ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Issue 4, April 2016

Patient Self-Controllable And Multi-Level Privacy-preserving cooperative Authendication Based on ECC

J.Mohammad Bilal
M.E.,Computer Science and Engineering,
Mohamed Sathak Engineering college,
Kilaklarai.
Mohammadbilal1987@gmail.com

Mr. S.Ramamoorthy M.E
Assistant Professor, Computer Science and Engineering,
Mohamed Sathak Engineering college,
Kilaklarai.

Abstract— **In the Medical Consultation, the efficient patient treatment was given by the Distributed m-healthcare cloud computing which allows for sharing health information among healthcare providers. Here a challenge is that keeping the data confidentiality and patients' identity privacy simultaneously. To solve this kind of problem, an Elliptical Curve Cryptography (ECC) algorithm is established. Here the Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. We propose a new technique, an attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) which realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Then, the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.**

Keywords*— *Authentication, access control, security and privacy, distributed cloud computing, m-healthcare system

Introduction

Distributed system for cloud is a file system that allows many clients to have access to the same data/file providing important operations (create, delete, modify, read, write). Each file may be partitioned into several parts called chunks. Each chunk is stored in remote machines. Typically, data is stored in files in a hierarchical tree where the nodes represent the directories. Hence, it facilitates the parallel execution of applications. There are several ways to share files in a distributed architecture. Each solution must be suitable for a certain type of application relying on how complex is the application, or how simple it is. Meanwhile, the security of the system must be ensured. Confidentiality, availability and integrity are the main keys for a secure system.

Now a days, users can share resources from any computer/device, anywhere and everywhere through internet thanks to cloud computing which is typically characterized by the scalable and elastic resources - such as physical servers, applications and any services that are virtualized and allocated dynamically. Thus, synchronization is required to make sure that all devices are up-to-date.

Distributed file systems enable also many big, medium and small enterprises to store and access their remote data exactly as they do locally, facilitating the use of variable resources.
In the fast growing world, mHealth is one aspect of eHealth that is pushing the limits of how to acquire, transport, store, process, and secure the raw and processed data to deliver meaningful results. mHealth offers the ability of remote individuals to participate in the health care value matrix, which may not have been possible in the past. Participation does not imply just consumption of health care services. In many cases remote users are valuable contributors to gather data regarding disease and public health concerns such as outdoor pollution, drugs and violence.
The motivation behind the development of the mHealth field arises from two factors. The first factor concerns the myriad constraints felt by healthcare systems of developing nations. These constraints include high population growth, a high burden of disease prevalence, low health care workforce, large numbers of rural inhabitants, and limited financial resources to support healthcare infrastructure and health information systems. The second factor is the recent rapid rise in mobile phone penetration in developing countries to large segments of the healthcare workforce, as well as the population of a country as a whole. With greater access to mobile phones to all segments of a country, including rural areas, the potential of lowering information and transaction costs in order to deliver healthcare improves.

Nowadays, mHealth (also written as m-health) is an abbreviation for mobile health, a term used for the practice of medicine and public health supported by mobile devices. The term is most commonly used in reference to using mobile communication devices, such as mobile phones, tablet computers and PDAs, for health services and information, but

also to affect emotional states. The mHealth field has emerged as a sub-segment of eHealth, the use of information and communication technology (ICT), such as computers, mobile phones, communications satellite, patient monitors, etc., for health services and information. mHealth applications include the use of mobile devices in collecting community and clinical health data, delivery of healthcare information to practitioners, researchers, and patients, real-time monitoring of patient vital signs, and direct provision of care (via mobile telemedicine).

While mHealth certainly has application for industrialized nations, the field has emerged in recent years as largely an application for developing countries, stemming from the rapid rise of mobile phone penetration in low-income nations. The field, then, largely emerges as a means of providing greater access to larger segments of a population in developing countries, as well as improving the capacity of health systems in such countries to provide quality healthcare. Within the mHealth space, projects operate with a variety of objectives, including increased access to healthcare and health-related information (particularly for hard-to-reach populations); improved ability to diagnose and track diseases; timelier, more actionable public health information; and expanded access to ongoing medical education and training for health workers.

According to an analyst firm, around 2.8 million patients worldwide were using a home monitoring service based on equipment with integrated connectivity at the end of 2012. The figure does not include patients that use monitoring devices connected to a PC or mobile phone. It only includes systems that rely on monitors with integrated connectivity or systems that use monitoring hubs with integrated cellular or fixed-line modems. It forecast that the number of home monitoring systems with integrated communication capabilities will grow at a compound annual growth rate (CAGR) of 26.9 percent between 2011 and 2017 reaching 9.4 million connections globally by the end of the forecast period. The number of these devices that have integrated cellular connectivity increased from 0.73 million in 2011 to about 1.03 million in 2012, and is projected to grow at a CAGR of 46.3 percent to 7.10 million in 2017.

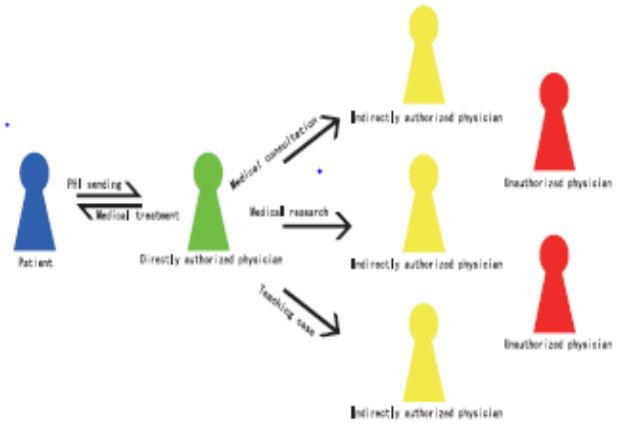
Data security, according to common definition is the "confidentiality, integrity and availability" of data. It the practice of ensuring that the data being stored is safe from unauthorized access and use, ensuring that the data is reliable and accurate and that it is available for use when it is needed.

Privacy, on the other hand, is the appropriate use of information. In other words, merchants and companies should use the data provided to them only for the intended purpose.

Privacy is the true objective of security. In the world of regulatory compliance, data security and privacy issues for some time now, and it is rare that I've seen companies undertake security for the sake of security. Most often, security programs are put in place to protect the privacy of consumers' information. Without appropriate security programs in place, it is very difficult to ensure that no unauthorized access or use (referred to above as "appropriate use") of consumer information has taken place.

Authentication is the act of confirming the truth of an attribute of a single piece of data (a datum) claimed true by an entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

In the fields of physical security and information security, access control is the selective restriction of access to a place or other resource. The act of *accessing* may mean consuming, entering, or using. Permission to access a resource is called *authorization*



I. MODELS AND DESIGN GOALS

In this section, we formalize the system model, security model, and identify our design goals.

A. System Model

Our system model is composed of the following parties: In this, Project we consider simultaneously achieving data Confidentiality and identity privacy with high efficiency. As is described in Fig. 1, in distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information and verify the patient's identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes (i.e., since they are not authorized by the patients, we use the term 'indirectly authorized' instead).

They can only access the personal health information, but not the patient's identity. For the unauthorized persons with red labels, nothing could be obtained. By extending the techniques of attribute based access control [22] and designated verifier signatures (DVS) [21] on de-identified health information [27], we realize three different levels of privacy-preserving requirement mentioned above. The main contributions of this paper are summarized as follows.

(1) A novel authorized accessible privacy model (AAPM) for the multi-level privacy-preserving cooperative authentication is established to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates.

(2) Based on AAPM, a patient self-controllable multilevel privacy-preserving cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system is proposed, realizing three different levels of security and privacy requirement for the patients.

(3) The formal security proof and simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving capability, computational, communication and storage overhead.

The rest of this paper is organized as follows. We discuss related work in the next section. In Section 3, the network model of a distributed m-healthcare cloud computing system is illustrated.

.

II. EXISTING SYSTEM

In the Existing system, by considering simultaneously achieving data confidentiality and identity privacy with high efficiency, the members are classified into three categories with the three different kinds of labels. They are directly authorized physicians with green label who are in the local healthcare provider. They are authorized by the patients and can both access the patient's personal health information and verify the patient's identity. And the second category is indirectly authorized persons with yellow labels, who are authorized by the direct physicians for their medical consultant and research process about the disease; here these peoples are not authorized by the patients. And the final category is the unauthorized persons with red label. The formal security proof and simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving capability, computational, communication and storage overhead.

Disadvantages

- Storage overhead is high when compared to others.
- Communication overhead is same with the different threshold value.

III. SYSTEM ARCHITECTURE

The basic e-healthcare system illustrated in Fig. 2 mainly consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers [1], [2]. The patient's personal health information is securely transmitted to the healthcare provider for the authorized physicians to access and perform medical treatment.

We further illustrate the unique characteristics of distributed m-healthcare cloud computing systems where all the personal health information can be shared among patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare providers and medical research institutions for medical consultation. A typical architecture of a distributed m-healthcare cloud computing system is shown in Fig. 3. There are three distributed healthcare providers A; B;C and the medical research institution D, where Dr. Brown, Dr. Black, Dr. Green and Prof. White are working respectively. Each of them possesses its own cloud server. It is assumed that patient P registers at hospital A, all her/his personal health information is stored in hospital A's cloud server, and Dr. Brown is one of his directly authorized physicians. For medical consultation or other research purposes in cooperation with hospitals B;C and medical research institution D, it is required for Dr. Brown to generate three indistinguishable transcript simulations of patient P's personal health information and share them among the distributed cloud servers of the hospitals B;C and medical research institution D.

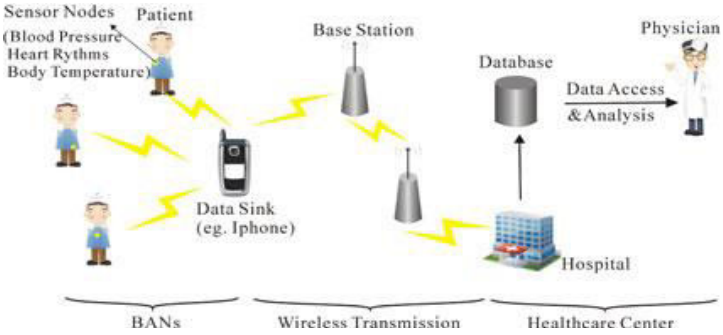


Fig 2 An basic architecture of the e-health system

IV. PROPOSED SYSTEM

We design a new framework called M-Healthcare Cloud Computing system which includes reduction of the storage overhead, communication overhead and improves the security by using the elliptical curve cryptography encryption algorithm that generates the key which is given to the patients

and to the healthcare providers for the secure transaction of messages and for the secret communication. Finally, our framework results the resultant graph that shows storage overhead, communication overhead, privacy-preserving capability, computational overhead and the enhanced security process.

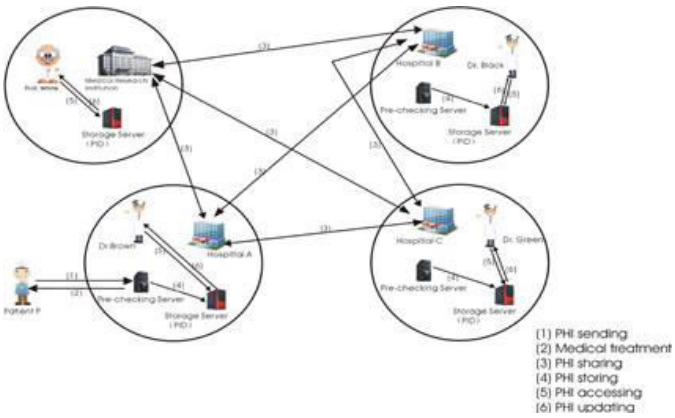


Fig 5.1 proposed system Architecture

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

1) ***Key Generation***

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number'd' within the range of **'n'**.

Using the following equation we can generate the public key

2) ***Q = d * P***

d = the random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve.

'Q' is the public key and'd' **is the private key.**

3)

4) *Encryption*

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Conside *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

5) ***C1 = k*P***

6) *C2 = M + k*Q*

C1 and C2 will be sending.

7) ***Decryption***

We have to get back the message 'm' that was send to us,

8) *M = C2 – d * C1*

M is the original message that we have send.

9) ***Proof***

How does we get back the message,

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (canceling out k * d * P)

= M (Original Message)

Fig 5.2 Data flow diagram

The above figure shows how data has been transferred from one module to another module, it explains the data flow from the node creation to graph generation,.
We design a new privacy model that solves the problem of how to protect both the patients' data confidentiality and identity privacy in the distributed m-healthcare cloud computing scenario under the malicious model which was left untouched.

Advantages

- Provides secure transmission of information
- Provides high data confidentiality and identity privacy simultaneously compared with existing system

V. SECURITY ANALYSIS

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

1) Symmetric key encryption

- In symmetric-key schemes, the encryption and decryption keys are the same.
- Communicating parties must have the same key before they can achieve secure communication.

2) Public key encryption:

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read. Here before then all encryption schemes were symmetric-key (also called private-key)

Public-key algorithms are based on mathematical problems that currently admit no efficient solution and are inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate a public and private key-pair and to use it for encryption and decryption. The strength lies in the "impossibility" (computational impracticality) for a properly generated private key to be determined from its corresponding ublic key. Thus the public key may be published without compromising security. Security depends only on keeping the private key private. Public key algorithms, unlike symmetric key algorithms, do *not* require a secure channel for the initial exchange of one (or more) secret keys between the parties.

VI. CONCLUSION

The privacy model process starts, by considering simultaneously achieving data confidentiality and identity privacy with high efficiency, the members are classified into three categories with the three different kinds of labels. They are directly authorized physicians with green label who are in the local healthcare provider. These peoples are authorized by the patients and can both access the patient's personal health information and verify the patient's identity. And the second category is indirectly authorized persons with yellow labels, who are authorized by the direct physicians for their medical consultant and research process about the disease; here these peoples are not authorized by the patients. And the final category is the unauthorized persons with red label. Our simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Issue 4, April 2016

capability, computational, communication and storage overhead. In our future work, we implement the framework called M-Healthcare Cloud Computing system which includes reduction of the storage overhead, communication overhead and improves the security by using the elliptical curve cryptography encryption algorithm which generates the key which is given to the patients and to the healthcare providers for the secure communication

References

1. J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 66–73, Feb. 2010.
2. X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for Ehealth systems," IEEE J. Sel. Areas Commun., vol. 27, no. 4, pp. 365–378, May 2009.
3. J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 373–382.
4. L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L. M. Ni, and J. Ma, "Pseudo trust: Zero-knowledge authentication in anonymous P2Ps," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1325–1337, Oct. 2008.
5.
6. J. Zhou and M. He, "An improved distributed key management scheme in wireless sensor networks," in Proc. 9th Int. Workshop Inf. Security Appl., 2008, pp. 305–319.
7. J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos, "Securing mhealthcare social networks: challenges, countermeasures and future directions," IEEE Wireless Commun., vol. 20, no. 4, pp. 12– 21, Aug. 2013.
8. M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.
9. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute- based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
10. N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 393–402.

10. F. Cao and Z. Cao, "A secure identity-based multi-proxy signature scheme," Comput. Electr. Eng., vol. 35, pp. 86–95, 2009.