International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 08, August 2017
ISSN: 2455-3778
http://www.ijmtst.com

Authorized Assistable Privacy Model for Healthcare Using ABBE Algorithm

Sangeetha B[1] | Prabhu P[2]

[1]M.Phil Scholar in Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.
[2]Professor, Department of Computer Science, Alagappa University, Karaikudi, Tamilnadu, India.

To Cite this Article
Sangeetha B and Prabhu P, "Authorized Assistable Privacy Model for Healthcare Using ABBE Algorithm", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 08, August 2017, pp.-1-5.

ABSTRACT

In distributed m-healthcare cloud computing system, only the authorized physicians or institutions that can recover the patient's personal information during data sharing. Most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. 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 inefficient in distributed m- healthcare systems. To solve this problem an Authorized accessible privacy model (AAPM) using ABBE algorithm which provides secure storage and control sharing of patient health data has been proposed. In this method, it explores broadcasting attribute based encryption as well as multi authority attribute based encryption to enforce patient access control policy, such that public user can download the data but only authorize user should view the medical records. This supports multiple owner scenarios and divides the users in the system into multiple security domains that greatly reduce the key management complexity for owners and users

Keywords: *Authentication, Access control, Cloud Computing, Data Storage, Public Domain, Private Domain, etc*

I. INTRODUCTION

Health care research studies often involve analysis of the huge amount of data collected from various sources, including health care providers, pharmacies, insurance companies, government agencies, and research institutions. Given the sensitive nature of health information and the social and legal implications for its disclosure, privacy is a major concern for information sharing in the healthcare domain.

Protecting the privacy of individually identifiable health information is more important when such information is used for clinical or health services related research. The Health Insurance Portability and Accountability Act (HIPAA) privacy rule strictly prohibits sharing of individually identifiable health information with clinical researchers who are not covered entities.

The covered entities, as defined in this privacy rule, include health plans, health care clearing houses, and health care providers that transmit health information electronically in connection with certain defined HIPAA transactions, such as claims or eligibility inquiries.

For preventing disclosure of individually identifiable information, usually de-identified or anonym Zed health data are shared with researchers. This data may be retrieved from multiple sites with different regulations on the disclosure of health information. In the absence of the identity information, correlation and integration of health data on a per patient basis in a privacy preserving manner are challenging issue.

One of the largest challenges in merging data is the lack of a common identifier across data systems. There are numerous commercial applications for creating enterprise master person indexes from distributed databases. Some of these are tolerant of missing, mistyped, or conflicting data. The approach commonly used by Regional Health Information Organizations (RHIOs) is that of RxHub – to only cross-link patients who have exact matches of five elements: first name, last name, birthday, gender, and zip code. RxHub is a third party data aggregator which has contracts with most major pharmacy benefits managers. Hospitals may use RxHub to request all historical pharmacy data from patients by sending those five demographic parameters to RxHub. RxHub queries its data sources to determine whether they have data for the requested patient, and if so, retrieve and organize the data from the various sources, keeping appropriate audit trails.

II. Related Works

2.1 Introduction

Research in any field requires literature review. A literature review is a written document that presents a logically argued case founded on a comprehensive understanding of the current state of knowledge about a topic of study. This case establishes a convincing thesis to answer a study's question. It will also give readers the necessary background to understand the research work.

Distinguishing what has been done from what needs to be done. Discovering important variables relevant to the topic. Synthesizing and gaining a new perspective. Identifying relationships between ideas and practice. Establishing the context of the topic or problem .Rationalizing the significance of the problem. Enhancing and acquiring the subject vocabulary. Understanding the structure of the subject. Relating ideas and theory to applications. Identifying the main methodologies and research techniques that have been used. Placing the research in a historical context to show familiarity with state-of-the-art developments.

Liang, et al. [1] Proposed a cipher text sharing mechanism with the following properties: Anonymity: given a cipher text, no one knows the identity information of the sender and receiver. Multiple receiver update: given a ciphertext, the receiver of the ciphertext can be updated at multiple times. Author refers to this property as "multi-hop". Conditional sharing: a ciphertext can be fine-grained shared with others if the pre specified conditions are satisfied. Achievements: Author investigates a new notion, AMH-IBCPRE and formalizes the definition and security model by incorporating the definitions.

Liu, et al. [4] Aims to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation. Author address the aforementioned privacy issue to propose a shared authority based privacy-preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. sThe main contributions are as follows. 1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority. 2) Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism. 3) Apply cipher text policy attributes based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

Ruj, et al. [5] proposed the privacy preserving access control with authentication for security of cloud data, the following points covered in scheme: 1) Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. 2) Authentication of users who store and modify their information of the cloud. 3) The identity of the user is protected from the cloud during authentication. 4) The architecture is decentralized, meaning that there can be several KDCs for key management. 5) The access control and authentication are both collision resistant. 6) The proposed scheme is resilient to replay attacks. 7) The protocol supports multiple read and writes on the data stored in the cloud. 8) The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

Zhou, et al. [2] proposed a novel authorized accessible privacy model (AAPM), for the multi-level privacy preserving cooperative authentication which 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. 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.

Zhang, et al. [3] defined multi-owner model for privacy preserving keyword search over encrypted cloud data, in which proposed an efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation. Author systematically construct a novel secure search protocol, which enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, and allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys. Also, proposed an Additive Order and Privacy Preserving Function family (AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately.

III. Research Methodology

A novel authorized accessible privacy model (AAPM) based on this propose a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA). Distributed m-healthcare realizing three levels of security and privacy requirement and patients can authorizes physicians by setting an access tree supporting flexible threshold predicates.

In this paper, by extending the techniques of attribute based access control and designated verifier signatures on de identified health information by realize three different levels of privacy-preserving requirement: only the physicians directly authorized by the patients can access the patients' personal health information and authenticate their identities simultaneously; the physicians and research staff indirectly authorized by patients cannot authenticate the patients' identities but recover the personal health information; while the unauthorized persons can obtain neither.

3.1 Preprocessing

1) Set up: the central authority or other trusted authority run a random algorithm. It takes security parameter as input and outputs a public key, secret key pair for every attribute authorities, also outputs a system public key and master secret key which will be used by the central authority.

2) Attribute Key Generation: An attribute authority run a random algorithm. It takes authority's secret key, a user's GID, the authority's value dk, and attributes in the authority's domain as input and output secret key for the user.

3) Central Key Generation: It is run by the central authority. It takes the master secret key and input is a user's GID and outputs are secret key for the user.

4) Encryption: It is runs by sender. It takes a set of attributes for each authority, a message, and the system public key as input and output is the cipher text.

5) Decryption: A deterministic algorithm runs by a user. It takes a cipher-text, that is encrypted under attribute set and decryption keys for that attribute set as input

3.2 Attribute Based Broadcast Encryption (ABBE) Algorithm

Attribute Based Broadcast Encryption as well as Multi Authority Attribute Based Broadcast Encryption to enforce patient access control policy such that public user can download the data but only authorize user should view the medical records.

This supports multiple owner scenarios and divides the users in the system into multiple security domains that greatly reduce the key management complexity for owners and users.

Finally, 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 computers, communication and storage overhead.

- Setup (, n, (B(u))1=u=n): takes as input the security parameter , the number of users n, and groups of users. It outputs an encryption key EK, and n decryption keys (dku)1=u=n.

- Encrypt (EK,BN ,BR): takes as input the encryption key EK and two sets of groups BN and BR. It outputs a header hdr and a message encryption key K . K is a finite set of message encryption keys.

- Decrypt (dku,hdr): takes as input a decryption key given to a user u and a header hdr. If the header hdr comes from an encryption using (BN ,BR)such that BN. B(u)and B(u)n BR = Ø, then it outputs a message encryption key K . K. In the other case, it outputs.

- In the encryption process, a message M is encrypted with a key K and the resulting cipher text C is sent together with the header hdr. Users in all groups mentioned in BN (needed groups) and outside all groups mentioned in BR (revoked groups) can compute K from the header hdr and their decryption key dku. Using the key K, a user recovers M from C.

3.2.1 High-level description of the algorithm

1. Key Expansions—round keys are derived from the cipher key using the Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round: Add Round Key—each byte of the state is combined with a block of the round key using bitwise OR.

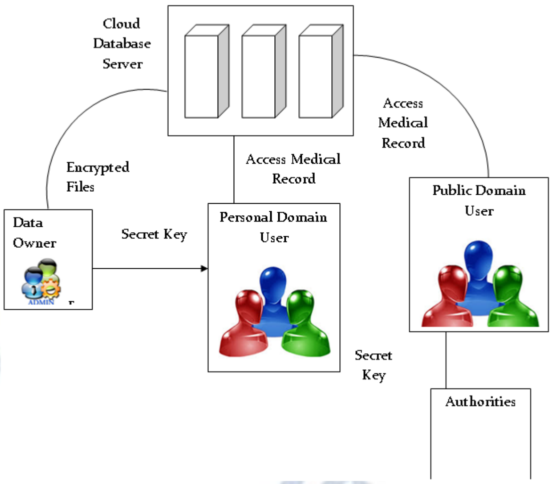
3. Rounds

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

b) Shift Rows—a transposition step where the last three rows of the state are shifted Cyclically a certain number of steps.

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

d) Add Round Key: In this step, each byte of the state is combined with a byte of the round sub key using the XOR operation.



IV. Experimental Evaluation

Functional Requirements:

This project has the following modules

a) User (Physian, Hospital Admin, Patient etc)

b) Cloud Server

c) Health Care Provider

V. Result and Discussion

This paper proposed design framework of secure sharing of personal medical records in cloud computing. Considering partially trustworthy cloud servers, patients shall have complete control of their own privacy through encrypting their medic al record files to allow fine-grained access. The attribute-based encryption model is enhanced to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy. In this paper, a novel authorized accessible privacy model (AAPM) and a patient self controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three different levels of security and privacy requirement in the distributed healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

VI. Conclusion

In this paper, a novel authorized accessible privacy model (AAPM) and a patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three different levels of security and privacy requirement in the distributed healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

VII. Future Enhancement

Protecting the privacy of user attributes and a new privacy challenge of data access in cloud computing authority sharing is a future enhancement of this paper. PHR system important issues such key efficient on-demand revocation will be solved in future.

VIII. Reference

[1] Hong Liu, Huansheng Ning, Qingxu Xiong, Laurence T. Yang, "Shared Authority Based Privacy Preserving Authentication Protocol in Cloud Computing", IEEE Transactions on parallel and distributed systems, VOL.26, NO. 01, pp. 241-251, January 2015.

[2] Jun Zhou, Xiaodong Lin, Xiaolei Dong, and Zhenfu Cao, "PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System", IEEE Transactions on parallel and distributed systems, VOL.26, NO. 06, pp. 1693-1703, June 2015.

[3] Kaitai Liang, Willy Susilo and Joseph K. Liu,"Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage", IEEE transactions on information forensics and security, VOL. 10, NO. 08, pp. 1578-1289, August 2015.

[4] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, VOL. 26, NO. 06, pp. 556-563, October 2012.

[5] Wei Zhang, Yaping Lin, Sheng Xiao, Jie Wu, Siwang Zhou," Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing", IEEE Transactions on computers, VOL. 10, NO. 01, pp. 1-14, January 2015.