International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume I, Issue I, 2016

ENHANCED APPROACH FOR SECURING HEALTH DATA IN THE CLOUD USING IDENTITY BASED ENCRYPTION

M. Rajakumar* & S. J. Vivekanandan**

* M.Tech Scholar, Department of Computer Science and Engineering, PRIST University, Thanjavur, Tamilnadu

** Assistant Professor and Head, Department of Computer Science and Engineering, PRIST University, Thanjavur, Tamilnadu

Abstract :

Cloud computing technology enables highly scalable services to be easily consumed over the Internet as per the need of the users according to their needs. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. Because of this reason emergency arises that leads to the development of viable protocols, architectures and system assuring privacy and security to protect the sensitive and personal digital information. Various techniques exists, but they do not address the issue regarding the illegal distribution of data. This system offers enhanced securing method using Identity Based Encryption that incorporates various logging mechanisms, Access Control Lists that can detect whether the health data have been illegally distributed, and identify possible sources of leakage.

Key Words: Access Control List, Identity Based Encryption, Logging Mechanism, Privacy & Security.

1. Introduction:

Cloud computing is the newest term for the long-dreamed vision of computing as a utility. The cloud provides convenient, on-demand network access to a centralized pool of configurable computing resources that can be rapidly deployed with great efficiency and minimal management overhead. As cloud storage becomes commonplace, the need to protect and encrypt data grows ever greater. Dozens of services shovel tons of free space to you just for signing up. But which of those services are looking at the files you upload, and most importantly, which services encrypt your personal data so *no one* can look at it. The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so.

One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service (or) data can be placed in the cloud, aiming to give a better understanding of this complex scenario [2].

The proposed system offers enhanced securing method using Identity Based Encryption that incorporates various logging mechanisms, access control lists that can detect whether the health data have been illegally distributed, and identify possible sources of leakage, giving an overview of the current status of security in this emerging technology.

2. Problem and Discussion:

2.1. Identity Based Encryption Algorithm (IBE):

The main objective of the proposed system is preserving the privacy of the information ensuring that this information cannot be misused. The encryption and decryption format is the soul of this project. The patient's report will reach the doctor in encrypted format, by using Identity Based Encryption algorithm (IBE), logging mechanisms, access control lists, while a master key helps to deliver the report to the doctor in decrypted format.

2.2. Private Key Generator (PKG):

A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID [2]. Also we can detect whether the health data have been illegally distributed, and identify possible sources of leakage.

2.3. Medical Information Privacy Assurance (MIPA):

Among the earliest efforts on e-health privacy, Medical Information Privacy Assurance (MIPA) [4] pointed out the importance and unique challenges of medical information privacy, and the devastating privacy breach facts that resulted from in sufficient supporting technology. MIPA was one of the few projects that sought to develop privacy technology and privacy-protecting infrastructures to facilitate the development of a health information system, in which individuals can actively protect their personal information.

Privacy-preserving health data storage is studied by Sun *et al.* [6], where patients encrypt their own health data and store it on a third-party server. This work and Searchable Symmetric Encryption (SSE) schemes [7]–[12] are most relevant to this paper.

There is also a large body of research works on privacy- preserving authentication, data access, and delegation of access rights in e-health systems [15], [16], while [6], [17]–[21] are most related to our proposed research.

2.4. Advantages of the Proposed System:

The identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. The authenticity of the public keys is guaranteed implicitly as long as the transport of the private keys to the corresponding user is kept secure (Authenticity, Integrity, Confidentiality) [2]. When the receiver contacts the PKG to retrieve the private key for this public key, the PKG can evaluate the identifier and decline the extraction if the expiration date has passed.

3. System Architecture:

3.1. System Architecture Description:

Step 1: Registration process of Patient or Doctor.
Step 2: Acknowledgement send to the user by the admin for the user Registration.
Step 3: Administrator or Doctor or Patient can login into Hospital Management System.
Step 4: Patient can upload Test Report into Hospital Management System.
Step 5: Doctor can view that report (step 4) and give Prescription.
Step 6: Doctor can issue the Decrypt key to the patient.

Step 7: Patient can now view the Prescription.

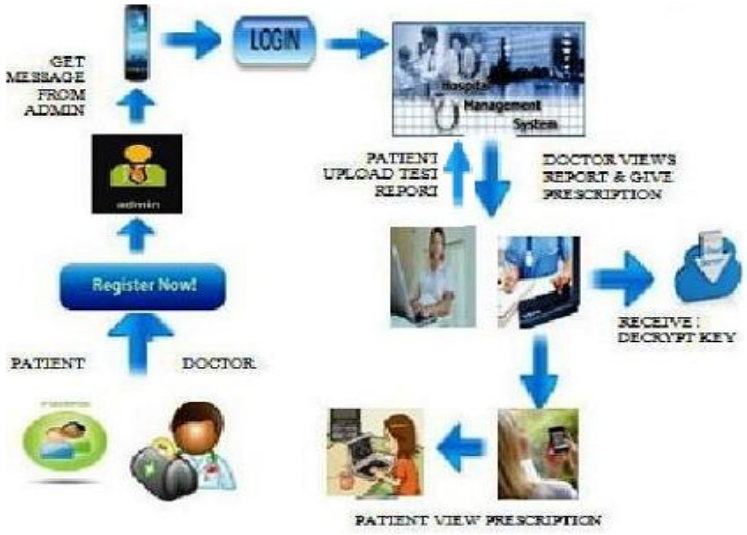

Figure: Architecture of the Proposed System.

4. Functions of System Design:

4.1. Overview:

Registration is a mandatory process to get into a hospital management system for any doctor and Patient.

4.2. Used Mechanisms:

The following are the mechanisms which are used in our proposed system. Such are:

- Identity Based Encryption (IBE).
- Access Control List (ACL).
- Other Security Measures.

4.2.1. Identity Based Encryption (IBE):

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 [2].

Identity (ID)-based encryption, or IBE for short, is an exciting alternative to public-key encryption, which eliminates the need for a Public Key Infrastructure (PKI) that makes publicly available the mapping between identities, public keys, and validity of the latter. The senders using an IBE do not need to look up the public keys and the corresponding certificate of the receivers, because the identities (e.g. emails or IP addresses) together with common public parameters are sufficient for encryption. The private keys of the users are issued by a trusted third party called the private key generator (PKG) [2].

ID-based encryption (or identity-based encryption (IBE)) is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This can use the text-value of the name or domain name as a key or the physical IP address it translates to. Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as *master key*).

Given the master public key, any party can compute a public key corresponding to the identity *ID* by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity *ID* contacts the PKG, which uses the master private key to generate the private key for identity *ID*. As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted, as it is capable of generating any user's private key and may therefore decrypt (or sign) messages without authorization. Because any user's private key can be generated through the use of the third party's secret, this system has inherent key escrow.

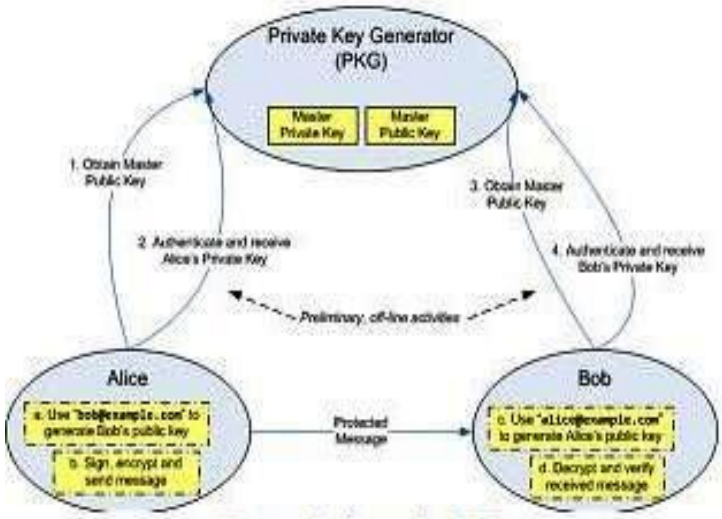

Figure 3: Steps for IBE

IBE Algorithm Consists of the Following Four Operations:

1. Setup, which initializes a key server. This algorithm is run by the PKG one time for creating the whole IBE environment. The master key is kept secret and used to derive users' private keys, while the system parameters are made public. It accepts a security parameter and outputs a set of system parameter, including the message space and cipher text space and a master key.

2. Key Generation, which generates a private key for a given user. This algorithm is run by the PKG when a user requests his private key. Note that the verification of the authenticity of the requestor and the secure transport of are problems with which IBE protocols do not try to deal. It takes as input and an identifier and returns the private key for user.

3. Encrypt, which encrypts a message for a given user.

4. Decrypt, which given a private key, decrypts a message.

4.2.2. Access Control List (ACL):

In many application scenarios, such as those in enterprises or organizations, users' access to data is usually selective and highly differentiated. Different users enjoy different access privileges with regard to the data. When data are outsourced to the cloud, enforcing secure, efficient, and reliable data access among a large number of users is thus critical. Traditionally, to control the dissemination of privacy-sensitive data, users establish a trusted server to store data locally in clear, and then control that

server to check whether requesting users present proper certification before letting them access the data.

From a security standpoint, this access control architecture is no longer applicable when we outsource data to the cloud. Because data users and cloud servers aren't in the same trusted domain, the server might no longer be fully trusted as an omniscient reference monitor for defining and enforcing access control policies and managing user details. In the event of either server compromise or potential insider attacks, users' private data might even be exposed.

One possible approach to enforce data access without relying on cloud servers could be to encrypt data in a differentiated manner and disclose the corresponding decryption keys only to authorized users. This approach usually suffers from severe performance issues, however, and doesn't scale, especially when a potentially large number of on-demand users desire fine-grained data access control. Researchers have been working on how to realize a fine-grained access control design that fully leverages the cloud's computation resource richness. Via this approach, data users would be able to securely delegate to the cloud most cumbersome user / data management workloads - such as handling frequent user access privilege updates in large dynamic systems while still preserving the underlying data confidentiality against any unauthorized access.

4.2.3. Other Security Measures:

In order to satisfy the presented security and privacy requirements, our architecture features a combination of established and new building blocks (below Table) [25]. Currently, we assume that "data owners" are the health centers. We leave an extension of this assumption to multilateral security requirements and in particular the challenges of patient-centric data management for future work.

In our approach, we assume that all participating organizations, such as HCs or CPs, have a common interest in securing the infrastructure and data against external, third-party adversaries. Hence, the establishment of common and cooperative security mechanisms will be feasible, even though many practical and procedural challenges could arise when implementing them in concrete usage scenarios.

5. Experimental Results:

5.1. Patient Registration

Registration is a mandatory process to get into a hospital management system for any doctor and Patient. A doctor and Patient have to provide their personal information to the patient healthcare monitoring to create their account.

Figure: User Registration

5.2. Administrator Updation:

Admin will assess the given detail of a user and activates their account to view the patient healthcare monitoring. After activation the user get message from admin by

their mobile. An existing user can directly login to the system with their valid user name and password. Activated User can enter into patient healthcare monitoring with their valid username and password.

Figure: Admin Updation

5.3. Patient Details Uploading:

User should have all their test reports whatever related to their disease which was advised by the doctor earlier. Cloud area serves as a storage medium where all user records are being stored. When doctor login to the patient healthcare monitoring by providing their valid user name and password, they can view the history of a patient.

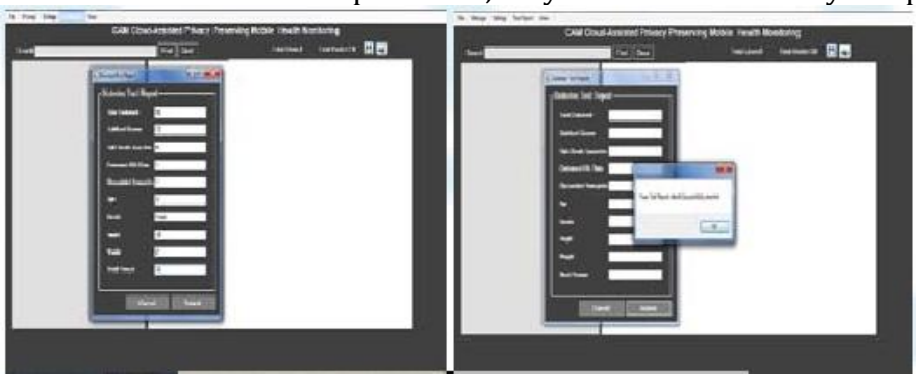

Figure: Patient Uploads Test Report

5.4. Doctors Receive ID and Private Master Key:

When doctor wants to view the files of any patient, he will be finding all their reports in encryption format. To decrypt this test report doctor have to get the patient ID from the appropriate column.

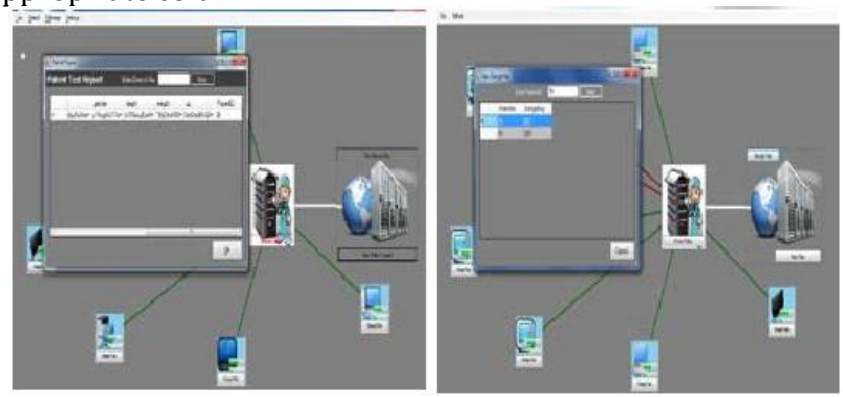

Figure: Doctor receives the ID&Private Master Key

5.5. Doctors Viewing the Patient Record:

This ID, which is used as Doctor's key. This helps him to view the patient test report in decrypted format. Then doctor will decide the medicine to be prescribed,

which will be entered by the doctor manually. This prescription to the user will be saved in cloud server in encrypted format. If the patient wants to view the doctor's prescription, user has to login into the patient healthcare monitoring.

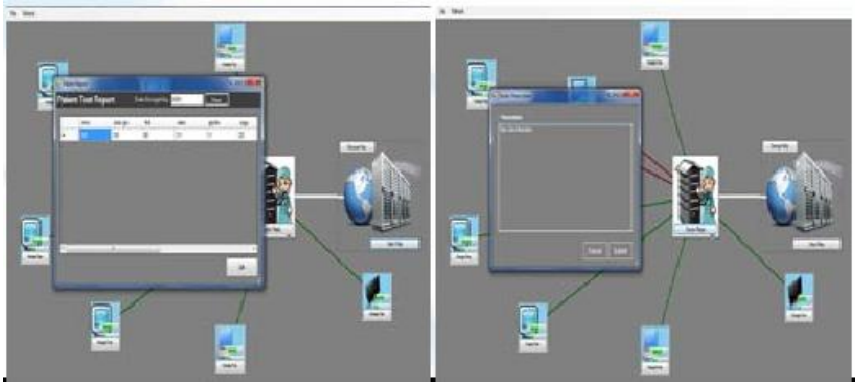

Figure: Doctor view the Test Report & Gives Prescription

5.6. Patient Receives Prescription:

Now the prescription will be in encrypted format. To decrypt they need a patient key. That will be sent to the given mobile number of the patient. Using patient key user can view the doctor's prescription.

Figure: Patient Get Decrypt Key & View Prescription

6. Conclusion and Future Work:

Cloud Computing technology provides human advantages such as economical cost reduction and effective resource management. However, if security accidents occur, economic damages are inevitable. Our paper proposed "**Enhanced Approach for Securing Health Data in the Cloud using Identity Based Encryption**" for effective resource. Proposed method consists of Identity Based Encryption (IBE) in which a master key helps to deliver the report and Outsourcing Decryption Technique in which a master key helps viewing the prescription [3]. The investigated techniques provide access control (in both normal and emergency cases) and auditability of the authorized parties to prevent misbehavior, by combining IBE-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.

Our main goal for future work is the full implementation of the cloud secret-sharing proxies, and their test in real networks using different real-world clouds. On the organizational side, corresponding security assumptions and processes will be evaluated with practice partners in healthcare, including signatures at an attribute-level or by individuals.

In the future, we also aim to better involve the patient into our architecture [25]. This could involve the inclusion of the patient as an actor, e.g., giving him or her control over shares of their EHRs. Moreover, we aim to address some of the corresponding research challenges. In particular, the problem of ownership of information, the feasibility of reliable auditing, patient consent for data access and access revocation can involve interesting challenges for our research and practice.

7. References:

1. Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability, Yue Tong, Student Member, IEEE, Jinyuan Sun, Member, IEEE, Sherman S. M. Chow, and Pan Li, Member, IEEE,-IEEE Journal Of Biomedical And Health Informatics, VOL. 18, NO. 2, MARCH 2014.
2. A Secured Patient Healthcare Monitoring in Cloud Infrastructure, Vaishnavi B, Yogeshwari R, International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878 Volume 2 Issue 1, January 2014.
3. Privacy Preserved and Auditable Health Data Access in Cloud using Threshold Signature with ABE based Access Control, S.SundarRajan, P.Nikitha, International Journal of Advanced Research in Science, Engineering and Technology, Vol. 2, Issue 2, February 2015.
4. G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, "Medical information privacy assurance: Cryptographic and system aspects," presented at the 3rd Conf. Security Communication Networks, Amalfi, Italy, Sep. 2002.
5. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.
6. J.Sn, X.Zhu, C.Zhang, and Y.Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.
7. E.-J. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
8. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," presented at the ACM Conf. Comput. Commun.Security, Alexandria, VA, USA, 2006.
9. Y. C.Chang and M.Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Security, 2005, pp. 442–455.
10. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searching on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.
11. O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," J. ACM, vol. 43, pp. 431–473, 1996.
12. R. Ostrovsky, "Efficient computation on oblivious RAMs," in Proc. ACM Symp. Theory Comput., 1990, pp. 514–523.
13. C. Wang, K. Ren, S. Yu, and K. Urs, "Achieving usable and privacy- assured similarity search over outsourced cloud data," in Proc. IEEE Conf. Comput. Commun., Mar. 2012, pp. 451–459.
14. N.Cao, Z.Yang, C.Wang, K.Ren, and W.Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 393–402. [22] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access.

15. L. Zhang, G. J. Ahn, and B. T. Chu, "A role-based delegation framework for healthcare information systems," in 7th ACM Symp. Access Control Models Technol., Monterey, CA, USA, 2002, pp. 125–134.
16. L. Zhang, G. J. Ahn, and B. T. Chu, "A rule-based framework for role- based delegation and revocation," ACM Trans. Inf. Syst. Security,vol.6, no. 3, pp. 404–441, 2003.
17. W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, Jan. 2008.
18. C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: An identity-based cryptography approach," in Proc. ACM Conf. Wireless Netw. Security, Apr. 2008, pp. 148–153.
19. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption : Ensuring privacy of electronic medical records," in Proc .ACM Workshop Cloud Comput. Security, 2009, pp. 103–114.
20. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.
21. C.-K. Chu, S. S. M. Chow, W.- G. Tzeng, J. Zhou, and R. H. Deng, "Key- aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 99, no. PrePrints, p.1,2013. Available: http:// doi.ieeecomputersociety.org /10.1109/TPDS. 2013.112.
22. M. Chase and S. S. M. Chow, "Improving privacy and security in multi- authority attribute-based encryption," in Proc. ACM Conf. Comput. Com- mun. Security, 2009, pp. 121–130.
23. 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.
24. Security Challenges for the Public Cloud, KuiRen, Cong Wang, and Qian Wang • Illinois Institute of Technology, IEEE Published by the IEEE Computer Society, 1089-7801/12/$31.00 © 2012, January/February 2012.
25. Secret Sharing for Health Data in Multi-Provider Clouds, Tatiana Ermakovaand Benjamin Fabian.