Implementation of Mobile-Healthcare Application Giving Access Control, Security and Privacy to Patients Confidential Data

Sharanya N R[1], Parkavi A[2]

[1]Student, Department of CSE, M S Ramaiah Institute of Technology, Bengaluru, Karnataka

[2]Assistant Professor, Department of CSE, M S Ramaiah Institute of Technology, Bengaluru, Karnataka

Abstract: ***Distributed m-healthcare systems support for efficient patient treatment of high quality, but it brings about series of challenges in personal health information confidentiality and patient's identity privacy. Many existing data access control and anonymous authentication schemes are inefficient in distributed m-healthcare systems. To solve the problem, in this paper we have established a novel authorized accessible privacy model using AES (Advanced Encryption Standards) and Homomorphic algorithms to provide multi-level privacy-preserving cooperative authentication scheme. Distributed m-healthcare realizing three levels of security and privacy requirement and patients can authorize physicians by setting an access tree supporting flexible threshold predicates.***

Keywords: Authentication; access control; security and privacy; distributed m-healthcare; access tree

1. Introduction

The healthcare industry has significantly underutilized technology to improve operational efficiency. Most healthcare systems still rely on paper medical records. Information that is digitized is typically not portable, inhibiting information sharing amongst the different healthcare actors. Use of technology to facilitate collaboration and to coordinate care between patients and physicians, and amongst the medical community is limited. Around the globe, healthcare reform has mandated that it is time for healthcare information technology (HIT) [1] to be modernized and cloud computing is at the center of this transformation. The healthcare industry is shifting toward an information-centric care delivery model, enabled in part by open standards that support cooperation, collaborative workflows and information sharing. Cloud computing provides an infrastructure that allows hospitals, medical practices, and research facilities to tap improved computing resources at lower initial capital outlays. Cloud computing caters to the key technology requirements of the healthcare industry. Data maintained in a cloud may contain personal, private or confidential information such as healthcare related information that requires the proper safeguards to prevent disclosure, compromise or misuse. Globally, concerns related to data security, privacy and compliance are impacting adoption by healthcare organizations. Although regulatory and security concerns have held back the health care industry from widespread adoption of public clouds, the overall cloud computing market in health care will grow to $5.4 billion by 2017, according to a report by research firm MarketsandMarkets [2]. There has emerged various research results [3-6, 7, 8, 9, 10] focusing on them. A fine-grained distributed data access control scheme [11] is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control method [12] provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing. However, it mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system. Moreover, it is not enough for to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, 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 was left untouched.

To address the security and privacy issue, the new solution considers simultaneously achieving data confidentiality and identity privacy with high efficiency using new technology Homomorphic algorithm to encrypt patient's personal information and AES encryption for patients' health information. In distributed m-healthcare cloud computing systems, all the members can be classified into three categories: 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.

2. System Architecture

Basic Architecture of the E-health System

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

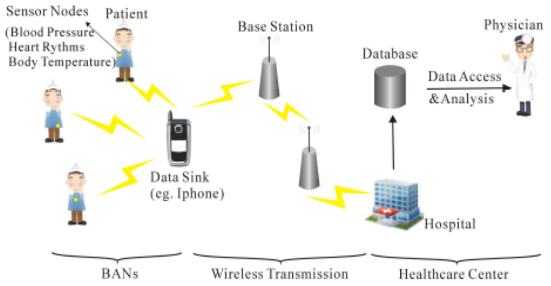


Figure 1: Basic Architecture of E-health System

Architecture of a Distributed m-Healthcare Cloud Computing System

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 Figure.

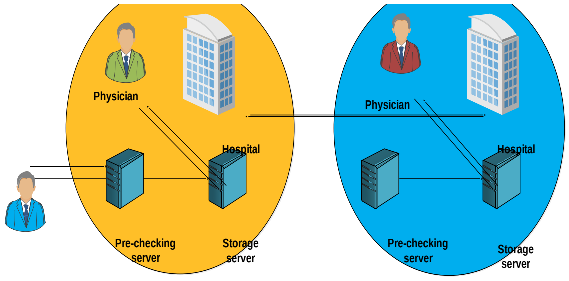


Figure 2: An Overview of Distributed m-Healthcare Cloud Computing System

3. Related Works

There exist a series of constructions for authorized access control of patients' personal health information. As we discussed in the previous section, they mainly study the issue of data confidentiality in the central cloud computing architecture, while leaving the challenging problem of realizing different security and privacy-preserving levels with respect to (w.r.t.) kinds of physicians accessing distributed cloud servers unsolved. On the other hand, anonymous identification schemes are emerging by exploiting pseudonyms and other privacy preserving techniques. Lin et. al. proposed SAGE achieving not only the content-oriented privacy but also the contextual privacy against a strong global adversary [12]. Sun et. al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge [11, 13]. Lu et. al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed m-healthcare cloud computing systems where the computational resource for patients is constrained. J. Misic et al. suggested patients have to consent to treatment and be alerted every time when associated physicians access their records. Riedl et. al. presented a new architecture of pseudonymiaztion for protecting privacy in E-health (PIPE). Slamanig et. al. integrated pseudonymization of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclosure attacks and statistical analysis in and suggested a secure mechanism guaranteeing anonymity and privacy in both the personal health information transferring and storage at a central m-healthcare cloud server [7]. Schechter et. al. proposed an anonymous authentication of membership in dynamic groups [6]. However, since the anonymous authentication mentioned above [6], [7] are established based on public key infrastructure (PKI), the need of an online certificate authority (CA) and one unique public key encryption for each symmetric key *k* for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed.

In this paper, the security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying GBDH problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed scenarios. It is noticed that our construction essentially differs from the recently published trivial combination of attribute based encryption (ABE) [13] and designated verifier signature
(DVS)

4. Problem Statement

We take into consideration that simultaneously achieving data confidentiality and identity privacy will be done with high efficiency. In distributed m-healthcare cloud computing systems, all the members can be brought under a tree of three different categories: the directly authorized physicians 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 in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes and unauthorized person who should not be able to access any data.

5. Implementation

We have implemented a Mobile application for patients and physicians to enter their information for hospital; here we have used two steps to encrypt the patient's data. Here we have used AES algorithm to encrypt patient's health information and Homomorphic encryption algorithm to encrypt patient's personal information by giving both security and privacy for hospitals confidential information.

Step 1: Advanced Encryption Standard (AES)
AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel

network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

High-level description of the algorithm

1. KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. InitialRound: AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds

a) SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

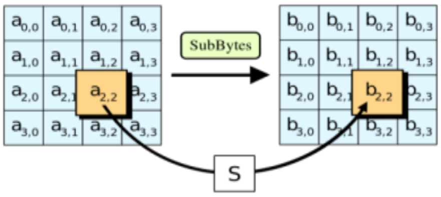


Figure 3: SubBytes module

b) ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps

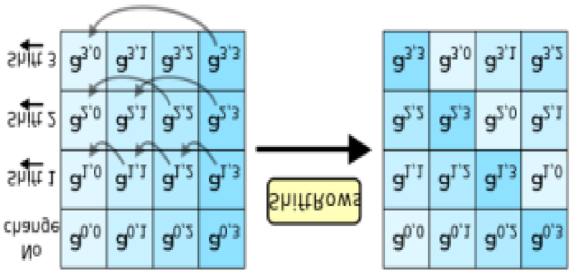


Figure 4: ShiftRow module

c) MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

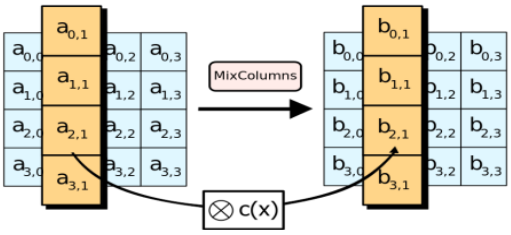


Figure 5: MixColumns module

d) AddRoundKey: In this step, each byte of the state is combined with a byte of the round subkey using the XOR operation

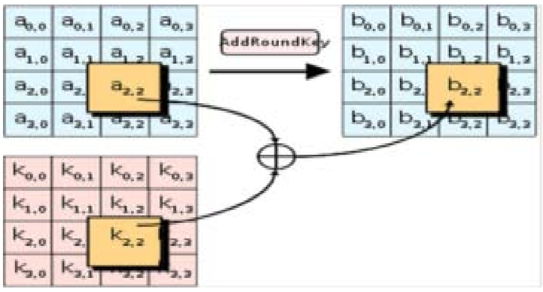
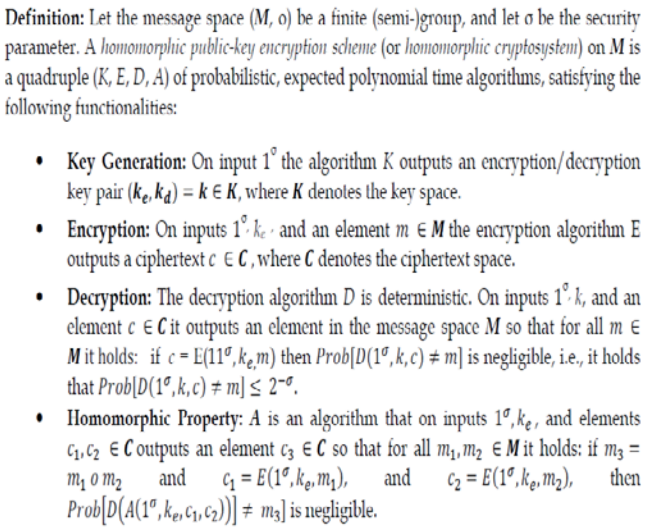


Figure 6: AddRoundKey module

Step 2: Homomorphic Algorithm

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is sometimes a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could 1) calculate the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services.[1] Homomorphic encryption schemes are malleable by design. This enables their use in cloud computing environment for ensuring the confidentiality of processed data. In addition the homomorphic property of various cryptosystems can be used to create many other secure systems, for example secure voting systems, collision-resistant hash functions, private information retrieval schemes, and many more.

High-level description of the algorithm:



Definition: Let the message space (M, o) be a finite (semi-)group, and let σ be the security parameter. A *homomorphic public-key encryption scheme* (or *homomorphic cryptosystem*) on M is a quadruple (K, E, D, A) of probabilistic, expected polynomial time algorithms, satisfying the following functionalities:

- **Key Generation:** On input 1^{σ} the algorithm K outputs an encryption/decryption key pair $(k_e, k_d) = k \in K$, where K denotes the key space.
- **Encryption:** On inputs $1^{\sigma}, k_e$ and an element $m \in M$ the encryption algorithm E outputs a ciphertext $c \in C$, where C denotes the ciphertext space.
- **Decryption:** The decryption algorithm D is deterministic. On inputs $1^{\sigma}, k$, and an element $c \in C$ it outputs an element in the message space M so that for all $m \in M$ it holds: if $c = E(11^{\sigma}, k_e, m)$ then $Prob[D(1^{\sigma}, k, c) \neq m]$ is negligible, i.e., it holds that $Prob[D(1^{\sigma}, k, c) \neq m] \leq 2^{-\sigma}$.
- **Homomorphic Property:** A is an algorithm that on inputs $1^{\sigma}, k_e$, and elements $c_1, c_2 \in C$ outputs an element $c_3 \in C$ so that for all $m_1, m_2 \in M$ it holds: if $m_3 = m_1 \, o \, m_2$ and $c_1 = E(1^{\sigma}, k_e, m_1)$, and $c_2 = E(1^{\sigma}, k_e, m_2)$, then $Prob[D(A(1^{\sigma}, k_e, c_1, c_2))] \neq m_3]$ is negligible.

6. Conclusion

In this paper, accessible privacy model and a patient self controllable multi-level privacy preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed healthcare cloud computing system using AES and Homomorphic encryption is proposed. In future its being a mobile android application we can include GPS to find near by hospitals to help patients with the popular physician based on the number of times the hospitals page is viewed.

References

[1] http://www.cloud-council.org/cscchealthcare110512.pdf
[2] http://www.eweek.com/c/a/Health-Care-IT/Cloud-Computing-in-Health-Care-to-Reach-54-Billion-by-2017-Report-512295
[3] J. Zhou and Z. Cao, *TIS: A Threshold Incentive Scheme for Secure and Reliable Data Forwarding in Vehicular Delay Tolerant Networks*, In IEEE Globecom 2012.
[4] S. Yu, K. Ren and W. Lou, *FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks*, In IEEE Infocom 2009.
[5] F.W. Dillema and S. Lupetti, *Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment*, In HealthNet 2007.
[6] J. Sun, Y. Fang and X. Zhu, *Privacy and Emergency Response in Ehealthcare Leveraging Wireless Body Sensor Networks*, IEEE Wireless Communications, pp. 66-73, February, 2010.
[7] J. Zhou and M. He, *An Improved Distributed Key Management Scheme in Wireless Sensor Networks*, In WISA 2008.
[8] J. Zhou, Z. Cao, X. Dong, X. Lin and A. V. Vasilakos, *Securing m-Healthcare Social Networks: Challenges, Countermeasures and Future Directions*, IEEE Wireless Communications, vol. 20, No. 4, pp. 12-21, 2013.
[9] J. Bethencourt, A. Sahai, and B. Waters, *Ciphertext-Plicy Attribte- Based Encryption*, In IEEE Symposium on Security and Privacy, 2007.
[10] N. Cao, Z. Yang, C. Wang, K. Ren and W. Lou, *Privacy-preserving Query over Encrypted Graph-structured Data in Cloud Computing*, ICDCS’11.
[11] S. Yu, K. Ren and W. Lou, *FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks*, In IEEE Infocom 2009.
[12] F.W. Dillema and S. Lupetti, *Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment*, In HealthNet 2007.
[13] PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System Jun Zhou, Xiaodong Lin, *Senior Member, IEEE* Xiaolei Dong, Zhenfu Cao, *Senior Member, IEEE*