Lightweight Traceable Smart Health Care System Using Cloud Computing

Kamini Jagtap[1], Rani Chouhan[2], Priyanka Ransing[3], Ritesh Thakur[4]
[1, 2, 3] Dept of Computer Engineering
[4]Associate Professor, Dept of Computer Engineering
[1, 2, 3, 4] Institute of Knowledge College of Engineering, Maharashtra, India

Abstract- *Cloud based data is safer than paper and client-server records. Now, medical practices just have to be willing to look to the cloud for the future of healthcare IT. There are lots of security issues related with the storage of sensitive personal health information in the cloud, which will make lots of security challenges to the EHR privacy and confidentiality. Cryptography is an essential tool that helps to assure our data accuracy. The Cryptographic techniques can be employed to protect the data in cloud environment. The technique used for security is multiple authority attribute based encryption technique which focuses on the multiple data owner scenario and divide the users in the PHR system into multiple security domains which leads to key management complexity for owners and users. In the proposed distributed attribute based encryption scheme PHR can be accessed from any hospital using a single key thereby reducing the complexity of key management.*

Keywords- Attribute based encryption, Cloud Computing, Key management, Personal Health Record.

I. INTRODUCTION

Cloud computing is an efficient technique by which the user can access data from anywhere and anytime through internet. Thus, it provides the new world of computing technology to the world. The personal health reords are thus also using this cloud computing technology for the efficient storage and retrieval system. But there is still a comparison is going on with the electronic health record and personal health record. Electronic health record is the electronic version of the medical record of the care and treatment the patient receives. It is maintained and managed by the health care organizations. But our Personal Medical Record is the collection of important information that the patient maintain about their health or the health of someone they are caring for. It may be short and simple or very detailed. The traditional Personal Medical Record was in the form of paper documents, electronic files maintained by their computer, but now the Personal Medical Record is created by using the tools available in the internet. So which make the facility to use the health information across any distances, and to share with the selective users with special read and write access.

The data stored in the cloud get increased every day and hence we need some mechanisms to ensure that our data is stored in secured manner without any unauthorized access. The main goal is to provide secure health record access even from different hospitals and efficient key management at the same time. Healthcare is an essential part of life.

Unfortunately, the steadily aging population and the related rise in chronic illness is placing significant strain on modern healthcare systems, and the demand for resources from hospital beds to doctors and nurses is extremely high. Evidently, a solution is required to reduce the pressure on healthcare systems whilst continuing to provide high-quality care to at risk patients.

Moreover, the busy work schedule in medical institutions also does not allow their physicians to wait for the charging of portable devices when their batteries are drain. Thus, it is critical to keep operations in all mobile devices lightweight in a mHealth system.

II. THE CLOUD BASED HEALTH CARE SYSTEM

The healthcare represents one of the challenges that every country is facing today. Although healthcare industry invests heavily in information technology, yet the promised improvement in patient safety and productivity have not been realized up to the standards. Digital information is siloed between departments and applications. Sharing of patient data among clinicians, departments and even patients is rare and complex. Cloud in healthcare may be the answer to enabling healthcare organizations to focus their efforts on clinically relevant services and improved patients outcomes which will make health monitoring, diagnostics and treatment in more timely and convenient manner and reduced cost The aim of this paper is to propose a Cloud-based healthcare information system intended for indoor use where a methodological approach to the design process is in focus.

The proposed user-driven Design Methodology is used to solve the problems of the real-life scenario of supporting seniors living alone, especially those with limited abilities to manage their daily lives. The conducted design process results in a system proposal that meets the required assumptions. The Cloud Computing is going to revolutionize healthcare in terms of security, privacy and reliability. The tracking, monitoring of patients and healthcare actors are one of the biggest challenging research directions for Cloud Healthcare.

For actual encryption/decryption of data we will be using Advance encryption Standard i.e. AES. The various algorithms which belong to DES standard are prone to attacks and also require huge computation. The major issue in adopting cloud is the security. The data stored in the cloud get increased every day and hence we need some mechanisms to ensure that our data is stored in secured manner without any unauthorized access.

III. PROPOSED FRAMEWORK FOR HEALTH CARE ON CLOUD

This System creates the patient's health record using that sensors data and user information and accumulated data gives the electronic health record (EHR). Also, the proposed system consists of several wireless relay nodes which are responsible for relaying the data sent by the coordinator node and forward them to the base station. The main advantage of this system in comparison to previous systems is to reduce the energy consumption to prolong the network lifetime, speed up and extend the communication coverage to increase the freedom for enhance patient quality of life. Also provide the paperless digital health recode for user can access & send it from anywhere in the environment.

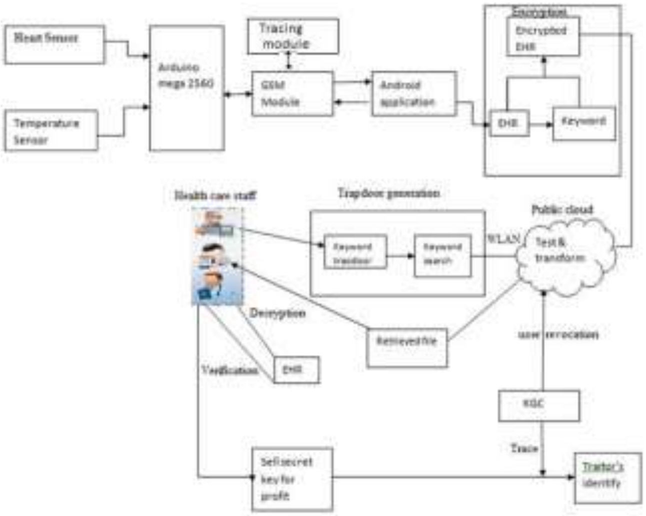

Fig -1 System Architecture

Healthcare staff is the data users in mHealth network. Each data user has a set of attributes, such as affiliation, department and type of healthcare staff, and is authorized to search on encrypted EHRs based on his set of attributes. In mHealth system, a data uses resource-limited mobile terminals to generate keyword trapdoors and conduct the information retrieval operation. The trapdoors are sent to the public cloud via wireless channel and the retrieved EHR files are returned. Then, the data user decrypts the EHR files and verifies the correctness of decryption.

The public cloud has almost unlimited storage and computing power to undertake the EHR remote storage task and respond on data retrieval requests. Lightweight test algorithm is designed in our proposed system to improve performance. KGC generates public parameters for the entire system and distributes secret keys to data users. A data user's set of attributes is embedded in his secret key in LiST to realize access control. If a traitor sells his secret key for financial gain, the KGC is able to trace the identity of the malicious user and revoke his secret key. This module is used to control all the process. Administration is a dynamic work in every field.

IV. MATHEMATICAL MODEL

- Let S be the whole system, S= {I,P,O}, where

  I = Input

  P = Procedure O = Output

- Users u = {Owner, Doctor}, where u= {u1,u2, …..,un}

- Keywords k = {k1,k2,…..,kn}

  H = Heart sensor

  T = Temperature sensor

  D = Details

  EHR = Electronic Health Record

  Trapdoor Generation t = {t1,t2,…..,tn}

- I = {I0,I1,I2,I3} I0 = {H,T,D} I1 = {u}

  I2 = {k}

  I3 = {EHR}

- P = {P0,P1,P2,P3,P4,P5} P0 = EHR encrypted P1 = k

  P2 = t

  P3 = key generate

  P4 = sell secret key

  P5 = KGC

- O= {O0,O1,O2}

  O0 = {EHR decrypted}

  O1 = {User revocation}

  O2 = {Traitors identification}

V. ALGORITHM

1. Key Expansions

For each round AES requires a separate 128-bit round key block plus one more.

2. Initial Round

- AddRoundKey—with a block of the round key, each byte of the state is combined using bitwise xor.

3. Rounds

- SubBytes—in this step each byte is replaced with another byte.
- ShiftRows— for a certain number of steps, the last three rows of the state are shifted cyclically.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

4. Final Round (no MixColumns)

- SubBytes
- ShiftRows
- AddRoundKey

VI. CONCLUSION

We proposed LiST, a lightweight secure data sharing solution with traceability for mHealth systems. LiST seamlessly integrates a number of key security functionalities, such as fine-grained access control of encrypted data, keyword search over encrypted data, traitor tracing, and user revocation into a coherent system design. Considering that mobile devices in mHealth are resource constrained, operations in data owners and data users devices in LiST are kept at lightweight. We formally defined the security of LiST and proved its security without random oracle. The qualitative analysis showed that LiST is superior to most of the existing systems. Extensive experiments on its performance (on both PC and mobile device) demonstrated that LiST is very promising for practical applications.

The personal health records are now considered as the emerging trend in the personal health information exchange field. So cloud computing storage and sharing service is highly utilized by the users. We can provide good security to our data's using encryption technique in cloud the data security is the main privacy issue. Hence, the attribute based encryptions and its variations such as distributed attribute based encryptions are applied for key management and for maximizing the security purpose. The PHR will use more secure encryption primitives in the future for reducing the key management problems and complexity and for providing more secure storage and sharing features to the data stored in the clouds.

REFERENCES

[1] M.P. Radhini, P. Ananthaprabha, P. Parthasarathi, "SecureSharing of Medical Records using Cryptographic Methods inClouds", Volume 3, Issue 4, April 2014

[2] Sapna Tyagi, Amit Agarwal, Piyush Maheshwari, "A conceptual framework for IOT based Health care system using Cloud Computing", 2016.

[3] Damian Dziak, Bartosz Jachimczyk, Wlodek J. Kulesza, "IOT based Information System for Healthcare Application: Design and Methodology Approach", June 2018.

[4] Stephanie B. Baker, Wei Xiang, Ian Atkinson, "IOT for Smart Healthcare: Technologies, Challenges and Opportunity", November 2017

[5] Sonali Muley, Dhamdhere Anand, Sunil Ghige, Omkar Mele, Vishal Yele, "Lightweight Shareable And Traceable secure Mobile Health System", Volume 3, March 2018