© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Privacy Preserving, Distributed and Secured Patient-controlled Mobile Health Record System

Sahana Andal R, Megana L. P, K. Tamilarasi
Computer Science and Engineering, Anna University Velammal Institute of Technology,
Panchetti, Tiruvallur District, Tamilnadu, India

ABSTRACT

In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers equipped with their own cloud servers for medical consultant. And also it gives the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering. In this paper, the security and anonymity level of our proposed construction is enhancing by number of patients' attributes to deal with the privacy leakage in patient sparsely distributed cloud system. Data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. Data mining is primarily used today by companies with a strong consumer focus - retail, financial, communication, and marketing organizations.

Keywords: m-healthcare social networks, Data Mining, HIPAA, Key extraction algorithm, Sign algorithm, Encryption and Decryption Model, Key Generation

I. INTRODUCTION

Data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. Data mining is primarily used today by companies with a strong consumer focus - retail, financial, communication, and marketing organizations.

Scope of the Project

The scope of our project a new technique of attribute-based designated verifier signature, a Privacy Preserving, Distributed and Secured Patient-controlled Mobile Health Record System realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. By using model of key extraction algorithm which is used 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 patient's identities by satisfying the access tree with their own attribute sets.

Existing System

All Distributed m-healthcare cloud computing systems have been increasingly adopted worldwide including the European Commission activities, the US Health Insurance Portability and Accountability Act (HIPAA) and many other governments for efficient and high-quality medical treatment. In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers

IJSRSET1522149 | Received: 20 April 2015 | Accepted: 25 April 2015 | March-April 2015 [(1)2: 531-334]

equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering.

- The challenge of keeping both the data confidentiality and patient's identity privacy simultaneously.
- Many existing access control and anonymous authentication schemes cannot be straight forwardly exploited.
- Central cloud computing architecture.

LIMITATIONS OF THE EXISTING SYSTEM

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 systems.

II. METHODS AND MATERIAL

PROPOSED SYSTEM

The security and anonymity level of our proposed system is significantly enhanced by using patient's attributes. The best way for the patient is to encrypt his own PHI under a specified access by each physician a secret key. The algorithms used in this system are,

1.Key extraction algorithm

It's an algorithm for extracting key phrases from text documents. It can be either used for free indexing, where key phrases are selected from the document itself, or for indexing with a controlled vocabulary. KEA can also be used for automatic tagging.

2.Sign algorithm

Digital signatures are used to detect unauthorized modifications to data. Also, the recipient of a digitally signed document in proving to a third party that the document was indeed signed by the person who it is claimed to be signed by. This is known as no repudiation, because the person who signed the document cannot repudiate the signature at a later time. A deterministic algorithm that uses the patient's private key skP , the uniform public key pkD of the healthcare provider where the physicians work and a message m to generate a signature σ. That is, σ ← Sign(skP , pkD,m). Verify. Assume a physician wants to verify a signature.

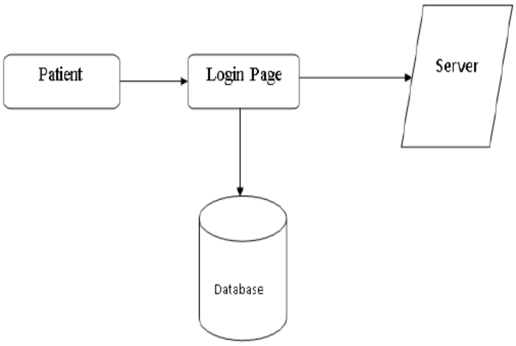
3. Verify and transcript simulation generation algorithm

$$K_{Encp}=e(g1,g2)^{b},\ K_{Enc}=H_2(K_{Encp}),$$
$$K_{Sig}=K_{Encp}e(pk^{HP},g2).$$

The proposed system involves the following modules

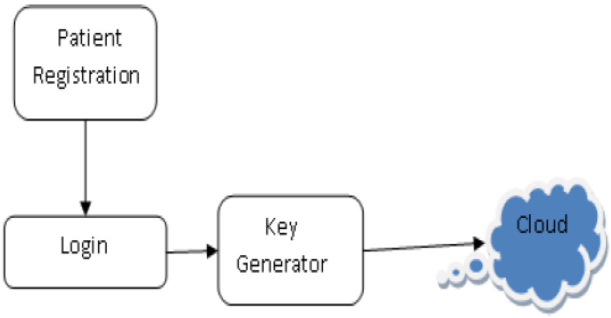
A. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



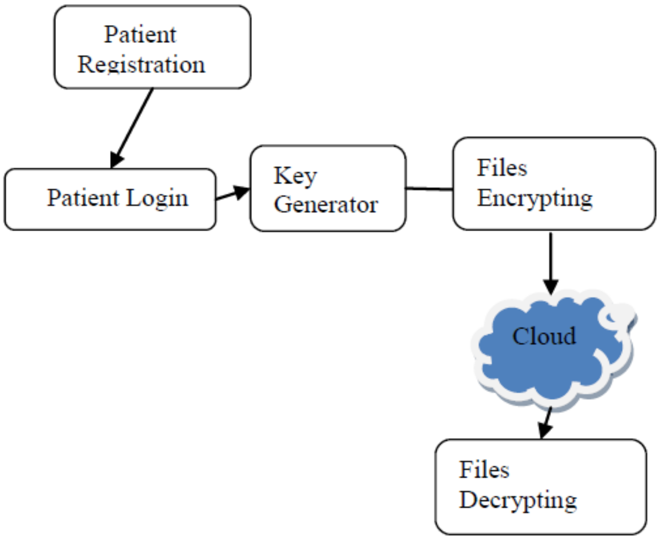
B. Key Generation Model

In this model the key generated by using Anonymous Id Assignment technique for that users wants to sharing the data's to database environment. Because the users upload the N no. of files can upload o the cloud with the ID assignment key only possible.



C. Encryption and Decryption Model

In this model the users wants to upload the files among the database. if either public or private mode of users to shares to the cloud. Whenever the users to upload the files with the key only can upload else can't. The files it could be either multimedia or any kind of files we can upload with the help of key. And the values finally converted into encryption model. After that the values are converted into decryption format.



D. Prescription Model

In this model the physician prescribe based on the problems and the physician will know about the patient's details regarding the problems.

EXISTING SYSTEM	**PROPOSED SYSTEM**
• The challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. • Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited.	• The security and anonymity level of our proposed system is significantly enhanced by using patient's attributes. • The best way for the patient is to encrypt his own PHI under a specified access by each physician a secret key.
TECHNIQUE:- • Central cloud computing architecture.	**ALGORITHM:-** • Key Extraction algorithm. • Verify and Transcript Simulation Generation algorithm
TECHNIQUE DEFINITION:- • To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. • There has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs).	**TECHNIQUE DEFINITION:-** • Propose an enhanced MA-ABE scheme. • In particular, an authority can revoke a user or user's attributes immediately by re-encrypting the cipher texts and updating users' secret keys.

III. CONCLUSION

A new model authorized accessible privacy model and a Privacy Preserving, Distributed and Secured Patient-controlled Mobile Health Record System realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system are proposed. An authentication scheme realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our system can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

IV. FUTURE ENHANCEMENT

The patient attribute values are stored in among cloud server only based on the patient problem not for maintained every patient. The separated data base we are allocated to every problem. So, that easily to achieve the data mining concept. The patient value must be an encrypted; the encrypted data's are stored among the cloud Server. The time of entering the patient must and should login then only permit to allow the take all attribute tests. So the login and the encrypted values to be decrypted by the same key only access. Method that involves finding existing patterns in data. In this context patterns often means association rules. The original motivation for searching association rules came from the desire to analyze supermarket transaction data, that is, to examine customer behavior in terms of the purchased products. The extension of the proposed main scheme the formal security proof and efficiency evaluations which illustrate various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

V. REFERENCES

[1] L.Gatzoulis and I. Iakovidis, Wearable and Portable E-health Systems, IEEE Eng. Med. Biol. Mag., 26(5):51-56, 2007.

[2] I. Iakovidis, Towards Personal Health Record: Current Situation, Obstacles and Trends in Inplementation of Electronic Healthcare Records in Europe, International Journal of Medical Informatics, 52(1):105-115, 1998.

[3] E. Villalba, M.T. Arredondo, S. Guillen and E. Hoyo-Barbolla, A New Solution for A Heart Failure Monitoring System based on Wearable and Information Technologies, In International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006, April, 2006.

[4] R. Lu and Z. Cao, Efficient Remote User Authentication Scheme Using Smart Card, Computer Networks, 49(4):535-540, 2005.

[5] M.D.N. Huda, N. Sonehara and S. Yamada, A Privacy Management Architecture for Patient-controlled Personal Health Record System, Journal of Engineering Science and Technology, 4(2):154-170, 2009.

[6] S. Schechter, T. Parnell and A. Hartemink, Anonymous Authentication of Membership in Dynamic Groups, in Proceedings of the Third International Conference on Financial Cryptography, 1999.

[7] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner and J. Thierry, Anonymity and Application Privacy in Context of Mobile Computing in eHealth, Mobile Response, LNCS 5424, pp. 148-157, 2009.

[8] 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.

[9] S. Yu, K. Ren and W. Lou, FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks, In IEEE Infocom 2009.

[10] F.W. Dillema and S. Lupetti, Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment, In HealthNet 2007.

[11] 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.

[12] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for Ehealth Systems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.

[13] J. Sun, X. Zhu, C. Zhang and Y. Fang, HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare, ICDCS'11.

[14] 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 Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, October, 2008.

[15] J. Zhou and M. He, An Improved Distributed Key Management Scheme in Wireless Sensor Networks, In WISA 2008.