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

Ahmed Lounis, Abdelmadjid Bouabdallah, Abdelkrim Hadjidj, Yacine Challal

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

Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah and Yacine Challal
{lounisah,ahadjidj,bouabdal,ychallal}@utc.fr
Université de Technologie de Compiègne
HEUDIASYC UMR CNRS 7253
BP 20529, Compiègne Cedex
France

***Abstract*—Recently introduced, Attribute-based encryption (ABE) is a promising cryptographic method proposed by Sahai and Waters. This technique provides means for designing scalable and fine-grained access control. In ABE, data are encrypted with an access 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. This makes ABE good solution to provide a fine-grained access control for medical applications, where data is outsourced on untrusted servers like the case of the Cloud. However, for emergency management, integrating ABE creates particular challenges for providing temporary access victims medical data when this is needed. In this paper 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.**

Keywords: Healthcare, Attribute based encryption, Emergency access control, Cloud computing, security.

I. Introduction

Emergency management is an essential field of medical services. Healthcare emergency consists in to provide first aid for person who needs immediate care. Then, where necessary to transport victim to healthcare 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 or 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.

The wireless sensor networks (WSN) is among the technologies that have had the greatest success in medical applications. Recent advances in medical sensors, wireless technologies and Micro-Electro-Mechanical systems have enabled the development of sensor nodes capable of sensing, processing and communicating several physiological signs. These lightweight miniaturized nodes collaborate to form a wireless sensor network that simplifies 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 enables to healthcare professionals to be timely aware of emergency case concern patients. Also, health information collected by sensor can be used to determine the cause of the incident.

A lot of research works are proposed, which enable to store and sharing patients' medical data between different healthcare professionals in order to privilege best knowing of patient and best health following. These solutions addressed challenges involved by storing and accessing medical data such scalability, security, availability, etc. Recently, there are research works [1], [2], [3], [4], [5], [6] which are motived by the cloud storage. these solutions proposed to outsource medical data on the cloud to benefice of advantages offered by the cloud. Indeed, the cloud for medical data storage provides a dynamic scalability via on-demand resource provisioning and virtually infinite data storage capacity. the Cloud computing eases storage, processing and sharing of medical data and provides anywhere/anytime access to medical data. However, considering social, ethical and legal aspects of medical systems, medical data is highly sensitive and should be managed properly to guarantee patients privacy. Hence, how to secure outsourcing medical data on the cloud is a challenging problem, since a cloud environment cannot been considered to be trusted. Also, access to medical data is often governed by complex policies that distinguish between each part of the data and each user privileges. Moreover, access in emergency case should be considered, where emergency staff need a temporary privileges enable them to ensure best knowing of victim over his medical data. Therefore, providing fine-grained access control that supports dynamic and complex organizational policies in normal and emergency situations 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 a lot of research works have been carried out in medical data outsourced on the cloud, only few studies have considered emergency management.

Recently introduced, Attribute-based encryption (ABE) is a promising cryptographic method proposed by Sahai and Waters [7]. The ABE provides means for designing scalable fine-grained access control. In ABE, data are encrypted with an access 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. This makes ABE good solution ideal technique to provide a fine-grained access control over medical data outsourced on the cloud. However, for emergency management, integrating ABE creates particular challenges for providing temporary access victims medical data when this is needed.

In this paper, 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 paper is organized as follows. In section II we review some related works. In section III we describe our proposed architecture. In section IV we present the implementation of our emergency access control with ABE. In section V, we provide simulation results and performance evaluation of our scheme compared to representative schemes from literature. In section VI we conclude the paper.

II. Related work

Attribute-based encryption (ABE) is a promising cryptographic method proposed by Sahai and Waters in 2005 [7]. The ABE technique extends the identity-based encryption to enable expressive access policies and fine-grained access to encrypted data. With 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 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 1). 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.

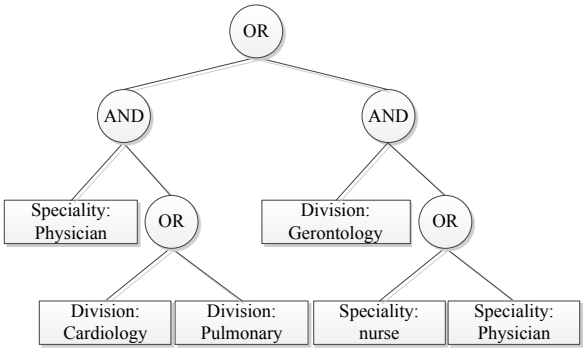

Fig. 1. An access tree T

In figure 1, 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) [8] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [9] 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 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 of CP-ABE necessary for understanding of our architecture. More extensive description of CP-ABE is available in [9].

In [1] 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 [1] 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,

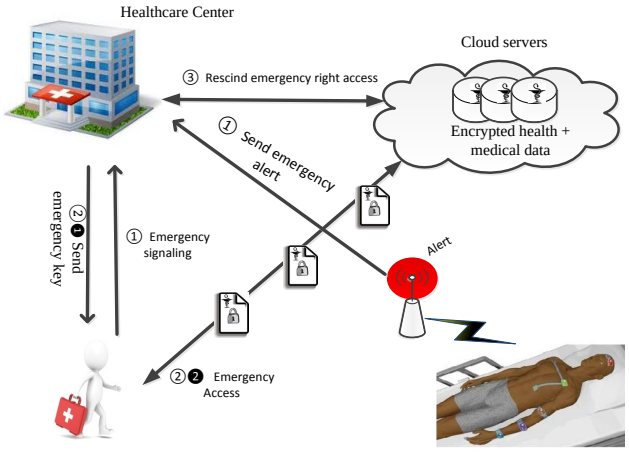

Fig. 2. Example of Emergency intervention

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 [10] 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 [11], 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 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.

III. Our architecture

In this section, we present our architecture described in figure 2, 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 2, 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.

IV. Implementation with ABE

The using ABE only for regular access control provides an unique access structure (regular access policy) to encrypt

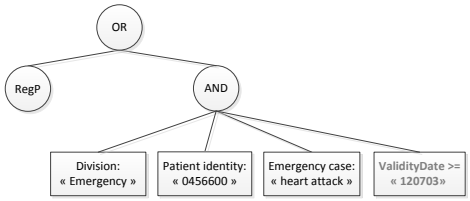

Fig. 3. An example of access structure for break-glass access

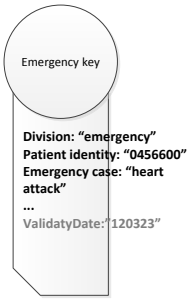

Fig. 4. Emergency key

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 3. 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 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. [9] 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.

V. 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 consider three operations: read a file from the cloud, write a file on the cloud and create a file on the cloud.

In a first scenario,we consider emergency situations together with previous 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. [1] solution. In Ming Li et al.[1], 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. However, in our solution we avoid this cost thanks to our break-glass access which is presented in section IV.

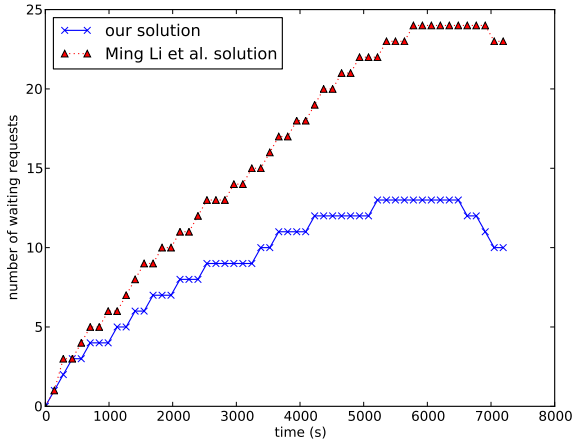

Fig. 5. Performance evaluation with emergency situations

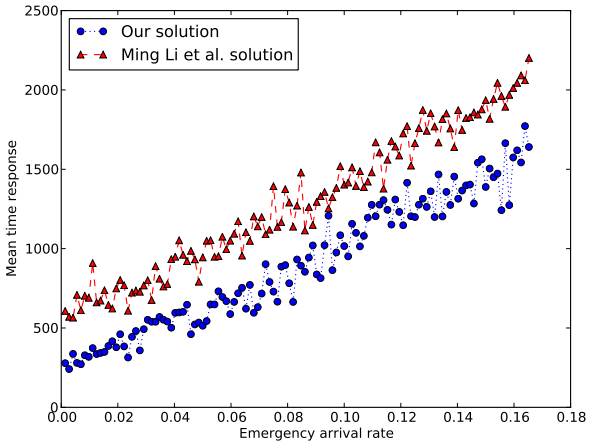

Fig. 6. Average waiting time according arrival rate (λ)

In the second scenario, we vary the rate of emergency arrivals and we compute the mean response time, figure 6 shows that increasing the arrival rate of emergency increases the response time. However, this growth in response time is more important in Ming Li et al. [1] solution.

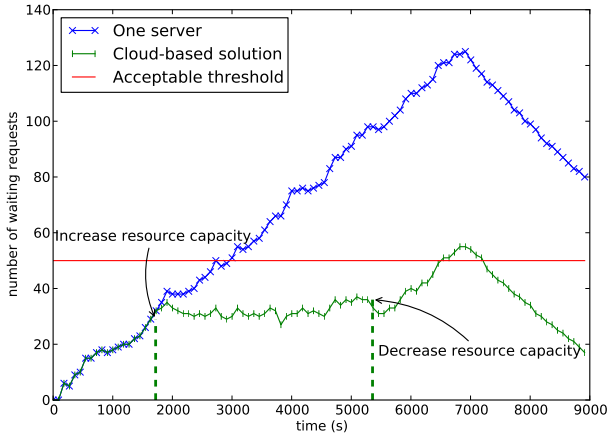

Fig. 7. Performance evaluation of our solution without/with the cloud

In the third 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 7 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 7 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).

VI. Conclusion

In this paper, 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.

References

[1] Y. Z. K. R. e. W. L. 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*, vol. 24, pp. 131 –143, 2013.

[2] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, ser. SPSM '11. New York, NY, USA: ACM, 2011, p. 7586.

[3] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: enabling security and patient-centric access control for eHealth in cloud computing," *International Journal of Security and Networks*, vol. 6, no. 2/3, pp. 67–76, Nov. 2011.

[4] O. Akan, P. Bellavista, J. Cao, F. Dressler, D. Ferrari, M. Gerla, H. Kobayashi, S. Palazzo, S. Sahni, X. S. Shen, M. Stan, J. Xiaohua, A. Zomaya, G. Coulson, M. Li, S. Yu, K. Ren, and W. 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*. Springer Berlin Heidelberg, 2010, vol. 50, pp. 89–106.

[5] 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*, Oslo, Norway, Jun. 2009, pp. 71–74.

[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW '09*, New York, NY, USA, 2009, pp. 103–114.

[7] A. Sahai and B. Waters, "Fuzzy Identity-Based encryption," in *Lecture Notes in Computer Science*, vol. 3494, 2005, pp. 457–473.

[8] V. Goyal, O. Pandey, A. Sahai, and B. 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*, New York, NY, USA, 2006, pp. 89–98.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy, SP '07*, Washington, DC, USA, 2007, pp. 321–334.

[10] A. D. Brucker, H. Petritsch, and S. 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.

[11] T. M. Krishna K. Venkatasubramanian and S. 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.