ISSN 2350 - 0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 2, February 2015

Privacy Preserved and Auditable Health Data Access in Cloud using Threshold Signature with ABE based Access Control

S.Sundar Rajan, P.Nikitha

Associate Professor, Department of Computer Science and Engineering, Surya Group of Institutions, Vikravandi, Villupuram District, Tamil Nadu, India.

PG scholar, Department of Computer Science and Engineering, Surya Group of Institutions, Vikravandi, Villupuram District, Tamil Nadu, India.

ABSTRACT: Accomplished with the strong security requirement in eHealth care systems and the latest developments in the cloud environments for outsourcing, hosting, accessing and easy retrieval of medical data, the proposed system builds privacy into mobile healthcare systems with the help of the private cloud. The private cloud also engages in bootstrapping of data for managing access control and auditing on authorized parties. Specifically, the proposed work integrates key management from pseudorandom number generator for unlink ability, a suitable indexing technique for maintaining confidential keyword based search which hides both surfing and data access patterns based on repetitive structures, and also binds up attribute based encryption with threshold signature exchange with audit ability for issuing role-based access control to prevent potential misbehavior, in both normal and emergency cases. The system devises mechanisms that can detect whether users health data have been illegally distributed and identifies possible sources of leakage. The main intruding network and the authorized party that did it will also be found, thus destroying the particular request of an intruder by crashing the attributes assigned to them.

KEYWORDS: Access control, auditability, eHealthcare, Privacy, Threshold, ABE**.**

I. INTRODUCTION

Fast access to health data enables better healthcare service provisioning, and assists in medical emergencies by widely helping in timely treatment of the enables. AAA electronic healthcare system is always vital. Facilities and services provided by the e-devices may cause only minimal interruption to the patients and may not affect their daily activities. These data which are managed by e-devices have to be outsourced to cloud environment for secure storage.

It is stated in a report that 8 million patients information was leaked in the websites. Hence, it is of high importance that these data has to be protected at the cyberspace. Outsourcing data storage and remote computational task in cloud environment is a popular trend. Hence, for safe and efficient outsourcing of patients' health details, private clouds are used for service offerings. The cloud enabled service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving e-device users with lightweight tasks.

ISSN 2350 - 0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 2, February 2015

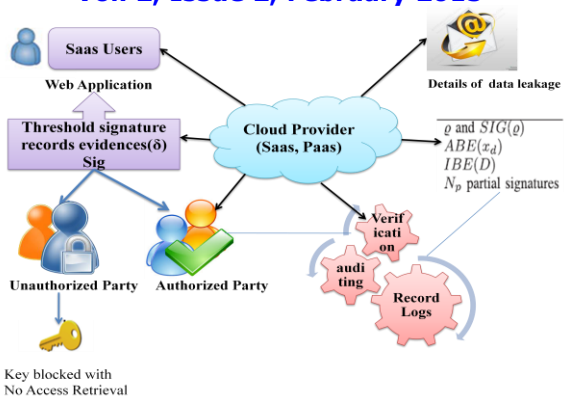


Fig 1: System Architecture

II. RELATED WORKS

Some early works on privacy protection for e-health data concentrate widely upon the associate design, including the demonstration of the importance of privacy for e-healthcare systems, the authorization relying upon existing adhoc wireless infrastructure, the role-based mechanism for access denials, etc. In particular, identity-based encryption (IBE) has been used for employing basic role-based cryptographic data access control. Amongst the earlier approaches on e-healthcare privacy, Medical Information Privacy Assurance (MIPA) pointed out the importance of MIPA and addressed the unique challenges of medical information privacy, and the exploring privacy breach issues, that resulted from insufficient coordinating technology. Among the known, MIPA was one first out of the few projects that was missioned to develop privacy technology and privacy-protecting infrastructures to facilitate the development of a healthcare system, in which individuals can actively protect their personal information. The security requirement for ehealth systems were summarized based on the collaboration with various researches.

The backup mechanism for emergency access relies on someone or something the patient trusts whose availability cannot be guaranteed at all times. Moreover, the storage privacy used for general eMedical data security is a weaker form of privacy because it does not hide search and access patterns. The previously stated research works failed to address the challenges in data privacy, all these challenges are tackled in this paper by the use of preliminaries and the threshold signature.

III. PROPOSED WORK

PRELIMINARIES

A. Privacy Preserved E-Health

The cloud-assisted privacy-preserving mobile healthcare system consists of two components: searchable encryption and auditable data management control. The users health data are processed by the private cloud and stored in the public cloud thus guaranteeing efficient & timely retrieval of data. The private cloud involves in the bootstrapping of data access and auditability scheme in association with users, so that it can later act on the users' behalf to exercise access control and eliminate unauthorized parties.

B. Storage Privacy and Efficient Retrieval

Storage privacy is an essential component for an ehealth system. Our storage mechanism benefits the usage of secure index or SSE, so that the user can encrypt the data with additional data structures to allow for efficient search.

ISSN 2350 - 0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 2, February 2015

It has been shown that the secure index-based approach is promising among different approaches for security in storage. In our environment, the role of the user is assigned to the private cloud, and the public cloud serves as the storage server in SSE.

C. Data Access Privacy and Auditability

The second component is the data access during emergencies where the EMT requests data through the private cloud. ABE serves as a gatekeeper to prevent unauthorized parties from decrypting the data. However, it does not provide any mechanism for auditability, i.e., to record and prove that an authorized party has accessed certain data. Without auditability, it is not possible to identify the source of breach if authorized parties illegally distribute the health data.

D. Storage privacy

The proposed approach guarantees the five storage privacy requirements. First ,since the data are encrypted, unauthorized intruder may not gain the knowledge of the content of the stored data. Second, our file identifiers are numeric values that do not divulge any information about the file content or the ownership So multiple data files cannot be linked by their identifiers. Third, by adding redundancy to the linked lists, the adversaries can hardly tell if the searches were for the same keyword, or if a set of data files contain a same keyword. The fourth requirement, i.e., the storage/retrieval anonymity can be easily satisfied because the private cloud performs the storage/retrieval for all the users.

E. Threshold signature with ABE

Fine-grained access control is achieved by ABE based threshold signing scheme, where the expensive ABE operations are only used for encrypting small secret values and the majority of data encryption is fulfilled by efficient symmetric key scheme. The threshold signature exchange used enables the private cloud to record evidence that is signed by the authorized parties which can be used as audit logs. By having the private cloud and EMT both signing the EMT's data access requests, users can later check whether the request is legitimate and accurate, and obviously be assured that the EMT cannot deny a request and the private cloud cannot falsely accuse an EMT.

IV. MODULES

A. Searchable Symmetric Encryption

The location unaware remote servers are used to store the encrypted documents in SSE by the data owners that are defined as honest-but-curious party and correspondingly pay a way to surf the encrypted content. More importantly, neither the operation of outsourcing nor keyword searching would result in any information leakage to any party other than the data owner, thus achieving a sound guarantee of privacy.

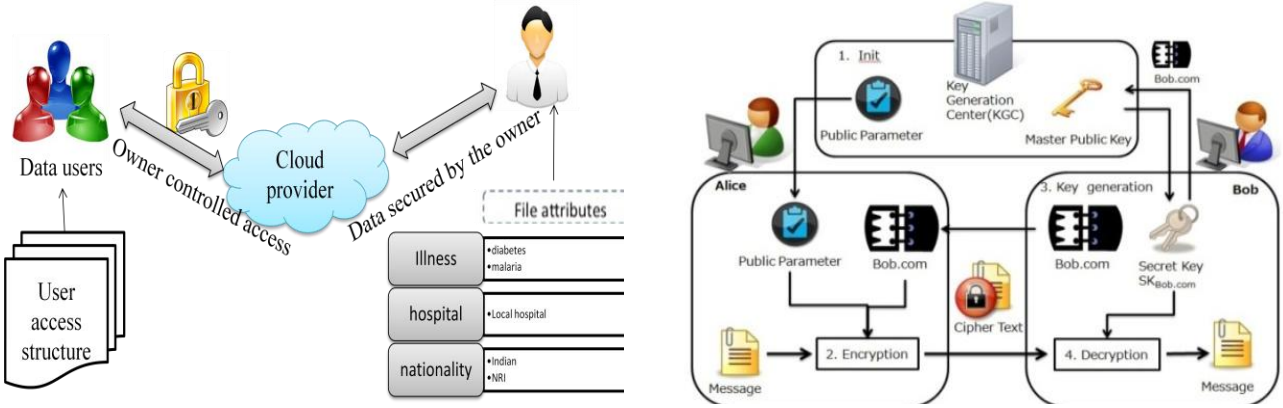
B. Identity-Based Encryption

Identity-based systems allow any party to generate a public key from a known identity value. IBE makes it possible for any party to encrypt message with no prior distribution of keys between various people. This is an critical form of pairing-based-cryptography.

C. Attribute-Based Encryption

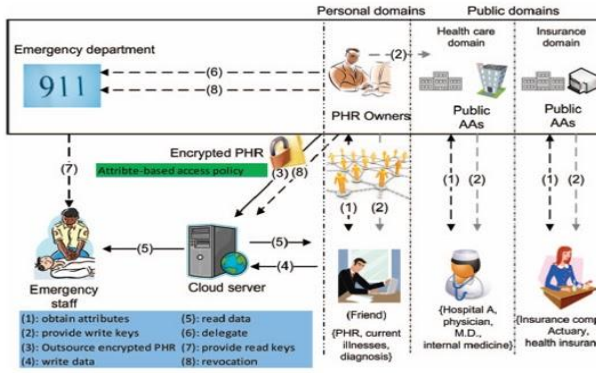
ABE has shown its promising future in fine-grained access control for outsourcing reliable data. Typically, data are encrypted by its sole owner under a set of attributes. Anyone who accesses the data are assigned access structures by the owner and decryption is done only if the structures are matched.

ISSN 2350 - 0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 2, February 2015

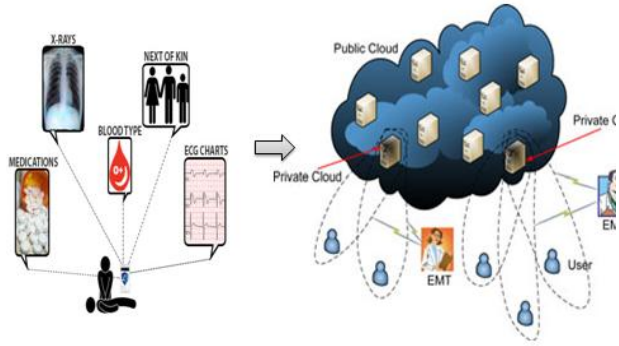


(a) (b)

Fig 2: (a) Trapdoor generation scheme (b) Identity based encryption



(c)



(d)

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 2 , February 2015

Fig 2: (c) Secure Data Access (d) Auditable health data access using threshold signature

D. Threshold Secret Sharing in MIPA

This is a mechanism for sharing secret information among multiple entities so that the cryptographic power is distributed at the same time to avoid single point of failure. The private cloud will process the data to add security features before it is stored on the cloud domain. Public cloud is owned by the cloud providers such as Amazon and Google which offers massive storage and rich computational resource. The bootstrap phase, there is a secure channel between the user and the private cloud.

V. COMPUTATION MECHANISMS

In privacy-preserving storage leveraging patient mobile devices, efficient secret key operations are mainly involved which we will not focus on in the evaluation. In emergency medical data access leveraging EMT mobile devices, the most costly real-time computation includes IBE decryption and ABE decryption, generating a regular signature on attributes and a partial threshold signature on the access request, and verifying the partial threshold signature from the private cloud. However, IBE decryption, ABE decryption, and regular signature can be performed once and for all access for the same patient, which is beneficial if the EMT will issue multiple access requests.

VI. ANALYSIS OF THE PAPER

A. Security Fulfillments

The proposed approach guarantees the five storage privacy requirements. First, since the data are encrypted, unauthorized parties cannot learn the content of the stored data. Second, our file indicators are countable values that do not specify any information about the file content or the ownership. So, multiple data files cannot be linked by their identifiers. Third, by adding redundancy to the linked lists, the unknown can rarely say if the searches were for the identical keyword, or if a set of data files contain a same keyword. The fourth requirement, i.e., the storage/retrieval anonymity can be easily satisfied because the private cloud performs the storage/retrieval for all the users it supports and no particular user can be associated with any storage retrieval techniques. Finally, the keyword for the search is encrypted in the trapdoor, and thus, no sensitive information is exposed.

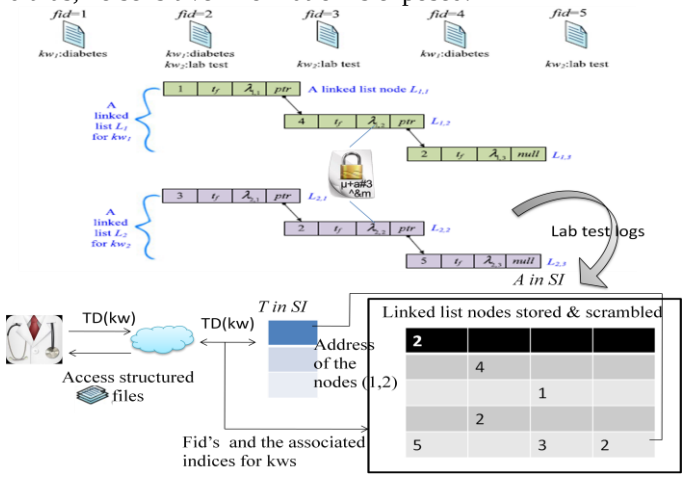


Fig 3: Construction of patient's record with the security fulfillments.

B. Privacy & Auditability Fulfillments

Fine-grained access control is achieved by our ABE-control threshold signing scheme, where the expensive ABE operations are only used for encrypting small secret values and the majority of data encryption is fulfilled by efficient symmetric key scheme. The threshold signature exchange used in our scheme enables the private cloud to record evidence that is signed by the authorized parties which can be used as audit logs. By having the private cloud and EMT

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 2 , February 2015

both signing the EMT's data access requests, users can later check whether the request is accurate based on the entry from the audit logs and the primary key stored at record logs of the potential server.

VII. COMPUTATION EFFICIENCY

In emergency medical data access leveraging EMT mobile devices, the most costly real-time computation includes IBE decryption and ABE decryption, generating a regular signature on attributes and a threshold signature which is partial on the access request, and verifying the partial threshold signature from the private cloud. The request and response mechanism of communicating parties such as the private, public cloud and technicians depends upon their attributes overhead.

Table 1: Communication overhead for successful data request

Collaborating parties	Hints	Threshold overhead
1. Technician 2. Private cloud 3. Insurance company 4. friends	ϱ and SIG(ϱ) ABE(x_d) IBE(D) N_p partial signatures	$N_A S_{Att} + S_s + S_{ABE} + S_{IBE} + N_p + S_s$ $N_p + S_s$
1. Cloud provider	A trapdoor redundant files for pattern hiding	$2S_g + (N_{kl}-1)N_{fk}S_F$

VIII. EXPERIMENTAL RESULTS

Amongst earlier works in ehealth care systems the following drawbacks were found. Users will have to send the data over insecure network after the data storage in private network. Technicians and doctors associated with the patients' will have direct access to the health data in case of medical emergencies. There are chances that secure health data be accessed without the knowledge of the data owner. These works make the paper vulnerable to certain types of attack. However, the proposed work overcomes almost all of the drawbacks by implementing the following technology aspects: pattern hiding scheme is used in order to hide keyword based surfing, this leads to high security standards with efficient data access and management retrieval. Moreover, bootstrapping is done by the private clouds such that burdens posted on the users are widely reduced. The amount of efficiency and computational aspects of this paper has been studied and revealed in graph format. The graph has been denoted based on the statistical measurement analytics that is composed based on the various parameters such as security, the level of difficulty posed on the users in order to manage the data securely, privacy and audits that involves in the effective management of the data. The security factor which is considered as the most primary requirement of this paper derives its source from the IBE & ABE based algorithm construction.

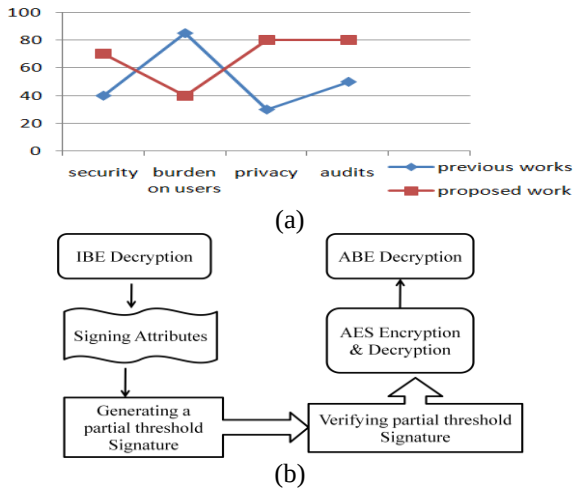


Fig 4: (a) Comparative survey of previous with current work (b) Preliminary security verification

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 2 , February 2015

IX. CONCLUSION & FUTURE WORK

The proposed work builds privacy into the mobile health systems with the help of the private cloud. Bootstrapping is the secure channel that is used for the private communication of cloud users who have been authenticated and authorized. A solution for privacy-preserving data storage is achieved by integrating a PRF based key management for unlinkability, a search and access pattern hiding scheme based on redundancy, and a secure indexing method for privacy-preserving keyword search. The investigated techniques provide access control (in both normal and emergency cases) and auditability of the authorized parties to prevent misbehavior, by combining ABE-controlled threshold signing with role-based encryption. Moreover, the unauthorized data access of a patients' record is identified. The details of the path and unauthorized network are resolved by means of enabling threshold signature exchange. The cloud network is managed by engaging audit & record logs.

As a future work, the illegal access patterns can be made to known in instant accessible electronic devices such as cell phones and PDA's, such that the basic level distribution of authorized data can be controlled and protected.

REFERENCES

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," *J. ACM*, vol. 43, pp. 431–473, 1996.
[2] R. Ostrovsky, "Efficient computation on oblivious RAMs," in *Proc. ACM Symp. Theory Comput.*, pp. 514–523, 1990.
[3] C. Wang, K. Ren, S. Yu, and K. Urs, "Achieving usable and privacyassured similarity search over outsourced cloud data," in *Proc. IEEE Conf. Comput. Commun.*, pp. 451–459, Mar. 2012.
[4] N. Cao, Z. Yang, C.Wang, K. Ren, andW. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in *Proc. IEEEInt. Conf. Distrib. Comput. Syst.*, pp. 393–402, Jun. 2011.
[5] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on PHI in ehealthcare systems," *Adv. Health Inform. Conf.*, pp. 1–5, Apr. 2010.
[6] M. Katzarova and A. Simpson, "Delegation in a distributed healthcare context: A survey of current approaches," in *Proc. 9th Int. Conf. Inform. Security*, pp. 517–529, 2006.
[7] Foster, C.Kesselman,G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in *Proc. ACMConf. Comput. Commun. Security*, San Francisco, CA, USA, pp. 83–92, 1998.
[8] X. Liang, R. Lu, L.Chen, X. Lin, andX. Shen, "PEC:Aprivacy-preserving emergency call scheme formobile healthcare social networks" *J. Commun.Netw.*, vol. 13, no. 2, pp. 102–112, 2011.
[9] S. S. M. Chow, "New privacy-preserving architectures for identity-/attribute-based encryption" Ph.D. dissertation, Courant Inst. Math. Sci.,New York University, New York, NY, USA, 2010.
[10] S. S. M. Chow, "New privacy-preserving architectures for identity- /attribute-based encryption" Ph.D. dissertation, Courant Inst. Math. Sci., New York University, New York, NY, USA, 2010.

BIOGRAPHY

S. Sundar Rajan is an Associate Professor of Computer Science & Engineering at Surya Group of Institutions, Vikravandi. He is a research scholar at St. Peters University, Chennai. He received his Master degree from Anna University, Chennai. His research interest includes Data Mining, Information & Knowledge Management, Cloud Computing and Computer Communication & Networks.

P.Nikitha is a PG Scholar of Computer Science & Engineering at Surya Group of Institutions, Vikravandi. She received her B.Tech degree from Anna University, Chennai. Her research interest includes Cloud Computing, Cloud related hypervisor technologies & Data Mining.