionally is stored and processed within trusted environment (such as authorized doctor's or patient's devices, healthcare provider's servers and other), traditional access control was sufficient mechanism to

prevent unauthorized access medical data in compliance with data protection government laws. But, recently, healthcare providers have been attracted to outsource their collected medical data into the cloud, which is untrusted environment. They are motivated by cost saving, mobility and scalability offered by the cloud. However, the security risks induced by medical data outsourcing are obstacles which need to be tackled.

The rest of this chapter is organized as follows. In the second section, we introduce some concepts of security including security services and security techniques. In the third section, we presents new advanced cryptography techniques, especially Attribute Based Encryption (ABE). Recently, this method has been gaining considerable attention as a useful technology for safe and secure storage of data in the cloud. However, ABE is needs to be more developed and extended for its successful integration in piratical systems. We also study many ABE related works, and consider several challenges induced by ABE integration in practical system. In the fourth section, we focus on data security issues due to the sensitive data storage in the cloud computing. We give some security threats of data outsourcing. Then, we present traditional access control that is not suitable for sensitive data outsourcing, and we study cryptographic access control and related existing works. In the last section, we conclude this chapter.

3.2 Security concepts

In this section, we define security services, then some security mechanisms are presented.

3.2.1 Security services

IT security organizations and professionals have defined some elements which are considered as key concepts of security. The ISO 7498-2 [ISO89] defines five main categories of security services :

- *Data confidentiality :* consists in ensuring that information cannot be disclosed to unauthorized users [ISO89]. The confidentiality of information could be ensured in transit during message transfer, and at rest on storage server [MKL09].

- *Data integrity :* consists in ensuring that data cannot be modified in an unauthorized or undetected manner [ISO89]. Integrity is violated when a message is actively modified in transit. Information security systems typically provide data integrity in addition to data confidentiality.

- *Authentication :* including origin authentication and entity authentication. Origin authentication is a security service that verifies the identity of a system entity that is claimed to be the original source of received data [Shi07]. Entity authentication is the process of verifying a claim that a system entity or system resource has a certain attribute value [Shi07]. This attribute is usually the user identity.

- *Availability :* the property of a system or a system resource being accessible or operational upon demand, by an authorized system entity, according to performance specifications for the system [Shi07].

- *Access control :* provides protection against unauthorized use of resources [ISO89].

- *Non-repudiation :* preventing denial of actions and commitments.

3.2.2 Security mechanisms

Cryptography is the science of information security. The Cryptography provides means for implementing security mechanisms that ensure certain security goals, termed security services. In this thesis, we are particularly interested in the following mechanisms : *Encipherment, Data integrity, Message authentication code, Digital signature, Access control.*

3.2.2.1 Encipherment

Encipherment, also called encryption, is a cryptography technique that transforms a readable message (plaintext) into an unreadable message (encoded) by using encryption algorithm, while only authorized reader who retains a secret key can retrieve the original message by using decryption algorithm. The aim of encryption techniques is to achieve the confidentiality. In cryptography, there are two branches of encryption systems : symmetric encryption systems and asymmetric encryption systems.

- **Symmetric encryption :** is a branch of cryptography in which the algorithms use the same key for both encryption of plaintext and decryption of ciphertext [Shi07]. For example, if two individuals agree on a shared secret (a secret key), then by using symmetric encryption they can send messages to one another on a medium that can be tapped, without worrying about eavesdroppers. All we need to do is have the sender encrypt the messages and the receiver decrypt them using the shared secret (as described by the figure 3.1). An eavesdropper will only see unintelligible data. Only symmetric encryption algorithms have the speed and computational efficiency to handle encryption of large volume of data [MKL09].

- **Asymmetric encryption :** is a modern cryptography technique, in which the algorithms use a pair of keys(a public key and a private key) and use a different component of the pair for each of two counterpart cryptographic operations (e.g., encryption and decryption, or signature creation and signature verification) [Shi07]. The private key is the secret component of this pair of keys which is kept secret, and the public key is publicly available component. Key-distribution can be done more easily with asymmetric algorithms compared to symmetric algorithms. Indeed, all users who obtained a pair of keys can communicate with any other user without the need of additional secret sharing. Asymmetric cryptography can be used to create algorithms for encryption, digital signature, and key agreement. In case of asymmetric encryption (see the figure 3.1), when a sender wants to ensure confidentiality for data he sends, he encrypts the data with a public key provided by the receiver. Only the receiver

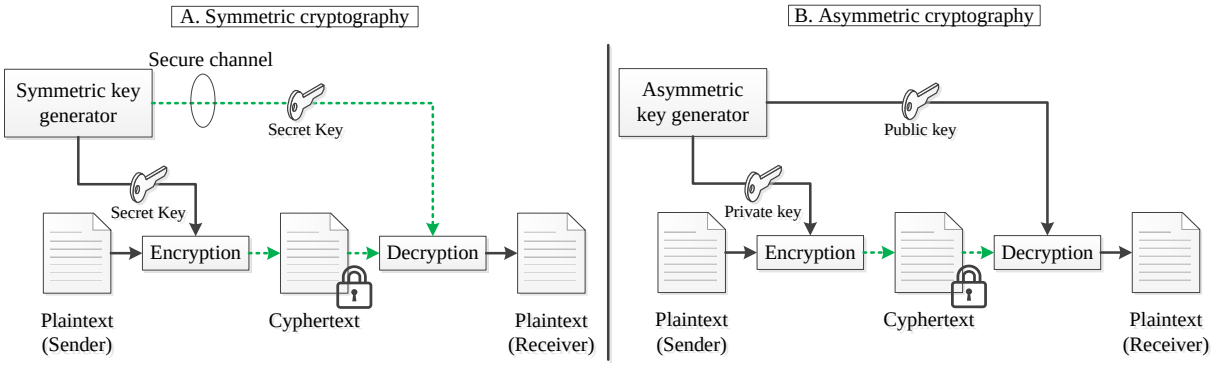


FIGURE 3.1 – Asymmetric and symmetric encryption

has the matching private key that is needed to decrypt the data.

3.2.2.2 Data integrity

The purpose of data integrity mechanism is to provide means for the recipient of message, to detect any unauthorized changes to data, including both intentional change or destruction and accidental change or loss, by ensuring that changes to data are detectable [Shi07]. Cryptographic hash functions are typically used to ensure data integrity [MVOV96]

A hash function : also called one-way encryption, is a mathematical transformation that takes a message (m) of arbitrary length and computes from it a fixed-length (short) hash-value (h)[KPS02]. It is also called message digest, hash-result, or simply : a hash. Hash functions have the following properties [KPS02] :

- It is relatively easy to compute hash value. In other words, a hash function is efficient to compute in processing time.
- It is computationally infeasible to find a message which corresponds to a given message hash value.
- It is computationally infeasible to find two different messages which produce the same hash value.

3.2.2.3 Message authentication code (MAC)

Message authentication code (MAC) is a checksum that is computed with a keyed hash [Shi07]. The keyed hash is a cryptographic hash in which the mapping to a hash result is varied by a second input parameter that is a cryptographic key (symmetric key)[Shi07]. MAC can be used to assure data origin authentication and data integrity at the same time.

Data origin authentication is a type of authentication whereby a party is corroborated as the (original) source of specified data created at some (typically unspecified) time in the past [MVOV96]. By definition, data origin authentication includes data integrity [MVOV96].

3.2.2.4 Digital signature and non-repudiation

Digital signature is value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity [Shi07].

Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation [MVOV96].

Hash function is used in conjunction with digital signature for data integrity and origin authentication : where a message is typically hashed first, and then the hash-value, as a representative of the message, is signed in place of the original message [MVOV96].

Digital signature offer an important advantage over MAC technique, is the non-repudiation service. This service provide protection against false denial of involvement in an association [Shi07].

3.2.2.5 Access control mechanisms

Access control is process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy [Shi07].

The main components of an access control are : access right and two entities which are subject and object.

- *A subject* can either be a user, process, thread, or program that wishes to take certain actions in a system.
- *An object* is a being item in the system on which an user can make actions.
- *Access rights* specify for each object the actions that a subject may perform.

There are several types of access control model (also known as access control policy), hence ISO7498-2 [ISO89] distinguishes between two types :

- *Identity-based* : in this access policy type, resources access decisions made on the basis of the identities of users and resources, e.g. Access control lists (ACL).
- *Rule-based :* here, resources access is controlled by global rules imposed on all users, with access decisions typically made using a comparison of the sensitivity of the resources with user attributes, e.g Role-based Access Control (RBAC).

3.3 Advanced encryption

In this section, we show two new asymmetric encryption systems : (1) Identity-based encryption, in which user's public key is a string (can be user's identity or mail address), (2) Attribute-based encryption, in which data is encrypted according to access policy, and user's private (secret) key is generated from a set of attributes. Then, we present extension works of attribute-based encryption for its integration in practical system.

3.3.1 Identity-based encryption

In 2001, Dan Boneh and Matthew Franklin solved identity-based encryption problem and developed a fully functional identity based encryption by using weil pairings on ecliptic curves [BF03]. The identity-based encryption is a type of asymmetric encryption in which user's public key is a string (can be user's identity or mail address) combined with public master key. User obtains his private key from Private Key Generator (PKG). The PKG is a trusted third party which publishes master public key, and retains the corresponding master private key. Only PKG can generate users' private keys by using master private key.

3.3.2 Attribute-based encryption (ABE)

The ABE technique extends the identity-based encryption to enable expressive access policies and fine-grained access to encrypted data, proposed by Sahai and Waters in 2005 [SW05]. ABE enables public key based one-to-many encryption and is envisioned as a promising cryptographic primitive for realizing scalable and fine grained access control systems, in which user can share his data according to encryption policy without prior knowledge of who will be receiving the data, and the access decision is based on a set of attributes. The concept of access structure is described as follows :

- **Universal attributes set (U) :** is the set of all attributes that describe data properties, user properties and environment properties.

- **Access structure :** is an access policy that designates who can access to what. It is built from an access tree (T) which can be seen as a logical expression combining several attributes through AND, OR or other operators (figure 3.2). Each non-leaf node of the tree represents a threshold gate, described by its children and the threshold gate value (AND, OR or other operators). Each leaf node of the tree is described by an attribute from U and a value.

In figure 3.2, we give an example of an access tree which is derived from the following logical expression : ((speciality = physician AND (division = cardiology OR division = pulmonary) OR (division = gerontology AND (speciality = nurse OR speciality = physician))). This expression means that data can be accessed by all physicians working in cardiology, pulmonary or gerontology divisions, as well as all nurses working in gerontology division have access.

Key-Policy Attribute-Based Encryption (KP-ABE) [GPSW06] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [BSW07] are the two main variants of ABE. KP-ABE assigns to each file a set of attributes to be encrypted, and assigns to each user an access structure, that represents his access scope, for data decryption. On the contrary, CP-ABE assigns to each file an access structure to be encrypted and uses a set of attributes to generate the user's key for data decryption.

For instance, in medical systems, healthcare professionals are assigned particular roles (e.g., general practitioner, nurse), and depending on their role, they get permissions to access to particular data or not. Implementing these policies is easier and more efficient using CP-ABE than using KP-ABE. Indeed, we can describe the role of each healthcare professional by assigning him a combination of attributes. At the same time, we encrypt each file by an access structure that expresses the access policy. In what follows, we present the basics and construction of CP-ABE [BSW07].

A CP-ABE scheme consists of four fundamental algorithms : setup, encrypt, key generation, and decrypt.

Setup : computes the public key (PK) and the master key (MK). The public key (PK) is used by encryption and decryption algorithms. The master key (MK) is needed to generate secret keys by the Key generation algorithm.

Encryption (PK, M, A) : it takes as input the public key PK, a message M, and an access structure A built over the universal attributes set (U). This algorithms encrypts the message M according to the access policy that is defined by the access structure A, and gives as output the ciphertext CT. Only users having a set of attributes corresponding to the access structure A can decrypt the ciphertext (CT).

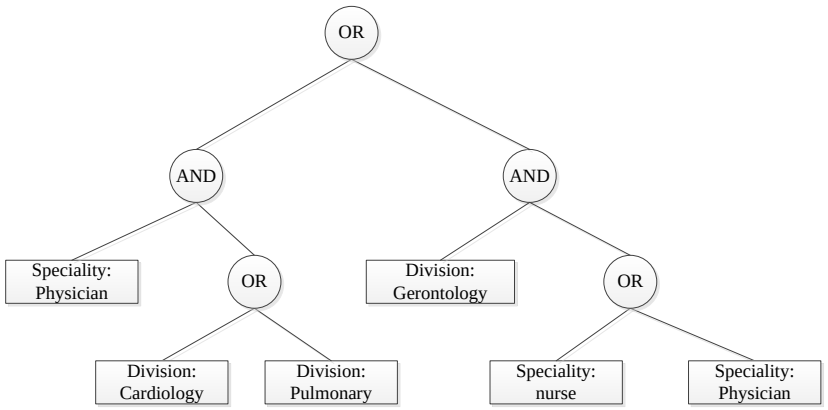


FIGURE 3.2 – An access tree T

Key generation (MK, S) : this algorithm takes as input a master key MK and the user set of attributes S and generates the user's secret key SK.

Decryption (PK, CT, SK) : it takes as input the public key PK, the ciphertext CT and a secret key SK. It returns a message M that is plaintext of CT if the set of attributes corresponding to SK satisfies the access structure A of CT.

3.3.3 ABE extension

Several research works have been proposed to enhance traditional attribute based encryption schemes by supporting other properties, and they tackle some relevant issues before these schemes are applied in practical systems. In what follows, we present some of these ABE related works :

3.3.3.1 Multi-authority

In attributed-based encryption schemes, there exists a central trusted authority that generates and keeps secret a master key and distributes secret keys to eligible users. So, in these schemes the user must go to a single trusted authority and prove his identity in order to obtain a secret key which will allow him to decrypt encrypted data. However, in many applications a part might want to share data according to

a policy written over attributes issued across different trust domains and organizations. Hence, Sahai and Waters [SW05] presented the multi-authority ABE problem as : is it possible to construct an attribute based encryption scheme in which many different authorities operate simultaneously, each handing out secret keys for a different set of attributes ? The main issue here is how to construct multi-authority ABE scheme which is secure against collusion attacks.

Chase [Cha07] have proposed a new cryptographic solution to resolve this challenge. Her solution provides multi-authority ABE with any polynomial number of independent authorities to monitor attributes and distribute secret keys. Chase is the first who applies a global identifier (can be security social number in medical applications) in multi-authority ABE for tying users' keys together as a solution against collusion-attacks.

In [LW11a], Lewko and Waters have shown limitations of the few existing works which have attempted to resolve multi-authority ABE problem, among them Chase solution [Cha07], because it is relied on a central authority and was limited to expressing a strict *AND* policy over a pre-determined set of attributes. In addition, Lewko and Waters [LW11a] proposed a new multi-authority Attribute-Based Encryption solution. In Their solution, any party can become an authority and there is no requirement for any global coordination. Also, It is more expressed compared to Chase solution since it accepts any access structure that can be expressed with any boolean formula over attributes issued from any chosen set of authorities. Finally, it does not require any central authority that avoid a single point of failure, and failure or corruption of some authorities will not affect untouched authorities.

3.3.3.2 Accountability

The main goal of accountable ABE scheme is to prevent the problem of key abuse such as illegally key sharing among colluding users. This problem is extremely important as in an ABE-based access control system, the users' secret keys contain users privileges to the protected resources. The dishonest users may share their secret keys with unauthorized users. Some solutions [LRK09, LRZW09] have proposed

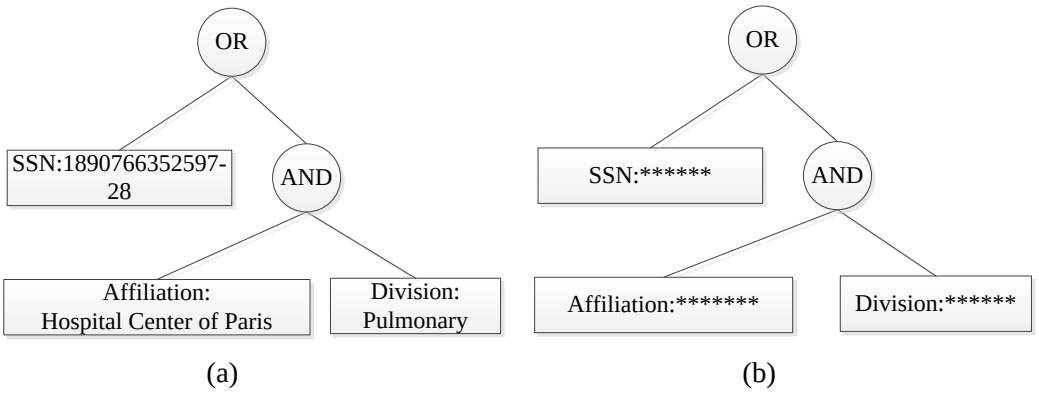


FIGURE 3.3 – An access structure (a) and the corresponding partially hidden access structure (b)

accountable ABE scheme by embedding additional user specific information in user's secret key, and adding the trace algorithm.

3.3.3.3 Privacy preservation

In traditional Attribute Based Encryption scheme, access structure (access policy) is associated with ciphertext and it is required for decryption. So, anyone who obtains a ciphertext can know the access structure associated with the ciphertext. In certain applications, access policies (here, are represented by access structures) contain sensitive information and must be protected from unauthorized users.

Several solutions [FAL06, KTS07, NYO08, LRZW09, LDL12] have been proposed to tackle the challenge of CP-ABE with privacy preserving. Nishide et al. [NYO08] proposed a first CP-ABE scheme with partial hidden access structure. Li et al. [LRZW09] followed their work and studied the problem of user accountability. All these works are not fully secure and they are limited to expressing a strict *AND* policy. Lai et al. [LDL12] proposed a fully secure CP-ABE scheme with partial hidden access structure (see figure 3.3). Also, their scheme is more expressive compared to above works, it accepts any access structure that can be expressed with any Boolean formula over universal attributes set.

3.3.3.4 Efficiency

Efficiency varies depending on kind of ABE used scheme or/and application (the system which integrates ABE). Several ABE scheme have been proposed that their efficiency depends on provided security properties. For example certain schemes are more secure than other but less efficient. In addition, certain application expects it by reducing cost of operations like bilinear pairings on encryptor and/or decryptor, where as other applications expects it by delegating computation intensive operations to more powerful devices (e.g., the cloud) in secure manner.

Green et al. [GHW11] proposed a new paradigm for ABE that eliminates overhead induced by ABE decryption operation. Because the size of the ciphertext and the time required to decrypt it grows with the complexity of the access structure. Their solution allows the cloud, in where ABE ciphertexts are stored, to transform ABE ciphertext into constant-size ciphertext, without the cloud being able to read any part of the users messages. Their solution is very interesting and useful for accelerating decryption on constrained devices such as mobile phone, tablet, sensor, etc.

To delegate intensive computation operations to the cloud many works [YWRL10a, ZHA+12, YWRL10b, TCN+13, HSM13] have used a cryptography technique called *Proxy re-encryption*. It is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher-text encrypted under Alices public key into another cipher text that can be opened by Bobs private key without seeing the underlying plaintext (see [BBS98] for details).

3.4 Using the cloud for sensitive data storage

In this section, we study the problem of outsourcing sensitive data in the cloud and existing works. First we define sensitive information. After that, we identify some security and privacy risks induced by using the cloud for medical data storage. Then, we show traditional access control methods and their limits. Finally, we present

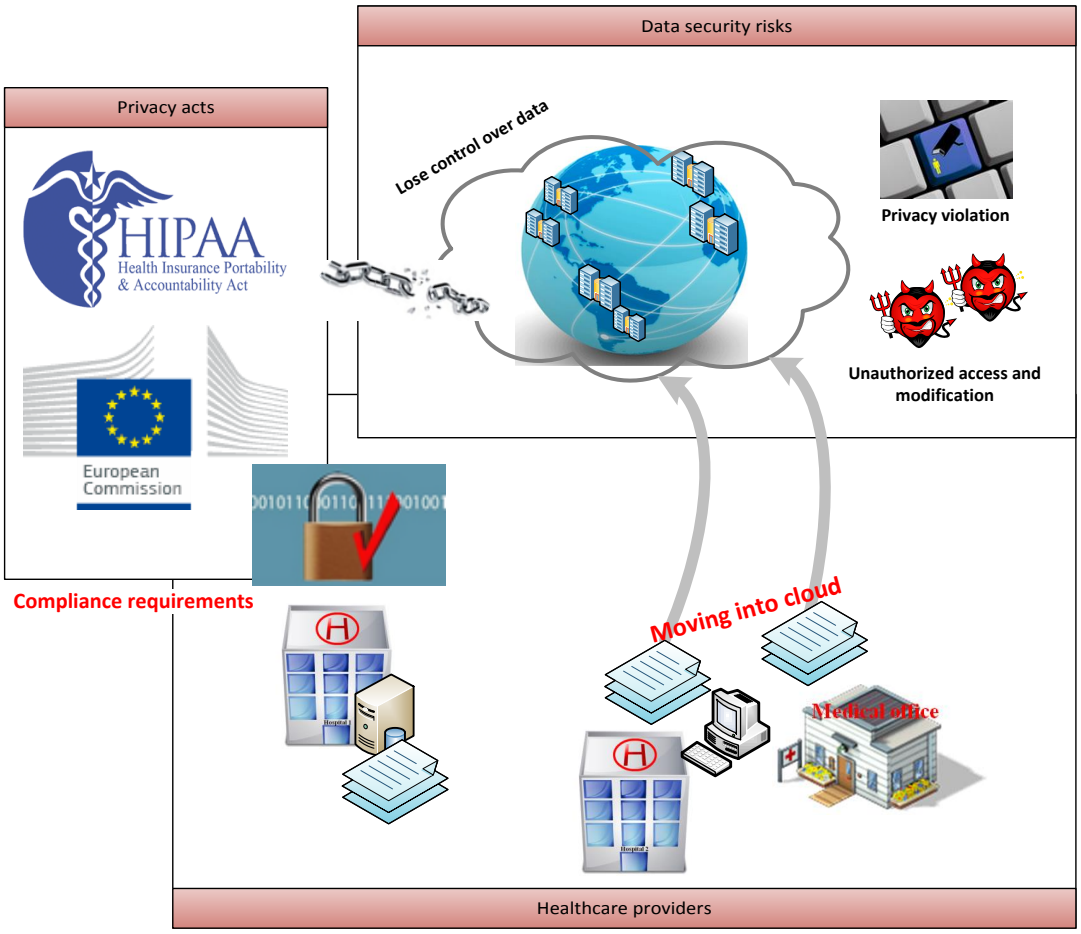


FIGURE 3.4 – Security threats when data is moved into cloud

cryptographic access control solutions and challenges of key management caused by encryption.

3.4.1 Sensitive information and data security threats

In [Shi07], sensitive information is defined as : " information for which disclosure, alteration, or destruction or loss could adversely affect the interests or business of its owner or user, or the privacy to which individuals are entitled under the privacy and confidentiality acts ".

In previous chapter (2), we have described health/medical data. This data contains information about patient health status and personal information. It is collected either by healthcare staffs (EHR systems), or by body sensors for healthcare monitoring. The outsourcing to cloud these applications brings several security risks. Medical data is high sensitive information which concerns privacy of patients such as health status, security social number, age, address, tracking information, etc. Using the cloud requires, compared to traditional infrastructure, moving this information to be stored and processed in cloud servers as described by the figure 3.4. Data privacy is at risk if data in the cloud is unencrypted. There is the potential for unauthorized access either by a rogue employee on the cloud service provider side or an intruder gaining access to the infrastructure. In addition, compliance requirements is another challenge, where different countries have different regulatory requirements on data privacy. Since cloud providers offer no information on the location of the data, it is important to consider the regulatory requirements on where data can reside.

Access to and use of sensitive information should be controlled, as required by the privacy and confidentiality acts. In context of this thesis, we are interested by health data which is considered as highly sensitive data, but our works can be applied for other instances of sensitive information.

In what follows, we will show existing solutions to protect against unauthorized access.

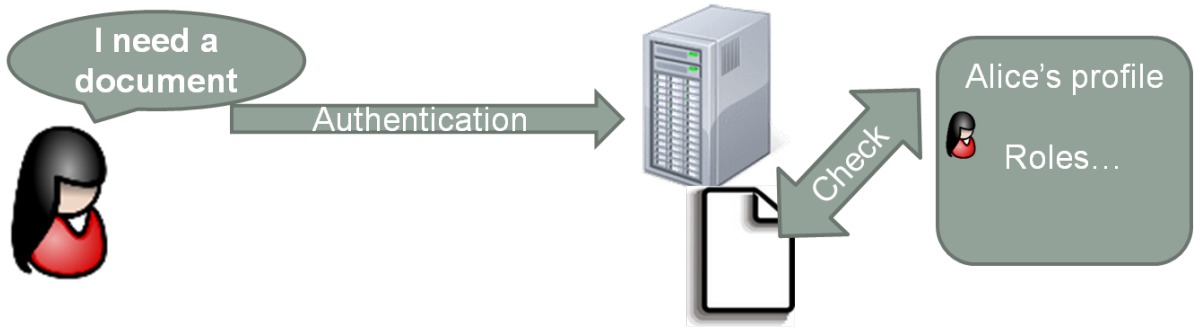


FIGURE 3.5 – Traditional access control

3.4.2 Traditional access control

Traditional access control mechanisms rely on a trusted server to mediate access in order to protect files. In case of electronic medical records (EMR), access policies are implemented and enforced by healthcare providers. The figure 3.5 illustrates this mechanism.

There exists various access control models. According to NIST [NIS10], there are three access control methods that are clearly distinguishable from one another.

- **Identity-based access control(IBAC) :** in IBAC method, access decision is based on user identity. IBAC model is simple to understand and implement on monolithic systems. It is often supported by access control list access control which associates to each resource an access control list of authorized users [NIS10]. It is extremely fine-grained in the sense that it becomes a user-specific rule. However, it is coarse-grained in the sense that it only considers one dimension, that of the user, ignoring resources, actions, and context. In addition, IBAC is not scalable to support large numbers of users (large enterprise) [NIS10].
- **Role-based access control (RBAC) :** in RBAC, access decision is not based on user identity but rather on user's role(s). For instance, a doctor might be allowed to read medical record of a patient. This right (or permission) is granted because that person has the role patient's doctor, not because of who they are. Typically, in RBAC, a user can have multiple roles to which different permissions can be granted. Users define roles and associate permissions to

roles and then roles to users therefore transitively granting users permissions. But roles have their limits too. How do you express other conditions or parameters ? What if you want to express a permission of the following form : "doctors can read medical record only during emergency intervention". With RBAC, you can express doctor + read medical record. But you cannot really express the time constraint. In addition, what if you want doctor who can only read medical record ? You would need to define doctor-read and a doctor-write role. This leads to role explosion [HFK+13].

- **Attribute-based access control (ABAC) :** in ABAC is a logical access control model, in which authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes [HFK+13].

3.4.3 Cryptographic access control

Traditional access control mechanisms rely on a trusted server to mediate access in order to protect files. However, when the centralized server is not enough trusted and/or data stored is highly sensitive, we need a cryptographic access control which relies exclusively on cryptography to provide confidentiality and integrity of data managed by the system. It is particularly designed to operate in untrusted environments where the lack of global knowledge and control are defining characteristics [HJ03].

The principle of cryptographic access control is encrypt data and disclose keys to authorized users, but it is not as simple as that. This kind of access control requires key management mechanism in order to handle and distribute keys used for data encryption. The figure 3.6 illustrates a cryptographic access control which associates a single symmetric key for each user file, which induces high complexity of key distribution and management. One critical issue with this approach is how to achieve the desired security goals without introducing a high complexity on key management and data encryption.

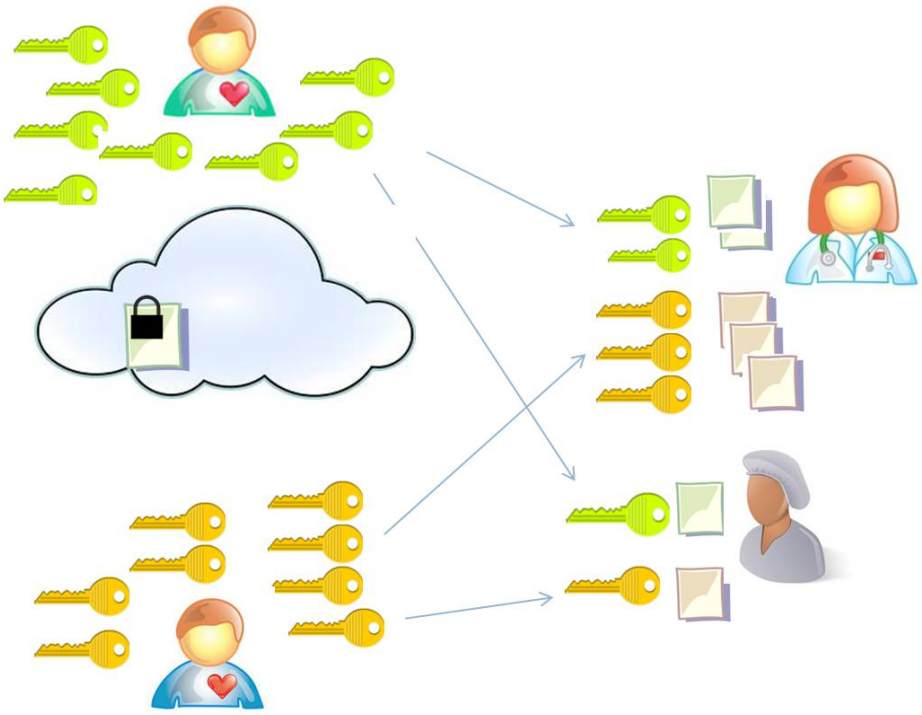


FIGURE 3.6 – Cryptographic access control

Key management for cryptographic access control brings several challenges and involve heavy computation overhead on the data owner for key distribution and data management. Several existing works haves been proposed to address the challenges of key management cryptographic access control [BLLS11, YWRL10a, KRS+03, GSMB03, dVFJ+07, TCN+13]. Many of these works create a trusted party, called the authority, which deals with key management tasks.

These solutions can be classed into three classes : *ACL-based solutions*, *Filegroup-based solutions*, *ABE based solutions*.

3.4.3.1 ACL-based solutions

These solutions [GSMB03] provide secure fine-grained access control by introducing a per file access control list (ACL). This kind of solutions attach each file with a meta data file that contains the file's access control list (ACL). Each entry of the file's ACL corresponds to a user with access right to this file. A file is encrypted

with a symmetric key, named file encryption key (FEK) in [GSMB03], and each entry of file's ACL is the encryption of file's FEK using the public key of an authorized user. This kind of solutions enable fine-grained access control, and allow to separate between reading and writing rights. However, the complexity of the ACL-based solutions would be proportional to the number of users in the system [YWRL10a].

3.4.3.2 Filegroup based solutions

These solutions [KRS+03, ZBS98, Fu99] categorize files into several file groups to provide efficient key management. In [KRS+03], Kallahalla et al. proposed Plutus as a cryptographic file system to secure file storage on untrusted servers. Plutus groups a set of files with similar sharing attributes as a file-group. Each file is encrypted using a unique symmetric file key which is further encrypted with the symmetric key of the file-group to which the file belongs. If the owner wants to share a file-group, he just delivers the corresponding file-group key to users. As the complexity of key management is proportional to the total number of file-groups, Plutus is not suitable for the case of fine-grained access control in which the number of possible " file-groups" could be huge [YWRL10a].

3.4.3.3 ABE-based solutions

Although symmetric and asymmetric cryptography based solutions provide secure storage over untrusted servers, they have several drawbacks. The achievement of fine-grained and scalable access control while ensuring confidentiality by encryption is still open challenge [YWRL10a].

Several recent works [YWRL10a, LYRL10, BLLS11, FAL06] have been interested by this technique to provide fine-grained access control. In what follows, we study some works that used ABE for building fine-grained access control.

In [YWRL10a], Yu et al. proposed a solution for securing shared medical data through the cloud. In their solution, they rely on Key-Policy ABE scheme, in which

files is encrypted according a set of attributes, and an access structure is assigned to each user. KP-ABE allows to enjoy of fine-grained access control. But this is not sufficient because owner is in charge of data and users management which requires that the owner have to be continuously on-line. Yu et al. [YWRL10a] tackle this challenge by using proxy re-encryption and lazy re-encryption to outsource some data files/users management tasks to cloud in secure manner. Their solution supports only one owner that enabled him to create files and shared them with other users through the cloud. Authorized users can only read files according to their access structures sent them by owner.

In [LYRL10], Li et al. proposed another solution that used multi-authority of Policy-Key ABE scheme, where each authority represents a security domain which manages only a subset of the users. This division allows to reduce key distribution complexity. This solution enables multi-owner to share their patient health record through the cloud. However, the both solutions [YWRL10a, LYRL10] are patient-centric approach (see PHR in chapter 2) in which medical data is created and managed by patient. In this kind of system, security of medical data is under the responsibility of his owner (the patient). In addition, KP-ABE is limited compared to CP-ABE (see the section 3.3.2). Since CP-ABE is the most method adapted to construct Role/Attribute based access control for medical applications.

3.5 Conclusion

In this chapter, first we have presented some security concepts related to our work in this thesis. After that, we have focused on advanced cryptography methods, especially Attribute Based Encryption. Recently, this method has been gaining considerable attention as a useful technology for safe and secure storage of data in the cloud. However, ABE is needs to be more developed and formed before its application in piratical systems. We have also studded many ABE related works. Then, we have addressed the challenge of secure data outsourcing in cloud computing. In which, we have given some security threats of data outsourcing, we have presented traditional access control that cannot resolve this problem, and we have studied cryptographic access control and related existing works.

Chapitre 4

Secure and scalable cloud-based architecture for medical applications

There has been a host of research works on wireless sensor networks for medical applications. However, the major shortcoming of these efforts is a lack of consideration of data management. Indeed, the huge amount of high sensitive data generated and collected by medical sensor networks introduces several challenges that existing architectures cannot solve. These challenges include scalability, availability and security. In this chapter, we propose an innovative architecture for collecting and accessing large amount of data generated by medical sensor networks. Our architecture overcomes all the aforementioned challenges and makes easy information sharing between healthcare professionals. Furthermore, we propose an effective and flexible security mechanism that guarantees confidentiality, integrity as well as fine grained access control to outsourced medical data. This mechanism relies on Ciphertext Policy Attribute-based Encryption (CP-ABE) to achieve high flexibility and performance. Finally, we carry out extensive simulations that allow showing

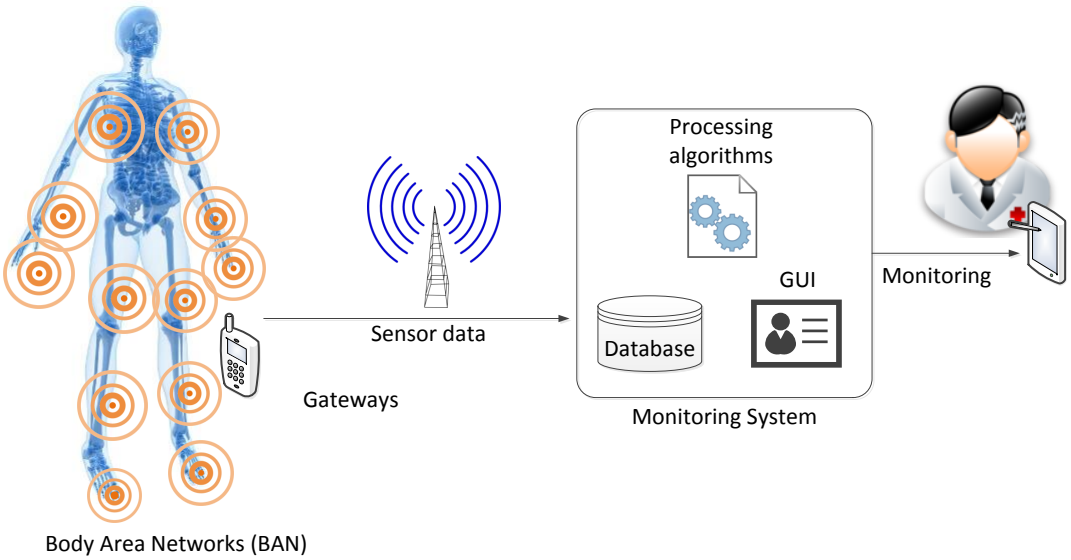


FIGURE 4.1 – Remote monitoring system architecture

that our scheme provides an efficient, fine-grained and scalable access control.

4.1 Introduction

Recent advances in medical sensors, wireless technologies and Micro-Electro-Mechanical systems have enabled the development of senor nodes capable of sensing, processing and communicating several physiological signs. These lightweight miniaturized nodes collaborate to form a wireless sensor network (WSN) that simplify the supervision of patients' health. The major breakthrough of this technology is providing continuous remote patient supervision both in and out of hospital conditions. Consequently, it reduces health cost and improves the quality of life of patients as well as the treatment efficiency.

Proposed solutions have adopted a common architecture with three main components as described in figure 4.1 : Body Area Networks (BAN), gateways, and remote monitoring system. The BAN is a set of sensor nodes carried by the patient to collect different health information. It sends collected data via wireless commu-

nication channel to the gateway which serves as a relay node to the monitoring system through a backbone network (ADSL, WiFi, or satellite). The remote monitoring system, usually a server hosted by the healthcare provider, is the heart of the architecture at which the collected data is stored, processed and accessed.

Scalability is a challenge that WSNs for medical applications should tackle. Indeed, the sampling of medical sensors is performed at high frequency which increases the amount of collected data. In addition, the frequency of sensor sampling is often increased if the condition of patients being monitored gets worse. The important size and heterogeneity of data drives a need for an increasing storage and processing capacities. In addition to scalability issues, medical data could be life saving and must be accessible at any time and from everywhere. Existing solutions rely on a centralized paradigm to store and process sensed data thus cannot tackle the aforementioned challenges. We definitely need new innovative solutions to meet the great challenges of handling the exponential growth in data generated by sensors.

Considering social, ethical and legal aspects of medical systems, data collected by sensor networks is highly sensitive and should be managed properly to guarantee patients' privacy. Therefore, it is essential to ensure security of data during transmission as well as during storage. Access to patient information must be strictly limited to authorized users in order to guarantee the confidentiality. Since data is vital for medical diagnosis, data integrity should be verified to prevent wrong treatments because of malicious or erroneous modifications. Access to medical data is often governed by complex policies that distinguish between each part of the data and each user privileges. Therefore, providing fine-grained access control that supports dynamic and complex organizational policies is a very hard challenge. Practical issues, such as security management, overhead and scalability of the access control with the number of users, also need to be considered. While lot of research works have been carried out in medical wireless sensor networks, only few studies have been achieved regarding security and existing solutions are far from mature [LLR10].

In this chapter, we address the challenge of data management in wireless sensor networks for patient supervision. We propose a secure and scalable architecture for collecting and accessing large amount of data generated by medical sensor networks. We leverage cloud computing technology to dynamically scale storage resources via

on demand provisioning. Furthermore, we propose an innovative security scheme that eliminates potential security threats of medical data outsourcing and guarantees confidentiality, integrity as well as fine grained access control. Our contributions in this work are many folds : First, we propose a new cloud based architecture for medical wireless sensor networks. Second, we show how we guarantee the confidentiality and the integrity of outsourced medical data without involving patients or doctors interventions. Third, we propose an innovative access control which allows implementing complex and dynamic security policies necessary to medical application while reducing the management and processing overhead. More specifically, we combine Ciphertext Policy Attribute Based Encryption (CP-ABE) and symmetric encryption to achieve fine grained access with low computation overhead.

The rest of the chapter is organized as follows. In section 2, we review some related works. In section 3, we present our proposed architecture. In section 4, we review attribute based encryption basics necessary to the understanding of our proposed access control. In section 5, we describe the security services that are ensured by our architecture. In section 6, we analyze the security of our solution, and we provide preliminary performance evaluation. In section 7, we provide simulation results and performance evaluation of our scheme compared to representative schemes from literature. In section 8, we conclude the chapter.

4.2 Related works

Scalability via on-demand resource provisioning and virtually infinite data storage capacity makes the cloud computing [BYV+09] compelling for managing data generated by WSNs. Cloud computing eases storage, processing and sharing of sensor data and provides anywhere/anytime access to supervision applications. Research works on coupling WSN and the cloud are still in their early infancy. A recent paper [LW11b] tried to identify the opportunities and challenges of connecting wireless sensor networks to the Cloud. Also, few papers introduced cloud computing to different WSN applications such as industrial supervision [RGPA10], patient data collection [RKW+10], energy monitoring [KB09] and environmental monitoring [LMHJ10]. However, all these papers described preliminary works and ignored the challenges

induced by combining WSN and cloud computing.

Authors in [HSH09] proposed a framework based on a publish/subscribe model which facilitates WSN-Cloud connection. In another paper [KVH+10], they used this framework to monitor human activities and to share information among doctors, care-givers, and pharmacies. However, authors did not discuss the security requirements for such a framework. In ESPAC [BLLS11], data collected from patients are sent to the hospital server before being stored on the Cloud. Despite taking advantage of the cloud to offer unlimited data storage, the scalability of this scheme is limited. Indeed, the hospital server is a bottleneck (single point of failure) that may crash in the case of flash crowd. In addition, no data storage neither data access are possible on the cloud if the hospital server is out of order or inaccessible.

The storage of sensitive data over untrusted servers requires cryptography techniques in order to keep data confidential and preserve patients' privacy. Various solutions, based on symmetric or public cryptography, have been proposed to provide cryptographic access controls that allow storage and sharing of data on untrusted servers [KRS+03][GSMB03][BCHL09][dVFJ+07][WLOB09]. However, These techniques do not support fine grained access control required by medical applications. Indeed, they are not scalable with the number of users and introduce high complexity in key distribution and management.

Recent works leveraged new cryptography techniques, such as Role Based Access Control (RBAC) and Attribute Based Encryption (ABE), to provide fine-grained access control required by personal medical systems. Ibraimi et al. [IAP09] applied Ciphertext Policy ABE (CP-ABE) to enable patients to securely store and share their health record on external third party servers. Barua et al. used bilinear pairing and ABE to guarantee data confidentiality and integrity as well as user privacy and authentication in cloud-based medical systems. In [LYRL10], authors proposed a novel practical framework for fine-grained data access control to medical data in Cloud. To avoid high key management complexity and overhead, they organized the system into multiple security domains where each domain manages a subset of users. Unfortunately, all these works adopted a patient-centric approach where each patient generates his own security keys and distributes them to authorized users. We argue that the patient-centric approach is not applicable to manage data collected by WSN

for patient supervision. Indeed, the access policies that govern such systems are often complex to be defined by the patient. In addition, the healthcare organization is the legal owner and the responsible for patient's health data during his hospitalization within the hospital or at home settings. Consequently, security policies must be fixed by the healthcare organization rather than the patient.

4.3 Our proposed architecture

In this section, we describe our architecture which enables a healthcare institution, such as a hospital or a clinic, to manage data collected by WSN for patient supervision. The proposed architecture is scalable and able to store the large amount of data generated by sensors. Since these data are highly sensitive, we propose a new security mechanism to guarantee data confidentiality, data integrity and fine grained access control. Unlike existing patient-centric systems, security configuration and key management in our solution are totally transparent to users (patients and doctors) and do not require their interventions.

In order to achieve the aforementioned objectives, we propose the architecture described in figure 4.2. This architecture considers two categories of users, healthcare professionals and patients, and is composed of the following components : (1) the WSN which collects health information from patients, (2) the monitoring applications which allow healthcare professionals to access to stored data, (3) the Healthcare Authority (HA) which specifies and enforces the security policies of the healthcare institution and (4) the cloud servers which ensure data storage. By storing data on the cloud, our architecture offers virtually infinite storage capacity and high scalability. Indeed, the architecture increases its storage capacity, through on-demand provisioning feature of the cloud, whenever it is necessary. In addition, it offers enormous convenience to the healthcare institution since it does not have to care about the complexity of servers' management.

To achieve fine-grained access control, we can use attribute based encryption (ABE) to encrypt data before storing them on the cloud. However, integrating ABE into medical systems is a real challenge. In ABE, data are encrypted with an access

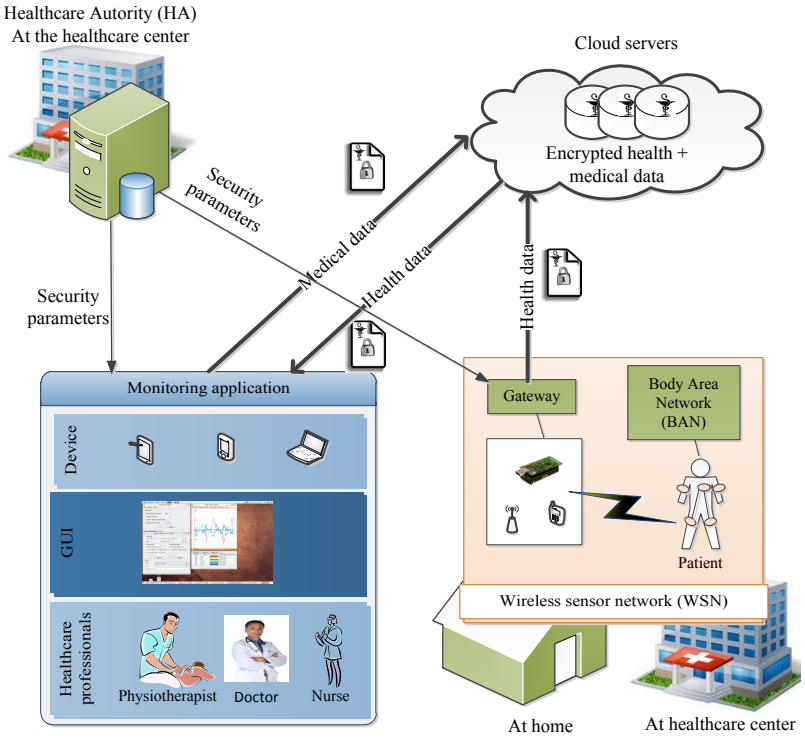


FIGURE 4.2 – The proposed architecture

structure which is the logical expression of the access policy (eg : the data can be accessed by physician in cardiology division or by nurses). The cyphertext (encrypted data) can be decrypted by any user if his secret key has attributes that satisfy the access policy. The power of ABE is that we do not need to rely on the storage server for avoiding unauthorized data access since the access policy is embedded in the cyphertext itself. However, this characteristic becomes an inconvenient when the access policy changes. Indeed, to apply a new access policy to a file, we must download it, re-encrypt it with a new access structure and upload it again to the cloud. The second challenge faced with the integration of ABE is keys and access structures management. Indeed, the questions of who should generate the access structure that govern the security policy and who should generate and distribute keys necessary to access to the data are a real challenge in medical systems. To answer these questions, existing ABE-based systems adopted a patient centric approach that we showed unsuitable for our application.

To tackle the first challenge of ABE integration, we propose to use both symmetric cryptography and ABE to encrypt data. More specifically, we propose to

encrypt each file with a randomly generated symmetric key (RSK) and encrypt the RSK with ABE. Both the encrypted file and the encrypted RSK are sent to the cloud for storage to allow fine grained data sharing with authorized users. Indeed, if a user has a secret key that satisfies the ABE access policy, he will be able to decrypt the RSK and hence to decrypt the file. Furthermore, if the file access policy changes, we should download and re-encrypt the RSK rather than the whole file. This lead to a significant gain in data communication and encryption operations. Finally, our solution has less encryption overhead compared to the naif utilization of ABE to encrypt the whole file. In fact, ABE consumes much more processing power than symmetric cryptography when we use complex access policy [BSW07] like ones used in medical systems.

To tackle the second challenge, which is mastering the complexity of security management, we introduce an entity that we call ***Healthcare Authority (HA)***. The HA specifies and enforces the security policies of the healthcare institution. It is used by the administrators of the healthcare institutions to define rules as "who can access to what". Based on these rules, the HA generates and sends to each user his ABE security parameters which are a pair of ***access structure*** and ***secret key***. The secret key is tagged with the user attributes set which represent the user privileges. This information is required to decrypt data that the user is allowed to access. The access structure represents the access policy that protects the user data. When a user encrypts the random symmetric key (RSK) that protects his data using this structure, he can be sure that only authorized users (who have the correct attributes) can decrypt and access to his data. Introducing the HA releases users from creating and distributing access structures and secret keys. Consequently, it improves the system usability since a patient has no action to do to secure his data. Also, the healthcare professionals transparently access to data falling under their scope. All the details of security operations are given in section V.

In our architecture, each patient has a personal WSN composed of a set of light-weight/small sensor nodes and a gateway. A WSN enables unobtrusive and continuous health supervision of the patient at the hospital and at home settings. Sensor nodes are carried by the patient to collect different ***health data*** such as heart beats, motion and physiological signals. Each sensor node sends the collected information via a wireless communication channel to the gateway. The gateway aggregates the

different health data into a file and encrypts it using the RSK. Thereafter, it sends the encrypted file along with the RSK encrypted using the access structure obtained from the HA to the cloud.

The monitoring application allows healthcare professionals to supervise their patients and enables them to access to a patient's data anytime and from everywhere using a computer or a Smartphone. The monitoring application downloads the required data from the cloud and decrypts it using its secret key. In addition, it allows the healthcare professionals to add ***medical data***, such as reports, diagnostics and prescriptions, to the patient's information. The medical data is also encrypted and stored on the cloud along with the patient's health data. Similarly to the gateway, the monitoring application encrypts the medical data using a RSK and the access structure obtained from the HA.

4.4 Background : Attribute-based encryption

Attribute-based encryption (ABE) is a recent promising cryptographic method proposed by Sahai and Waters in 2005 [SW05]. The ABE technique extends the identity-based encryption to enable expressive access policies and fine-grained access to encrypted data . In ABE, the access control decision is based on a set of attributes and the concept of access structure described as follows :

- **Universal attributes set (U) :** is the set of all attributes that describe data properties, user properties and environment properties.

- **Access structure :** is an access policy that designs who can access to what. It is built from an access tree (T) which can be seen as a logical expression combining several attributes through AND, OR or other operators (figure 4.3). Each non-leaf node of the tree represents a threshold gate, described by its children and the threshold gate value (AND, OR or other operators). Each leaf node of the tree is described by an attribute from U and a value.

In figure 4.3, we give an example of an access tree which is derived from the following logical expression : ((speciality=physician AND (division=cardiology OR cardiology=pulmonary) OR (cardiology=gerontology AND (speciality=nurse OR speciality=physician))). This expression means that data can be accessed by all physicians working in cardiology, pulmonary or gerontology divisions, as well as all nurses working in gerontology division have access.

Key-Policy Attribute-Based Encryption (KP-ABE) [GPSW06] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [BSW07] are the two main variants of ABE. KP-ABE assigns to each file a set of attributes to be encrypted, and assigns to each user an access structure, that represents his access scope, for data decryption. On the contrary, CP-ABE assigns to each file an access structure to be encrypted, and uses a set of attributes to generate the user's key for data decryption. In medical systems, healthcare professionals are assigned particular roles (eg. general practitioner, nurse), and through those role they get permissions to access to particular data. Implementing these policies is easier and more efficient using CP-ABE than using KP-ABE. Indeed, we can describe the role of each healthcare professional by assigning a combination of attributes. At the same time, we encrypt each file by an access structure that express the access policy. In what follows we present the basics of CP-ABE necessary for the understanding of our architecture. More extensive description of CP-ABE is available in [BSW07].

A CP-ABE scheme consists of four fundamental algorithms : setup, encrypt, key generation, and decrypt.

Setup : defines the universal attributes set (U) and computes the public key (PK) and the master key (MK). The public key (PK) is used in encryption and decryption algorithms. The master key (MK) is needed to generate secret keys in the Key generation algorithm.

Encryption (PK, M, A) : it takes as input the public key PK, a message M, and an access structure A built over the universal attributes set (U). This algorithms encrypts the message M according to the access policy that is defined by the access structure A, and gives as output the ciphertext CT. Only users having a set of attributes corresponding to the access structure A can decrypt the ciphertext (CT).

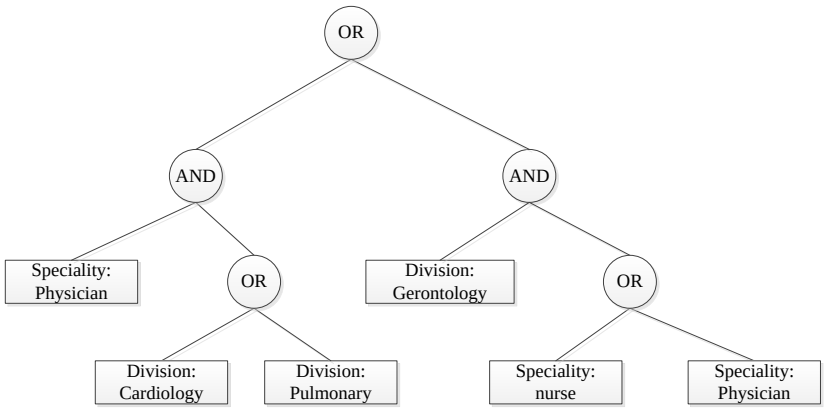


FIGURE 4.3 – An access tree T

Key generation (MK, S) : this algorithm takes as input a master key MK and the user set of attributes S and generates the user's secret key SK.

Decryption (PK, CT, SK) : it takes as input the public key PK, the ciphertext CT and a secret key SK. It returns a message M that is plaintext of CT if the set of attributes corresponding to SK satisfies the access structure A of CT.

4.5 Security services implementation

In this section, we give the security model and define the services that are ensured by our architecture. Then, we detail the implementation of these security services.

4.5.1 Security Model

Our system is composed of the following parts : users (patients and healthcare professionals), cloud servers and the healthcare authority (HA) server. We assume that communication channels between users, the HA and cloud servers are secured by a security protocol such as SSL. Even if SSL guarantees data confidentiality and integrity during transfer, we should encrypt data at the user level because we consider that cloud servers are untrusted. Indeed, data are stored on clouds operated

by companies that may disclose personal information to third parties. For legal and ethical concerns, the cloud provider should neither be able to access to patients' data nor perform data mining or patients profiling. Furthermore, we consider that cloud servers might collude with some malicious or revoked users for illegal data access. Similarly, users might collude together to illegitimately access to file contents. The Healthcare Authority (HA) assures keys and access policies management. We consider that the HA is trusted and secured. Finally, we assume that each party has a public/private key pair and the public key can be easily obtained by other parties through a Public Key Infrastructure (PKI).

4.5.2 Security services

Our architecture guarantees the following security services.

4.5.2.1 Fine-grained Access control

Access control is a security service that protects against a system entity (here, it may be cloud administrator, unauthorized healthcare professional or patient's kin) using a system resource (here, it is reading and updating encrypted medical data)in a way not authorized by the system's security policy ; in short, protection of system resources against unauthorized access [Shi07].

Our solution ensures secure access control and healthcare information confidentiality. Also, our access control is fine-grained which allows to express any complex access policy to data stored on the cloud. Furthermore, it ensures access control in multi-writers access mode on medical data.

4.5.2.2 Integrity and authenticity

Integrity service is a security service that protects system resources in a verifiable manner against unauthorized or accidental change, loss, or destruction [Shi07].

Authentication service is a security service that verifies an identity claimed by or for an entity. There are two general forms of authentication service : data origin authentication service and peer entity authentication service [Shi07].

Integrity and authentication services are closely linked and reinforce each other. As it is detailed in [Shi07] : data origin authentication service provides verification that the identity of the original source of a received data unit is as claimed ; there can be no such verification if the data unit has been altered. Peer entity authentication service provides verification that the identity of a peer entity in a current association is as claimed ; there can be no such verification if the claimed identity has been altered.

Our solution ensures message integrity during transfer between two parties. Furthermore, it ensures data integrity during storage on cloud servers. Also, each party authenticates the origin of each message received from others parties.

4.5.2.3 Availability

Availability [Shi07] is The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system ; i.e., a system is available if it provides services according to the system design whenever users request them.

Our solution ensures availability of service for legitimate users when they need it, and it is resilient when a large group of legitimate users' access at the same time (flash crowd). Furthermore, it is resilient against Denial of Service attacks.

4.5.2.4 Collusion resistance

Our solution enforces the access control system and guarantees collusion resistance, meaning that users (patients/healthcare staffs) cannot collude and gain access to data, when they are not authorized to access. Our architecture resists against the collusion attacks to avoid any unauthorized access to medical data.

Notation	Description
PK, MK	System public key and master key
$Priv_P$, Pub_P	Patient private key and public key
$Priv_{HP}$, Pub_{HP}	Healthcare professional private key and public key
$Priv_{cloud}$, Pub_{cloud}	Cloud private key and public key
SK_P	Patient secret key
SK_U	User secret key
RSK	Symmetric random secret key
AR_P	Patient access structure for read access
AW_P	Patient access structure for write access
AR_{HP}	Healthcare professional access structure for read access
AW_{HP}	Healthcare professional access structure for write access
ID	Unique file identifier which is a structure allowing to find the file we need.
PASS	Password

FIGURE 4.4 – Notation used in our solution

4.5.3 Security implementation

In this section, we present all functionalities of our system with their security implementation details. The first step is system initialization within required system security parameters are generated. This first step allows using of our solutions through others functionalities which are : adding new user, health data management, medical data management, data health deletion and user revocation. Adding new user operation enables either a patient to join the system for health data collection about his health status, or a health professional such as doctor, who follows his patients through their collected health information.

4.5.3.1 System initialization

At the installation of our architecture, the HA creates the universal attributes set and calls the ABE setup algorithm to generate the master key (Mk) and the public key (Pk). The Mk must remain secret while the Pk must be shared with all users since they need it to decrypt data. To share the Pk, the HA signs it with its private key and sends it, along with the signature, to cloud servers. Once the Pk on the cloud, users can download it and check its authenticity thanks to the signature.

4.5.3.2 Adding new user

When a new patient is admitted to the hospital, the Healthcare Authority gives him a secret key and an access structure. The access structure allows him to encrypt his data before uploading it on the cloud and ensures that only authorized users can access to it. The secret key allows him to access to medical data on which he has right. The following steps are performed each time a new patient P joins the system :

1. The PKI generates a couple of private/public keys ($Priv_P$, Pub_P) for the patient P.
2. The HA calls the key generation algorithm of CP-ABE to generate the secret key SK_P. Furthermore, it builds the access structure AR_P that the patient P will use to encrypt his health data.
3. The HA asks the cloud to add the patient P to the users list.
4. Upon receiving the patient addition request, the cloud adds the patient P and his public key Pub_P to the users list (LU).
5. When the patient's gateway establishes a connection to the HA for the first time, it receives the corresponding secret key SK_P, access structure AR_P and private key $Priv_P$.

The difference between the security parameters of a patient and a healthcare professional comes from the fact that a patient needs to encrypt *health data* which can be only read while a healthcare professional needs to encrypt *medical data* which can be both read and modified. The read access policy and the write access policy which govern a medical data may be different. For example, a nurse can only read a report while a doctor can read and modify it to add comments. Consequently, the healthcare professional should obtain two access structures for read and for write policies. The following steps are performed each time a new healthcare professional HP joins the system :

1. The PKI generates a couple of private/public keys ($Priv_{HP}$, Pub_{HP}) for the HP.
2. The HA calls the key generation algorithm of CP-ABE to generate the secret key SK_{HP}. Furthermore, it builds an access structure AR_{HP} that the HP will use to encrypt the medical data. Also, it builds another access structure AW_{HP} for protecting the write mode. We will explain how the AW_{HP} is used in the medical data management subsection.
3. The HA asks the cloud to add the HP to the users list.
4. Upon receiving the HP addition request, the cloud adds the HP and his public key Pub_{HP} to the users list (LU).
5. When the HP establishes a connection to the HA for the first time, its application receives the corresponding secret key SK_{HP}, private key $Priv_{HP}$ and access structures AR_{HP}, AW_{HP}.

4.5.3.3 Health data management

Health data files are information collected by the WSN and can be accessed only in reading mode. The gateway continuously receives information collected by sensor nodes and executes the following algorithm when this data is ready to be uploaded to the cloud :

1. Assign an unique identifier ID to the health data file F. it is a structure allowing to find the file we need.
2. Generates a random secret key RSK for a symmetric cryptography algorithm
3. Computes H the hash value of the file F
4. Uses RSK to encrypt the concatenation of the file F and the hash value H
5. Encrypts RSK with CP-ABE encryption algorithm according to the access structure AR_P
6. Sends to the cloud the following data :

ID	$\{RSK\}_{AR_P}$	$\{(Data + H)\}_{RSK}$

Once stored on the cloud, the health data can be used by healthcare professionals to remotely supervise the patient or by the patient himself. When a user U wants to access a health data file, he starts by downloading this file from the cloud server. After, he decrypts the RSK field of the file using ABE and his secret key SK_U. If he has the right to access this file (his secret key corresponds to the access structure of the patient P), he gets the correct RSK and hence decrypts the file. After the decryption, the user checks the integrity of the content thanks to the hash value. If he detects that the data file was altered he signals it to the Healthcare Authority. Figure 4.5 shows the different steps performed from adding a new patient until its supervision.

4.5.3.4 Medical data management

The medical data (such as reports, diagnostics and prescriptions) are created by healthcare professionals and can be modified by other authorized users. The read access to medical data is similar to health data management. However, to control medical files updates, we assign to each file a password given to only authorized

entities (users or cloud) to allow them to modify the file. To allow a user to upload a new version of a file F, the cloud asks him for the file password. If the user provides the correct password, the new file version is accepted. When a healthcare professional HP creates a new medical file F, he performs the following actions :

1. Assigns a unique identifier ID to the medical data file F
2. Generates a random secret key RSK for a symmetric cryptography algorithm
3. Generates a random password $PASS$ for protecting controlling the write access
4. Computes H the hash value of the file F
5. Uses RSK to encrypt the concatenation of the file F and the hash value H
6. Encrypts RSK with CP-ABE encryption algorithm using the read access structure AR_{HP}
7. Encrypts $PASS$ with CP-ABE encryption algorithm using the write access structure AW_{HP}
8. Encrypts $PASS$ with the public key of the cloud
9. Sends to the cloud the following data :

ID	$\{RSK\}_{AR_{HP}}$	$\{PASS\}_{AW_{HP}}$	$\{PASS\}_{Pub_{Cloud}}$
$\{(Data + H)\}_{RSK}$			

To read the content of a medical file, a user U performs the same actions described in the last section (access to health file). However, to modify a medical file he performs the following actions :

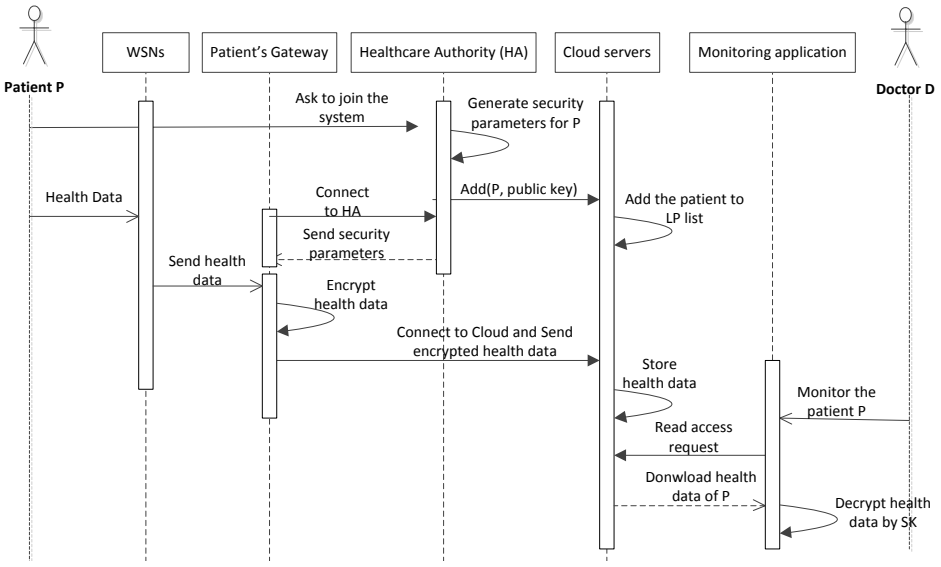


FIGURE 4.5 – Example of patient supervision

1. Downloads the medical file
2. Updates the file content and computes the new hash value of the file ;
3. Encrypt the medical content along with the new hash value using RSK ;
4. Decrypt the password with ABE and Sk_U
5. Sends to the cloud an update request containing the new file along with computed password
6. Upon receiving the update request, the cloud decrypts the password of the original file using his private key $Priv_{cloud}$. The new version of the file is accepted if and only if the password computed by the cloud is equal to the password in the update request.

4.5.3.5 Data health deletion

This operation can be performed only by the file owner. To delete a file, the owner signs and sends a delete request to the cloud. Upon receiving this request, the cloud checks if the sender is the real owner of the file based on the signature and proceeds to the deletion.

4.5.3.6 Revocation

There are two types of revocation. The first one consists of limiting access to data through modifying the access policy. To change a data access policy, we should create a new data access structure and re-encrypt the desired data. The second one consists of revocation of attributes that are associated to a user to limit his access scope. To do so, the system should determine the set of attributes which must be updated. Then, it regenerates new system master key and public key (MK and PK) of ABE. Finally, according to the updated attributes set, some user's secret keys must be also updated and some files must be re-encrypted. However, these operations induce high computational overhead for key management and distribution. So then, the user attribute revocation is not scalable.

In [YWRL10b], to allow scalable revocation S. Yu et al. rely on dynamic scalability of the cloud by delegating most of laborious revocation tasks such as user secret key update and file re-encryption to the cloud without disclosing file contents or user access privilege information. This solution implements the proxy re-encryption technique on the cloud. The goal of re-encryption proxy is securely to enable the re-encryption of ciphertexts from one secret key to another, without relying on trusted parties. Our scheme supports the implementation of this solution. However, this solution does not reduce computational overhead, it only enables the cloud deals with some revocation tasks.

In our solution, to allow an efficient revocation and solve this challenge, we add an expiration time attribute to each user's key. This expiration time indicates until when the key is considered valid. Indeed, to avoid revocation tasks user access privileges are temporary allocated. After expiration of user key, he needs a new key to allow him continuing to access patient's medical data.

4.6 Security and performance analysis

In this section, we show the feasibility of our solution by a security analysis and performance evaluation.

4.6.1 Security analysis

Our solution guarantees message integrity, authenticity and confidentiality during data transfer through SSL protocol. Furthermore, it ensures a secure and fine grained access control to data files stored on the cloud. Indeed, data files are encrypted by a randomly generated symmetric key, and this key is encrypted by CP-ABE. The CP-ABE scheme has been proved secure in [BSW07]. Especially, The CP-ABE scheme has been proved resistant against collusion attacks and ensuring that encrypted data cannot be accessed by unauthorized users. From this, we deduce that the random symmetric key is confidential and can be accessed only by authorized users. Consequently, the data confidentiality is guaranteed by the standard symmetric encryption security.

Since our scheme enables scalable and fine-grained access control, the HA is able to define and enforce expressive and personalized access structure for each user. These access structures enable us to select with fine granularity which users can access to the symmetric key of a given file. Since accessing the symmetric key is necessary to access the file, we deduce that these access structures enable us to select with fine granularity which user can access a file contents. Finally, by using separate access structures for the read and write policies, we separate between read and write access to medical data.

Furthermore, our scheme is resilient against man-in-the-middle attacks by considering two concerns : the first is the attack during communication between entities of the system that requires verifying if public key is correct, and belongs to the person or entity claimed, and has not been tampered with, or replaced by, a malicious third party. The second is how to ensure that Public Key of CP-ABE system is the original PK which is provided by our healthcare authority. In our scheme, to respond

to the first issue, each emitter sends his digital certificate issued by our public key infrastructure to receiver. Then, the receiver verifies validity of certificate by using public key of our PKI. For the second issue, the CP-ABE PK is signed by Healthcare authority, and any entity of the system can verify authenticity of CP-ABE public key before to use it.

4.6.2 Performance analysis

CP-ABE enables fine grained access control to data but induces important processing overhead with complex access policies like the ones used in medical systems. The encryption time of CP-ABE is linear with the number of leaf nodes of the used access structure. However, measuring the decryption time is more difficult since it significantly depends on the used access tree (number of leaf nodes, the type of used operators, the depth of the tree ...) and the set of involved attributes [BSW07]. Here we present preliminary performance evaluation to show the benefit of our solution compared to ABE. We considered several random access structures and attribute sets that we can meet in a real medical system. We used the toolkit developed in [JB11] for ABE and the AES implementation of OpenSSL for the symmetric encryption.

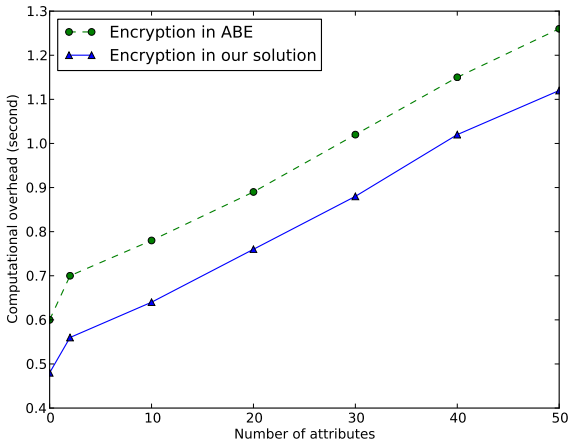


FIGURE 4.6 – Encryption evaluation

First we present performance evaluation of encryption and decryption operations that is shown respectively in Figures 4.6 and 4.7. For this, we compute time ove-

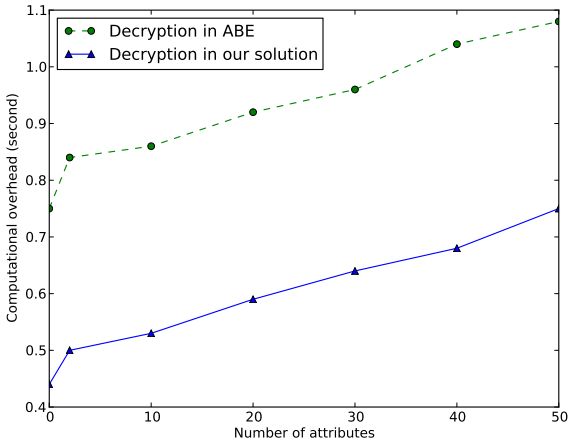


FIGURE 4.7 – Decryption evaluation

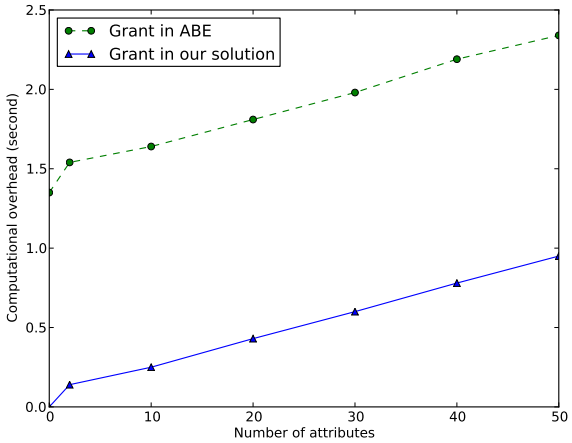


FIGURE 4.8 – Grant evaluation

rhead of encryption and decryption while varying the number of leaf nodes of access structure (number of attributes). Figures 4.6 and 4.7 respectively show that ABE consumes more time than our solution in both encryption and decryption. These results match our expectations and show that our control access scheme is more efficient in terms of cryptographic operations. Indeed, our solution uses AES to encrypt the data file and uses CP-ABE to encrypt only the AES key (256 bits). Since AES is faster than ABE, we reduce the whole encryption and decryption time. This reduction varies between 11% and 20% for encryption, and between 32% and 41% for decryption in the studied samples. Notice that these performance evaluations do not consider the significant gain that we can achieve in grant and revocation thanks

to our access control. Indeed, our evaluation of grant shows that our access control is very efficient when the reduction of encryption overhead varies between 60% and 90% in the studied samples, shown in figure 4.8. We can explain this by the fact that in our solution, we re-encrypt only AES key, so just a data of 256 bits, instead of re-encrypt the whole data file with new access structure in ABE.

4.7 Simulation

To evaluate the performance of our solution we simulate several scenarios when multiple parameters are varied to analyze their impact on our solution. We present first our simulation model, then we present the scenarios.

4.7.1 Simulation model

In this simulation, we establish a model for cloud storage cryptographic access control system as a queuing network. Indeed, We use two interconnected queues : we use a queue to accommodate different requests arrived to the cloud, and another queue to accommodate different requests arrived to Healthcare Authority. The operations considered by this simulation are read, write, create, and access policy changes. Read, write and create operations don't need HA, they perform a simple request on cloud server queue. However, access policy change operations are composed requests which move from HA queue to the cloud server queue. The arrival times of user requests depends in operation type.

The arrival times of patient requests are modeled as non probability distribution with arrival rate of WSN collected data creation requests (λ_{WSNs}). This arrival rate is the multiplication of number of connected patients ($NB_{Patients}$) by WSN sampling frequency (WSN_SAMP_Freq) as :

$$\lambda_{WSN} = NB_{Patients} \times WSN\_SAMP\_Freq$$

For other operation types the arrival times of user requests are modeled as Poisson distribution with corresponding arrival rate to operation type.

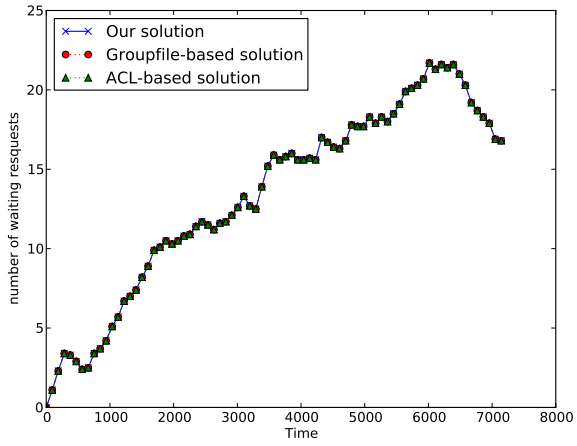


FIGURE 4.9 – Performance evaluation WRT read, write and create operations

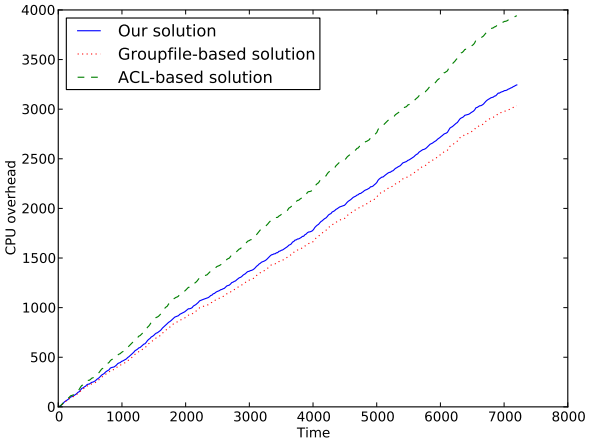


FIGURE 4.10 – Performance evaluation w.r.t. read, write and create operations

4.7.2 Performance evaluation : read, write and create operations

In the first scenario, we assume that there is no access policies update during time of evaluation. We consider three operations : read a file from the cloud, write a file on the cloud and create a file on the cloud. We study the mean number of waiting requests during an interval of time.

We evaluate three schemes : the first, our security scheme which combines CP-ABE with symmetric AES encryption. The second, filesgroup-based solution where a same symmetric key is used to encrypt and decrypt files of a same group such as in Plutus [KRS+03]. The last, access control list (ACL) based solution where each file is associated with a meta data file that contains file's access control list such as in SiRiUS [GSMB03]. In ACL-based solution, each entry in the ACL is the file's encryption key encrypted with the public key of an authorized user.

The arrival times of user requests are modeled as Poisson distribution with arrival rate ($\lambda_{RWCoperation}$). Also, we use a queue to accommodate different requests which arrive to the cloud.

Although, encryption and decryption overhead is not the same for the three solutions the figure 4.9 shows that we have more or less the same performance with the three solutions. This can be explained by the fact that response time depends more on file transfer delays than encryption or decryption time.

When we reduce the size of files and we compute CPU overhead induced by encryption operations rather than number of waiting requests, the figure 4.10 shows that our solution and filesgroup-based solutions have almost the same performance. However, the ACL-based solution has more encryption overhead due to creation operations that depend on number of authorized users. Indeed, taking health data collected by sensors about heart rate as an example. In filesgroup-based solution, we put files which are about heart rate of a patient in the same filesgroup, so, we use a same key to encrypt these files and authorized users can obtain key of this filesgroup. In ACL-based solution, we must encrypt file's key with each public key of

authorized users, so, we do multiple encryption operations. In our solution, we avoid multiple encryption of file's key thanks to use an access structure which expresses access policy to patient's heart rate files.

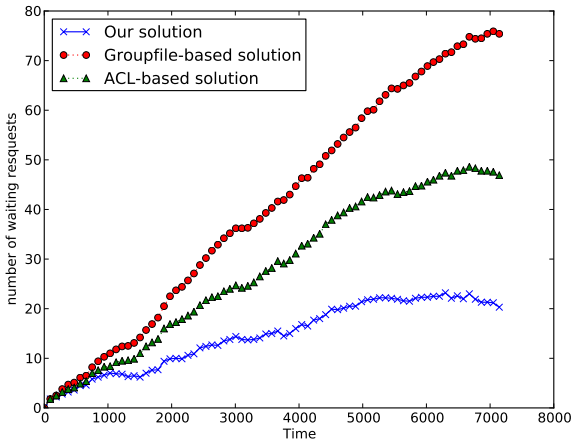


FIGURE 4.11 – Performance evaluation with access policy changes

4.7.3 Performance evaluation with access policy changes

In the second scenario, we introduce multiple changes on access policies that results in right revocations and grants. In this case, we observe that our scheme depicts higher performance than the other two solutions, as shown in figure 4.11. Indeed, revocations overhead is high in ACL-based solution and more in files-group based solution compared to our solution. This overhead is due to re-encryption operations caused by access policies update. In case of files-group based solution, we need to change key of one or several groups that induces re-encryption of all files of group. In case of ACL-based solution, it is necessary to re-encrypt concerned files and update their meta data files. Sizes of the latter depend on the number of authorized users. In our solution, we avoid these operations by using key expiration time where the access rights are temporary assigned to users. Consequently, this shows that unlike to other two solutions, with our solution we can achieve simultaneously fine-grained access and scalability. The figure 4.12 shows different proprieties of each solution studied in this simulation.

Solutions	**Scalable**	**Fine-grained**	**Flexible**
Filesgroup-based solution	+	-	-
ACL-based solution	-	+	++
Our solution	++	++	+

FIGURE 4.12 – A tabular comparison of the cryptographic access control models

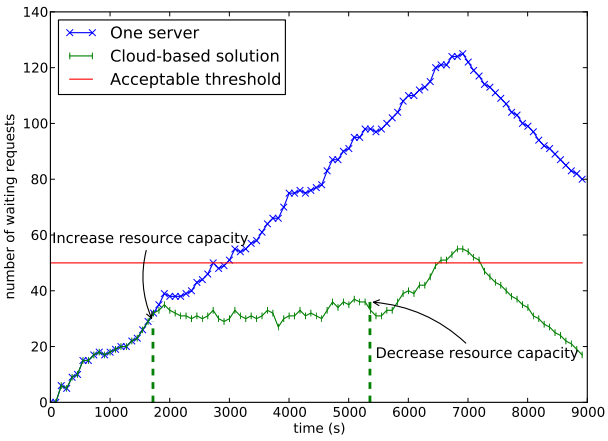


FIGURE 4.13 – Performance evaluation of our solution without/with the cloud

4.7.4 Cloud elasticity

In the fifth scenario, we evaluate the system load of two solutions : our solution which is hosted on the cloud and other solution which is hosted on traditional infrastructure with a single server. In different moments we compute the number of waiting user requests which arrive according to Poisson process. In our solution, initial configuration of resource capacity is similar to the single server configuration, and more resources are added or released to deal with load variation thanks to elasticity of the cloud. Figure 4.13 shows that with a single server the increasing load induces performance degrade of solution. Indeed, the number of waiting requests in queue will be high and may exceed acceptable threshold level. However, using the cloud elasticity allows dealing with load variation to keep the system stable with acceptable threshold level of waiting requests. Also, the figure 4.13 shows that at when the arrival rate of requests is down at 5000s time the load system is also reduced at 7000s time. Consequently, The load variation depends on arrival rate of requests which is dynamic according to several factors (high rate of emergency accident in late in the day).

4.8 Conclusion

In this chapter, we addressed the challenge of data management in wireless sensor networks for patient supervision. We proposed a secure and scalable architecture that leverages cloud computing technology to dynamically scale storage resources via on demand provisioning. Furthermore, we proposed an innovative security scheme that eliminates potential security threats of medical data outsourcing and guarantees confidentiality, integrity without involving patients or doctors interventions. To implement complex and dynamic security policies necessary to medical application, we developed a fine grained access control that combines attributes based encryption and symmetric cryptography. This combination reduced the management overhead and the encryption/decryption time as showed by our preliminary performance evaluation. Finally, we carried out extensive simulations that allowed showing that our scheme provides an efficient, fine-grained and scalable access control. However, Another challenge is still not tackled and concerns medical applications which is emergency management. In chapter 5, we address this challenge and we extend our architecture to support emergency access.

Chapitre 5

Secure medical architecture on the cloud using wireless sensor networks for emergency management

WSNs for medical applications provide useful and real information about patients' health state. This information should be available for healthcare providers to facilitate response and to improve the rescue process of a patient during emergency. In previous chapter, we have proposed an innovative cloud-based architecture for collecting and accessing large amount of data generated by medical sensor networks. Also, we have integrated CP-ABE for providing a secure fine-grained access control over medical data outsourced on the cloud. However, for emergency management, integrating CP-ABE creates particular challenges for providing temporary access victims medical data when this is needed. In this chapter we present our architecture for secure emergency management in healthcare area. We address the challenge of ABE integrating for providing temporary access victims medical data in emer-

gency situation. In addition, we use wireless sensor network (WSN) technology to provide early emergency detection.

5.1 Introduction

Emergency management is an essential field of medical services. Healthcare emergency consists in to provide first aid for person who needs immediate care, and possibly moving the victim to health-care center to ensure suitable treatment. The first challenge with emergency is time, where time is of the essence in emergency situations, which a delay in treatment is likely to result in victim's death or permanent impairment. Indeed, when emergency happens, the victims need emergency care. For this reason, victim or anyone around him try timely contact emergency services. Unfortunately, in some cases the victim is not able to contact emergency services or anyone to help him, especially persons who are elderly or disabled. The second challenge of emergency intervention is the availability of patient's medical data, which is needed in order to accelerate the emergency procedure and provide the appropriate care. It is may be needed at in/out care place. Ideally, this data would be with the patient at all times, but alternatively they should be universally available, such as accessible via Internet.

WSNs for medical applications is a means to detect and provide useful and real time information about patients' health state to the doctors and emergency staff. Moreover, WSNs facilitate response in case of emergency which can save patients' lives. In emergency intervention, medical information of victims is required by emergency staff who may not have enough privileges to access this information. Traditional solutions suggest disabling security system in emergency situations in order to allow emergency staff to access full victim's medical information for controlling emergency. Given the sensitivity of WSNs medical information, an access control solution that supports emergency access to some information without disabling security is then required.

In previous chapter, we have proposed an innovative cloud-based architecture for collecting and accessing large amount of data generated by medical sensor networks.

In this architecture, each patient has a personal WSN composed of a set of lightweight/small sensor nodes and a gateway. A WSN enables unobtrusive and continuous health supervision of the patient at the hospital and at home settings. Sensor nodes are carried by the patient to collect different ***health data*** such as heart beats, motion and physiological signals. Each sensor node sends the collected information via a wireless communication channel to the gateway. The gateway aggregates the different health data into a file and sends file to the cloud. The healthcare professionals can supervise their patients and access to a patient's data anytime and from everywhere using a computer or a Smartphone. In addition, they can add ***medical data***, such as reports, diagnostics and prescriptions, to the patient's information. To ensure secure storage of medical data on the cloud we have integrated ABE to provide a secure fine-grained access control, in which medical data is encrypted with an access structure (e.g., the data can be accessed by physician in cardiology division or by nurses). Also, each healthcare staff obtains his secret key generated from his attributes (roles), and represents his access scope in the system. A healthcare staff can gain to access to medical data if his secret key has attributes that satisfy the access policy. The power of our access control is that we do not need to rely on the storage server for avoiding unauthorized data access since the access policy is embedded in the medical data itself. However, for emergency management, integrating ABE creates particular challenges for providing temporary access victims medical data when this is needed.

In this chapter, we propose a secure scalable architecture for emergency management in healthcare area, which enables healthcare staff to provide timely and appropriate emergency services. We use wireless sensor networks (WSN) for early detection of emergency and cloud computing technology to dynamically scale storage resources via on demand provisioning system. Our contributions in this work are many folds : first, we provide emergency management with two options : A) In proactive manner, our solution relies on sensor networks to detect emergency. Thereafter, our system determines responders and give them temporal access. B) Emergency reporting, where our system enables individual (the victim himself, emergency staff,...) to report emergency situations that WSNs cannot detect. Second, we provide an attribute-based encryption access control with emergency access. Finally, we carried out some simulations that allowed showing that our scheme provides an

efficient access control.

The rest of the chapter is organized as follows. In section 2 we review some related works. In section 3 we describe our proposed architecture. In section 4 we present the implementation of our emergency access control with ABE. In section 5 we conclude the chapter.

5.2 Related work

In [ML13] Ming Li et al. proposed a patient-centric framework. Using ABE, they implemented secure, scalable and fine-grained access control to Personal Healthcare Records (PHRs) stored in the cloud. Ming Li et al. considered emergency access by providing break-glass access for extending a person's access rights in emergency cases. In [ML13] break-glass access is managed by an authority called emergency department (ED). Each patient delegates his emergency key to ED which will give it to medical staff in emergency situation after identifying and verifying enquirer. This solution is simple and allows exceptional access to victim's PHRs when emergency happens. However, the separation between break-glass access and regular access makes this kind of solution suffering from duplication issues of PHRs storage, where PHRs are stored in two forms : PHRs encrypted with ABE system and PHRs encrypted with emergency key. Also, despite the introduction of ED which is in charge of key management, after each emergency situation, the victim should be online to revoke emergency access. In [BPW10] A D.Brucker et al. have proposed a fine-grained break-glass access which is constructed by integrating break glass access concept into a system for end-to-end secure data sharing based on ABE. In [KKVG12], K. Venkatasubramanian et al. proposed a criticality aware access control for emergency (criticality) management in smart-infrastructure. This solution can be applied in several emergency management applications, such as the case where a patient needs urgent medical assistance. In emergency situation, this solution becomes more proactive, where the system evaluates emergency situation to identify the response actions that need to be taken and enables them, and allows chosen responders (subject) to access the system with set of privileges for emergency management. However, this solution does not provide encryption service for available

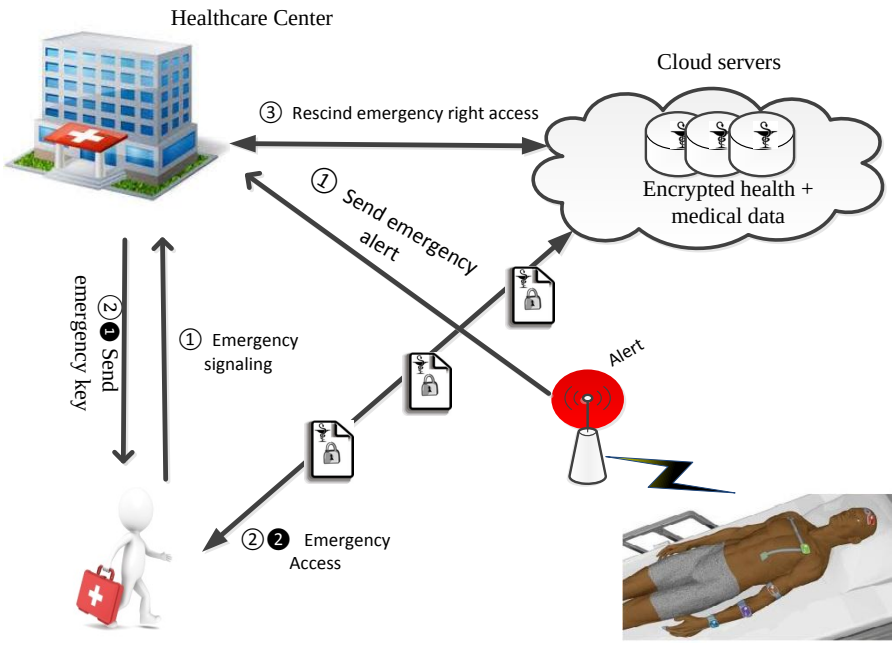


FIGURE 5.1 – Example of Emergency intervention

medical data in emergency management. Since the cloud is untrusted, and there is no totally transparency and control on data when it outsourced on the cloud. The medical data is highly sensitive, when it is unencrypted and stored on the cloud, the risk of unauthorized disclosure is very high.

5.3 Our architecture

In this section, we present our architecture described in figure 5.1, which allows promoting timely intervention of healthcare staff as and when required. Emergency situation can be detected either by the deployed WSN or by a human intervention. Indeed, medical WSN could detect some emergency situations by analyzing collected information. Then, it alerts the healthcare staff for timely intervention. Cardiovascular diseases which include heart attacks, heart failure, stroke, coronary artery

disease are an example of emergency intervention. When an emergency situation is not detected by WSN infrastructure, the emergency may be reported by emergency responders who need access to patient's medical data, or by any person which is not medical staff (patient, patient's family) : for example, a patient who is victim of a road accident.Therefore, we distinguish two possible emergency scenarios :

1. **Proactive scenario**. In this scenario, our access control deals with emergency in proactive manner. Namely, the system can detect emergency situation when it happens thanks to analyzing health data collected by WSN, and determines a set of responders (emergency staff, patient's doctor) and access rights which enable them to access victim's medical data needed in emergency. In our architecture, as shown in figure 5.1, the healthcare authority is alerted by the gateway which informs that an emergency case happened with a patient. Then, the healthcare authority finds responders and gives them access privileges (emergency key) of victim's medical data according to emergency case.

2. **Passive scenario**. In this scenario, the emergency detection is done by a human intervention. In this case, the first aiders and doctors dealing with the victim request for getting temporary access victims medical data when this is needed. We call this case a passive scenario.

The both described scenarios consist of three phases :

1. **Emergency detection :** this phase is responsible for identification of emergency situation when it is happens.

2. **Response :** after identification of emergency, the system gives access rights to responders. To improve response time of access to victim's data in emergency situation our access control should give the priority to emergency access while ensuring bounded waiting time for other requests.

3. **Mitigation :** when the time allowed for emergency is over, our system revokes the given access rights.

In what follows, we present our solution which allows managing emergency situation which satisfies the following :

- Allows responders to access victim's medical data in emergency situation while preserving patient's privacy. Indeed, responders need a temporary access to a part of the victim's medical data to ensure timely intervention.
- Preserves the fine-grained access property of our solution. Hence, allow access to data according to complex policies in emergency situations.
- Preserves the scalability of our access control while considering requests which due to emergency situations.

5.4 Implementation with ABE

The using ABE only for regular access control provides an unique access structure (regular access policy) to encrypt medical data. Consequently, the users cannot momentary access to patient's medical data (during emergency case) if they do not have sufficient access rights to satisfy the regular access policy. To provide emergency management we should provide a temporary access during emergency case. To support emergency access, we define a new access structure generated by healthcare authority that are disjunction of emergency and regular access structures, as shown in figure 5.2. We generate the emergency access structures from emergency policies in ABE form. So, authorized user (emergency staff, patient's doctor,...) can decrypt medical data if his secret key satisfies regular access policy or if his emergency key satisfies emergency access policy and the used key is still valid. To construct an emergency access structure, we use the attributes used in regular policies. For example, the "division" attribute is used to define a particular policy applied for a specific division in hospital, the "function" attribute is used to define a particular policy applied for specific medical function. In addition, we define other new attributes for emergency management such as Emergency Case (EC) which allows the identification of required medical data to ensure emergency response. Moreover, we indicate the patient identity (PI) in emergency policies and emergency key to avoid

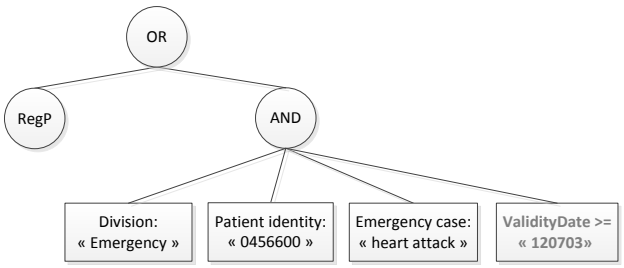


FIGURE 5.2 – An example of access structure for emergency access

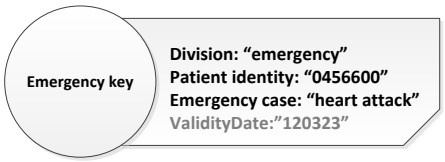


FIGURE 5.3 – Emergency key

unauthorized access to medical data of other patients who are not concerned with the current emergency case. In order to accelerate emergency response, we suggest that emergency keys are prebuilt and stored (in HA or patient's device such as mobile phone) in a secure manner.

Since emergency access is temporary and it should be disabled after the end of the time granted to emergency response, it is necessary to revoke access rights given in emergency situation (Healthcare authority should revoke emergency keys). However, revocation is a very difficult issue in attribute based encryption schemes and may generate high overhead. To handle the revocation problem of emergency key in our scheme, we provide a temporal access to patient's medical data by using integer values and integer comparisons proposed in Bethencourt et al. [BSW07] scheme. To do so, we introduce a numerical attribute which has a date value to express validity date VD of emergency key in the format VD=*YYYYMMDD* (Y : year, M : mounth, D : day), and each medical data is encrypted according to access structure which contains numerical comparison of validity date attribute as $VD \geq$ YYYYMMDD.

Consequently, the user can decrypt medical data with his emergency key expiring on VD only if access structure comparison ($VD \geq$ `YYYYMMDD`) is verified and the rest of the emergency policy matches the user's emergency attributes. When the time allowed for emergency response comes to end, the available patient's medical data in emergency should be re-encrypted with the current new date. Note that to revoke medical data access, we need only to re-encrypt the random secret keys RSKs of concerned files.

5.5 Simulation

In this simulation, we use the same model of the chapter 4. We use two interconnected queues : we use a queue to accommodate different requests arrived to the cloud, and another queue to accommodate different requests arrived to Healthcare Authority. We add a new operation which is emergency access. The operations considered by this simulation are read, write, create, emergency and access policy changes. Read, write and create operations don't need HA, they perform a simple request on cloud server queue. However, access policy change and emergency operations are composed requests which move from HA queue to the cloud server queue. The arrival times of user requests depends in operation type.

The arrival times of patient requests are modeled as non probability distribution with arrival rate of WSN collected data creation requests (λ_{WSNs}). This arrival rate is the multiplication of number of connected patients ($NB_{Patients}$) by WSN sampling frequency (WSN_SAMP_Freq) as :

$$\lambda_{WSN} = NB_{Patients} \times WSN\_SAMP\_Freq$$

For other operation types the arrival times of user requests are modeled as Poisson distribution with corresponding arrival rate to operation type.

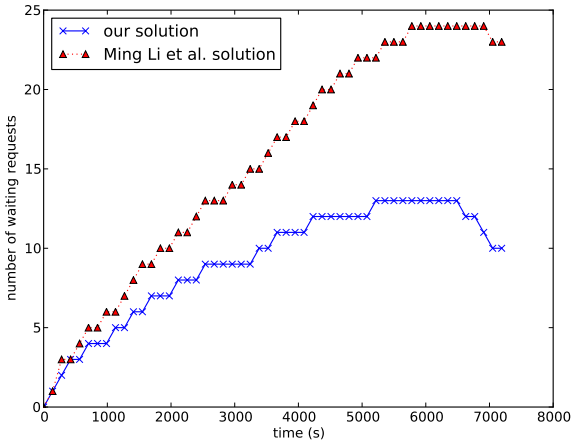


FIGURE 5.4 – Performance evaluation with emergency situations

5.5.1 Performance evaluation with emergency situations : fixed arrival rate

In the first scenario, we consider emergency situations together with the other types of operations. An emergency situation involves three phases where each phase results in one operation. These operations are respectively : emergency detection, emergency access and emergency revocation. In addition to our solution, we also evaluate break-glass access of Ming Li et al. [ML13] solution. In Ming Li et al.[ML13], each data available to emergency access is duplicated and encrypted with emergency key. To revoke emergency access rights, the data is re-encrypted with a new emergency key. The re-encryption of data after each emergency access induces high overhead costs, as shown in figure 5.4. However, in our solution we avoid this cost thanks to our break-glass access which is presented in section the next chapter.

5.5.2 Performance evaluation with emergency situations : variable arrival rate

In the second scenario, we vary the rate of emergency arrivals and we compute the mean response time, figure 5.5 shows that increasing the arrival rate of emergency increases the response time. However, this growth in response time is more important

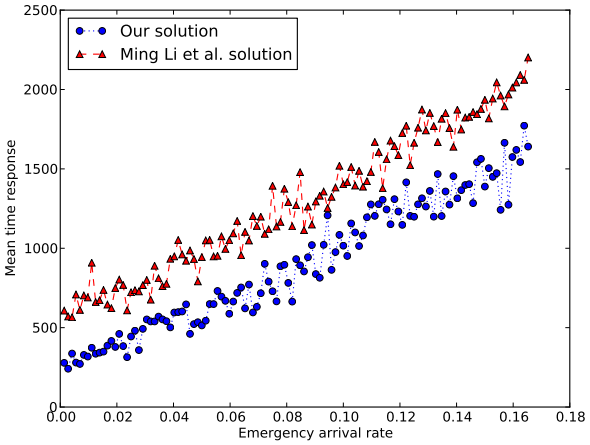


FIGURE 5.5 – Average waiting time according arrival rate (λ)

in Ming Li et al. [ML13] solution.

5.6 Conclusion

In this chapter, we propose a secure and scalable architecture for emergency management. This architecture leverages cloud computing technology for providing dynamically scale storage resources via on demand provisioning, and WSN technology for early emergency detection. In addition, we address the challenge of ABE integrating for emergency access in medical applications . Finally, we carried out some simulations that allowed showing that our scheme provides an efficient and fine-grained access control.

Chapitre 6

Conclusion and perspectives

6.1 Conclusion

Cloud computing has recently emerged as a new paradigm where resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings many new challenges for data security and access control when enterprises or organizations outsource sensitive data to take advantage of the cloud, which are not within the same trusted domain as their traditional infrastructures.

In this thesis, we considered data security challenges and issues due to using the cloud for critical applications. Specially, we have considered using the cloud storage for medical applications such as EMR systems and medical Wireless Sensor Net-

works. First, we have identified the benefits and risks of using the cloud for medical applications with a key focus on security and privacy issues.

After, we have investigated how to make the cloud more secure for medical applications. First, we have studied some security concepts related to our work. After that, we focused the background presentation on advanced cryptography methods, especially Attribute Based Encryption (ABE). Recently, this method has been gaining considerable attention as a useful technology for safe and secure storage of data in the cloud. Then, we addressed the challenge of secure data outsourcing in cloud computing. We have identified security threats of data outsourcing that cannot be solved by traditional access control techniques. This conclusion, drived us to investigate solutions relying on cryptographic access control that suites better to shared data protection.

The huge amount of high sensitive data generated and collected by medical wireless sensor networks introduces several challenges, such as scalability, availability, security, fine-grained access. In order to address some of theses challenges, we have proposed a secure and scalable architecture that leverages cloud computing technology to dynamically scale storage resources via on demand provisioning. Furthermore, we have proposed an innovative security scheme that eliminates potential security threats of medical data outsourcing and guarantees confidentiality and integrity without requiring patients or doctors interventions. To implement complex and dynamic security policies necessary to medical applications, we have developed a fine-grained access control that combines ciphertext-policy attributes based encryption and symmetric cryptography. This combination reduces the management overhead and the encryption/decryption time as we have shown through our performance evaluation. Finally, we have carried out extensive simulations which shows that our scheme provides an efficient, fine-grained and scalable access control.

WSNs for medical applications provide useful and real time information about patients' health state. This information should be available for healthcare providers

to facilitate response and to improve the rescue process of a patient during emergency. In the previous contribution, we have proposed an innovative cloud-based architecture for collecting and accessing large amount of data generated by medical sensor networks. We have integrated CP-ABE for providing a secure fine-grained access control over medical data outsourced on the cloud. However, for emergency management, integrating CP-ABE creates particular challenges for providing temporary access to patients medical data when this is needed. Therefore, we have developed an architecture for secure emergency management in healthcare area. The proposed architecture overcomes the challenges arising from using ABE for access control. In addition, we have used wireless sensor network (WSN) technology to provide early emergency detection.

From these contributions, we have identified some open research for the future that we summarize in what follows.

6.2 Perspectives

We identify three directions for future work for secure cloud services as follows.

6.2.1 User revocation

Chapter 4 presents our secure and scalable cloud-based architecture for medical applications. In this architecture, we have used Ciphertext-Policy Attribute Based Encryption (CP-ABE) to provide secure, scalable and fine-grained access control for medical applications. Although we have proposed revocation by implementing *temporary access control*, *immediate revocation* of users' keys is not supported by our previous solution.

In *temporary access control*, trusted authority generates users keys (represent users access privileges) by specifying exactly when users access ends (expiration time). Trusted authority should enable only non-revoked users to update their keys in order to continue accessing data. However, in practice, the validity period of access

privileges has to be small to reduce the window of vulnerability when a user key is compromised, e.g. a day, a week or a month. At the end of this period of time, the entire key will have to be re-generated and re-distributed with an updated expiration time imposing a heavy burden on the trusted authority and key distribution process [BKP09].

User revocation is an important issue of attribute-based encryption scheme. The initial scheme of CP-ABE proposed by Bethencourt et al. [BSW07] does not support immediate revocation of users' keys without issuing new keys to other users or re-encrypting existing ciphertexts. Consequently, this induces high computational overhead for key management and distribution. However, It may be necessary to remove keys from operational use prior to their originally scheduled expiry, for reasons including key compromise and key abuse.

Immediate revocation can be done by using CP-ABE scheme that supports negative clauses, proposed by Ostrovsky, Sahai and Waters [OSW07]. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance. Attrapadung and Imai [AI09b] proposed an ABE system with direct revocation. Such a system allows senders to specify the revocation list directly when encrypting. Therefore, revocation can be done instantly and does not require the key update phase as in temporary access control. Despite this clear advantage, in contrast, its disadvantage is that it requires senders to possesses the current revocation list. While the management of revocation list itself could be already a troublesome task, this requirement renders the system not being so purely attribute-based (An ideal attribute-based setting should allow users to just create ciphertext based solely on attributes and not to worry about revocation) [AI09a].

To tackle the challenge of revocation, we plan to develop a hybrid revocable access control which provides two revocation mechanisms : (1) *Temporary access* with adequate validity period to reduce computational overhead of key update. (2) *Immediate revocation* which is implemented by using users blacklist in encryption, and only non blacklist users can decrypt data. This solution reduces the window vulnerability when a user key is compromised without heavy computational overhead. In addition, we aim to protect access policies especially users blacklist in order to give

revoked users the chance to return to the system. To do so, we will rely on a ABE scheme with hidden access policies (see chapter 3).

6.2.2 Intercloud

In this thesis, we have proposed a secure and scalable architecture that leverages a single cloud to dynamically scale storage resources via on demand provisioning. We have tackled the challenge of security data stored in the cloud by developing a fine-grained access control. However, challenges due to a single cloud including reliability of data stored in the cloud and lock-in (see chapter 2), are not addressed here. Several works [BCQ+11, APST12, CHV10, BRC10] have recently been conducted in order to address the challenges of a single cloud, by proposing "intercloud" or "cloud of clouds" model (Intercloud is an interconnected global cloud of clouds). This new model still needs to be more developed to address various challenges including security [BV10] and fault-tolerance. We can cite the encryption of sensitive data stored in the cloud that involves utmost need of new robust and scalable key management mechanisms.

6.2.3 ABE-SSL : Towards Virtual Private Networks Over Clouds

In our access control, we have used ABE to provide security of data at rest, and SSL protocol to provide security of data in transit. However, This separation induces some redundancies including ABE key management, SSL public key management, ABE session key, SSL session key, etc. To the best of our knowledge, there is no work that provides ABE-based SSL protocol, in other words, tunneling protocol relying on ABE. We believe that a ABE-SSL protocol can eliminate redundancies, improve performances and simplify key management. Moreover, This generic protocol can be very useful for deploying virtual private networks over clouds.

We believe that some of the ideas presented in this thesis pave the way for secure sharing over the clouds and represent a good basis tackle the aforementioned future

directions.

Bibliographie

[AI09a] Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting Direct/Indirect revocation modes. In Matthew G. Parker, editor, *12th IMA International Conference.*, volume 5921 of *Lecture Notes in Computer Science*, pages 278–300. Springer, 2009.

[AI09b] Nuttapong Attrapadung and Hideki Imai. Conjunctive broadcast and attribute-based encryption. In Hovav Shacham and Brent Waters, editors, *Pairing 2009,*, volume 5671 of *Lecture Notes in Computer Science*, pages 248–265. Springer Berlin Heidelberg, January 2009.

[All13] Marshall Allen. How many die from medical mistakes in u.s. hospitals ? *ProPublica, Journalism in the Public Interest*, 2013.

[APST12] M.A. AlZain, E. Pardede, B. Soh, and J.A. Thom. Cloud computing security : From single to multi-clouds. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 5490–5499, Jan 2012.

[ASMR11] José A Afonso, Helder D Silva, Pedro Macedo, and Luis A Rocha. Design and implementation of a wireless sensor network applied to motion capture. In *Portuguese conference on wireless sensor networks*, Coimbra, Portugal, March 2011.

[BBS98] Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In *In EUROCRYPT*, pages 127–144. Springer-Verlag, 1998.

[BCHL09] Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter. Patient

controlled encryption : ensuring privacy of electronic medical records. In *Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW '09*, pages 103–114, New York, NY, USA, 2009.

[BCQ+11] Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando André, and Paulo Sousa. Depsky : Dependable and secure storage in a cloud-of-clouds. In *Proceedings of the Sixth Conference on Computer Systems*, EuroSys '11, pages 31–46, New York, NY, USA, 2011. ACM.

[BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3) :586–615, March 2003.

[BFR+06] D. Brunelli, E. Farella, L. Rocchi, M. Dozza, L. Chiari, and L. Benini. Bio-feedback system for rehabilitation based on a wireless body area network. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, pages 527–531, Pisa, Italy, 2006.

[BKP09] Rakesh Bobba, Himanshu Khurana, and Manoj Prabhakaran. Attribute-Sets : a practically motivated enhancement to Attribute-Based encryption. *Computer Security ESORICS'09*, pages 587–604, 2009.

[BLL02] O. Boric-Lubeke and V.M. Lubecke. Wireless house calls : using communications technology for health care and monitoring. *Microwave Magazine, IEEE*, 3(3) :43–48, Sep 2002.

[BLLS11] Mrinmoy Barua, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. ESPAC : enabling security and patient-centric access control for eHealth in cloud computing. *International Journal of Security and Networks*, 6(2/3) :67–76, November 2011.

[BPW10] Achim D. Brucker, Helmut Petritsch, and Stefan G. Weber. Attribute-Based encryption with Break-Glass. In *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*. Springer Berlin Heidelberg, 2010.

[BRC10] Rajkumar Buyya, Rajiv Ranjan, and Rodrigo N Calheiros. Intercloud : Utility-oriented federation of cloud computing environments for scaling

of application services. In *Algorithms and architectures for parallel processing*, pages 13–31. Springer, 2010.

[BSW07] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based encryption. In *Proceedings of the IEEE Symposium on Security and Privacy, SP '07*, pages 321–334, Washington, DC, USA, 2007.

[BV10] David Bernstein and Deepak Vij. Intercloud security considerations. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, pages 537–544. IEEE, 2010.

[BYV+09] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. Cloud computing and emerging IT platforms : Vision, hype, and reality for delivering computing as the 5th utility. *Journal of Future Generation Computer Systems*, 25(6) :599–616, June 2009.

[Cha07] Melissa Chase. Multi-authority attribute based encryption. In *Proceedings of the 4th Conference on Theory of Cryptography*, TCC'07, pages 515–534, Berlin, Heidelberg, 2007. Springer-Verlag.

[CHV10] Christian Cachin, Robert Haas, and Marko Vukolic. Dependable storage in the intercloud. *IBM Research*, 3783 :1–6, 2010.

[Clo13] Clouds. The types of clouds - public, private, hybrid, community. *Online at http ://techshakes.com/the-types-of-cloud-public-private-hybrid/*, 2013.

[dVFJ+07] Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Over-encryption : management of access control evolution on outsourced data. In *Proceedings of the 33rd international conference on Very large data bases*, VLDB '07, pages 123–134, 2007.

[EHR] Electronic health record. *Online at http ://en.wikipedia.org/w/index.php ?title=Electronic_ health_ record.*

[FAL06] K. Frikken, M.J. Atallah, and Jiangtao Li. Attribute-based access control with hidden policies and hidden credentials. *IEEE Transactions on Computers*, 55(10) :1259–1270, 2006.

[FIP] Fair information practices (fip). *Online at http ://whatis.techtarget.com/definition/Fair-Information-Practices-FIP.*

[FPE10] R.R. Fletcher, Ming-Zher Poh, and H. Eydgahi. Wearable sensors : Opportunities and challenges for low-cost health care. In *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*, pages 1763–1766, Aug 2010.

[Fu99] Kevin E Fu. *Group sharing and random access in cryptographic storage file systems.* PhD thesis, Citeseer, 1999.

[GCAM08] Óscar Gama, Paulo Carvalho, J. A. Afonso, and P. M. Mendes. Quality of service support in wireless sensor networks for emergency healthcare services. In *EMBC 2008*, pages 1296–1299, August 2008.

[GHW11] Matthew Green, Susan Hohenberger, and Brent Waters. Outsourcing the decryption of ABE ciphertexts. In *USENIX Security Symposium*, pages 34–34, Berkeley, CA, USA, 2011.

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security, CCS '06*, pages 89–98, New York, NY, USA, 2006.

[GSMB03] Eu-jin Goh, Hovav Shacham, Nagendra Modadugu, and Dan Boneh. Sirius : Securing remote untrusted storage. *Network and distributed systems security, NDSS'03*, pages 131—145, 2003.

[HFK+13] Vincent C Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. Guide to attribute based access control (abac) definition and considerations. *NIST Special Publication*, 800, 2013.

[HJ03] Anthony Harrington and Christian Jensen. Cryptographic access control in a distributed file system. In *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies*, SACMAT '03, pages 158–165, New York, NY, USA, 2003. ACM.

[HSH09] Mohammad Mehedi Hassan, Biao Song, and Eui-Nam Huh. A framework of sensor-cloud integration opportunities and challenges. In *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, ICUIMC '09*, pages 618–626, New York, NY, USA, 2009.

[HSM13] Jinguang Han, Willy Susilo, and Yi Mu. Identity-based data storage in cloud computing. *Future Generation Computer Systems*, 29(3) :673 – 681, 2013. Special Section : Recent Developments in High Performance Computing and Security.

[IAP09] L. Ibraimi, M. Asim, and M. Petkovic. Secure management of personal health records by applying attribute-based encryption. In *6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health, pHealth'09*, pages 71–74, Oslo, Norway, June 2009.

[ISO89] ISO7498. Iso7498-2 : 1989. *Information processing systems-Open Systems Interconnection*, 1989.

[JB11] Brent Waters John Bethencourt, Amit Sahai. Cp-abe library. *Online at http ://acsc.cs.utexas.edu/cpabe/*, 2011.

[KB09] Werner Kurschl and Wolfgang Beer. Combining cloud computing and wireless sensor networks. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services, iiWAS '09*, pages 512–518, New York, NY, USA, 2009.

[KKVG12] Tridib Mukherjee Krishna K. Venkatasubramanian and Sandeep K. S. Gupta. Caac - an adaptive and proactive access control approach for emergencies for smart infrastructures. *ACM Transactions on Autonomous and Adaptive Systems Special Issue on Adaptive Security*, 2012.

[KPS02] Charlie Kaufman, Radia Perlman, and Mike Speciner. *Network Security : Private Communication in a Public World, Second Edition.* Prentice Hall, 2002.

[KRS+03] Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian Wang, and Kevin Fu. Plutus : Scalable secure file sharing on untrusted storage. In *Proceedings of the 2nd USENIX Conference on File and Storage Technologies*, pages 29–42, Berkeley, CA, USA, 2003. USENIX Association.

[KTS07] Apu Kapadia, Patrick P. Tsang, and Sean W. Smith. Attribute-based publishing with hidden credentials and hidden policies. In *In The 14th Annual Network and Distributed System Security Symposium (NDSS*, pages 179–192, 2007.

[KVH+10] A. M Khattak, La The Vinh, Dang Viet Hung, Phan Tran Ho Truc, Le Xuan Hung, D. Guan, Z. Pervez, Manhyung Han, Sungyoung Lee, and Young-Koo Lee. Context-aware human activity recognition and decision making. In *12th IEEE International Conference on e-Health Networking Applications and Services, Healthcom'10*, pages 112–118, Lyon, France, July 2010.

[LDL12] Junzuo Lai, Robert H. Deng, and Yingjiu Li. Expressive CP-ABE with partially hidden access structures. In Heung Youl Youm and Yoojae Won, editors, *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '12, pages 18–19, New York, NY, USA, 2012. ACM.

[LLR10] Ming Li, Wenjing Lou, and Kui Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1) :51–58, February 2010.

[LMHJ10] K. Lee, D. Murray, D. Hughes, and W. Joosen. Extending sensor networks into the cloud using amazon web services. In *IEEE International Conference on Networked Embedded Systems for Enterprise Applications, NESEA'10*, pages 1–7, Suzhou, China, November 2010.

[LRK09] Jin Li, Kui Ren, and Kwangjo Kim. A2BE : accountable attribute-

based encryption for abuse free access control. *IACR Cryptology ePrint Archive*, (118) :118, 2009.

[LRZW09] Jin Li, Kui Ren, Bo Zhu, and Zhiguo Wan. Privacy-aware attribute-based encryption with user accountability. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio A. Ardagna, editors, *Information Security*, number 5735 in Lecture Notes in Computer Science, pages 347–362. Springer Berlin Heidelberg, January 2009.

[LW11a] Allison Lewko and Brent Waters. Decentralizing attribute-based encryption. In *Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques : Advances in Cryptology*, EUROCRYPT'11, pages 568–588, Berlin, Heidelberg, 2011. Springer-Verlag.

[LW11b] Ruoshui Liu and Ian J. Wassell. Opportunities and challenges of wireless sensor networks using cloud services. In *Proceedings of the workshop on Internet of Things and Service Platforms, IoTSP '11*, pages 41–47, New York, NY, USA, 2011.

[LYRL10] Ming Li, Shucheng Yu, Kui Ren, and Wenjing Lou. Securing personal health records in cloud computing : Patient-Centric and Fine-Grained data access control in multi-owner settings. In *Security and Privacy in Communication Networks*, volume 50, pages 89–106. Springer Berlin Heidelberg, 2010.

[MKL09] Tim Mather, Subra Kumaraswamy, and Shahed Latif. *Cloud security and privacy.* O'Reilly, Beijing ; Cambridge [Mass.], 2009.

[ML13] Y. Zheng K. Ren et W. Lou M. Li, S. Yu. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption . *IEEE Transactions on Parallel and Distributed Systems*, 24 :131 –143, 2013.

[MVOV96] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography.* CRC press, 1996.

[NAH08] The national alliance for health information technology report to the office of the national coordinator for health information technology on defining key health information technology terms, August 2008.

[NIS10] NIST. Privilege (access) management workshop collaboration team. Technical report, National Institute of Standards and Technology, 2010.

[NKVV13] Venetia Notara, Konstantinos Koulouridis, Aristidis Violatzis, and Elissabet Vagka. Economic crisis and health. the role of health care professionals. *Health Science Journal*, 7(2), 2013.

[NYO08] Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. In *Applied cryptography and network security*, pages 111–129. Springer, 2008.

[Org05] World Health Organization. WHO | preventing chronic diseases : a vital investment. *Online at http ://www.who.int/chp/chronic$_d$isease$_r$eport/contents/en/*, 2005.

[OSW07] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM conference on Computer and communications security*, CCS '07, pages 195–203, New York, NY, USA, 2007. ACM.

[PRI] International privacy laws. *Online at http ://www.informationshield.com/intprivacylaws.html.*

[PT11] Mell Peter and Grance Timothy. The nist definition of cloud computing. Technical Report NIST SP 800-145, National Institute of Standards and Technology, september 2011.

[RGPA10] V. Rajesh, J. M Gnanasekar, R. S Ponmagal, and P. Anbalagan. Integration of wireless sensor network with cloud. In *International Conference on Recent Trends in Information, Telecommunication and Computing, ITC'10*, pages 321–323, Kochi, India, March 2010.

[RKW+10] C. O Rolim, F. L Koch, C. B Westphall, J. Werner, A. Fracalossi, and G. S Salvador. A cloud computing solution for patient's data collection in health care institutions. In *Second International Conference on*

eHealth, Telemedicine, and Social Medicine, ETELEMED '10, pages 95–99, St. Maarten, Netherlands Antilles, 2010.

[Shi07] Robert W. Shirey. Internet security glossary, version 2, 2007.

[Sin02] Munindar P Singh. Treating health care [being interactive]. *Internet Computing, IEEE*, 6(4) :4–5, 2002.

[SNO+08] M. Soini, J. Nummela, P. Oksa, L. Ukkonen, and L. Sydanheimo. Wireless body area network for hip rehabilitation system. *Ubiquitous Computing and Communication Journal*, 3 :7, 2008.

[SW05] Amit Sahai and Brent Waters. Fuzzy Identity-Based encryption. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer, 2005.

[TCN+13] Danan Thilakanathan, Shiping Chen, Surya Nepal, Rafael Calvo, and Leila Alem. A platform for secure monitoring and sharing of generic health data in the cloud. *Future Generation Computer Systems*, 2013.

[TH12] Lionel Dupré Thomas Haeberlen. Cloud computing : Benefits, risks and recommendations for information security. Technical report, The European Network and Information Security Agency (ENISA), December 2012.

[Var07] Upkar Varshney. Pervasive healthcare and wireless health monitoring. *Mobile Networks and Applications*, 12(2-3) :113–127, 2007.

[vir14] Virtualization. *Online at http ://en.wikipedia.org/w/index.php ?title=Virtualization*, 2014.

[WLOB09] Weichao Wang, Zhiwei Li, Rodney Owens, and Bharat Bhargava. Secure and efficient access to outsourced data. In *Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW '09*, pages 55–66, New York, NY, USA, 2009.

[YWRL10a] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM*, pages 1–9, 2010.

[YWRL10b] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Attribute based data sharing with attribute revocation. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS '10*, pages 261–270, New York, NY, USA, 2010.

[ZBS98] Erez Zadok, Ion Badulescu, and Alex Shender. Cryptfs : A stackable vnode level encryption file system. Technical report, Citeseer, 1998.

[ZHA+12] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wang. Towards temporal access control in cloud computing. In *INFOCOM, 2012 Proceedings IEEE*, pages 2576–2580, March 2012.