Design Secure Mobile Healthcare System with Sharable and Traceable Features

Miss Rote Rohini R[1]., Prof. Markad Ashok V[2].

[1]*ME Second Student, Department of IT Engineering, Amrutvahini College Of Engineering, Sangmner, MH, India*

[2]*Assistant Professor, Department of IT Engineering, Amrutvahini College Of Engineering, Sangmner, MH, India*

Abstract- **Portable well-being (mHealth) has developed as another patient driven model which permits continuous accumulation of patient information by means of wearable sensors, collection and encryption of this information at cell phones, and afterward transferring the encoded information to the cloud for storage and access by human services staff and doctors. In any case, proficient and adaptable sharing of encoded information has been an extremely difficult issue. In this project, we propose a Lightweight Sharable and Traceable (LiST) secure versatile wellbeing framework in which tolerant information are scrambled end-to-end from a patient's cell phone to information clients. Rundown empowers productive catchphrase hunt and fine-grained get to control of encoded information, underpins following of double crosser's who offer their look and access benefits for money related pick up, and permits on-request client denial. Rundown is lightweight as in it offloads the majority of the substantial cryptographic calculations to the cloud while just lightweight operations are performed toward the end client gadgets. We formally characterize the security of LiST and demonstrate that it is secure without irregular prophet. We likewise direct broad examinations to get to the frameworks execution.**

I. INTRODUCTION

Modern healthcare services are serving patient's needs by using new technologies such as wearable devices or cloud of things. The new technology provides more facilities and enhancements to the existing health care services as it allows more flexibility in terms of monitoring patient's records and remotely connecting with the patients via cloud of things. However, there are many security issues such as privacy and security of health care data which need to be considered once we introduce wearable devices to the health care service. Mobile health (mHealth) has emerged as a new patient centric model which allows real-time collection of patient data via wearable sensors, aggregation and encryption of these data at mobile devices, and then uploading the encrypted data to the cloud for storage and access by health care staff and researchers. However, efficient and scalable sharing of encrypted data has been a very challenging problem.

In this project, we propose a Lightweight Sharable and Traceable (LiST) secure mobile health system in which patient data are encrypted end-to- end from a patient's mobile device to data users. LiST enables efficient keyword search and fine-grained access control of encrypted data, supports tracing of traitors who sell their search and access privileges for monetary gain, and allows on-demand user revocation. LiST is lightweight in the sense that it offloads most of the heavy cryptographic computations to the cloud while only lightweight operations are performed at the end user devices. We formally define the security of LiST and prove that it is secure without "Secure Mobile Health System with Sharable and Traceable Features" random oracle. We also conduct extensive experiments to access the system's performance. The use of information technology within the health care domain is increasing day by day all over the world. Previously, mainly devolved countries were using computers and their devices within the health care domain. But nowadays developing countries are also moving towards it. Coverage of mobile networks in most of all areas in a country makes everyone interested to use mobile phones. And within the last few years the uses of smart phones drastically increased. Due to this change, user community is pushing for development of mobile applications. Now user can use most of all desktop applications in their smart phones. Even health care service providers and patients are feeling comfortable to use mobile devices for patient records and/or patient diagnostic process. The use of mobile phone within the health care domain is called m-healthcare. An m-healthcare application can be used by patients as well as by physicians.

II. RELATED WORK

To acknowledge fine-grained get to control for outsourced information, ABE gives a cryptographically way to deal with accomplish one-to- numerous information encryption and sharing. The idea of ABE was first advanced by Goyal. et al [5]. They proposed the first key arrangement ABE (KP-ABE) plot and the main cipher text strategy ABE (CP-ABE) conspire in view of access tree. Ostrovsky et al [6] presented another KP-ABE plan such that users private key can speak to any Boolean access recipe over traits. To expel the confided in focal specialist, [7] and [8] display multi-expert framework to acknowledge decentralized ABE. In any case, these plans experience the ill effects of a vast calculation overhead. Keeping in mind the end goal to decrease the calculation operations at an end clients gadget, Green et al. [9] acquainted outsourcing unscrambling instrument with ABE framework, which enables an intermediary to change a cipher text into another shape so the client can recuperate the message productively. Be that as it may, the rightness of change in [9] cannot be confirmed. Afterward, Lai et al. [10] exhibited an irrefutable outsourced unscrambling (VOD) ABE conspire by affixing a repetitive message as the helper confirmation data. Despite the fact that irrefutability is accomplished in [10], it pairs the length of cipher text and presents huge overhead in encryption operation. The VOD issue is additionally talked about in plans [11], [12]. The unscrambling calculation overhead is diminished in these plans, however the encryption cost still develops with the unpredictability of access structure. Moreover, these plans cannot give look work on cipher texts. Another issue in the ABE instrument is that a client's mystery key is related with an arrangement of properties instead of the client's personality. A similar arrangement of traits can be shared by a gathering of clients. On the off chance that a malevolent approved client offers his mystery key for monetary benefit, it is difficult to recognize the suspect in the customary ABE plans. The issue of following the first client from a mystery key is named as white-box traceability. In the event that the spillage is the unscrambling gear rather than the mystery key, this more grounded following thought is called discovery traceability. Existing double crosses following plans either requires the upkeep of a client list or brings about a vast calculation overhead. In this paper, we give an answer for lightweight white-box traceability

III. OBJECTIVES

We have planned to develop an application that will provide interface to both physicians and patients. We have developed an m-healthcare application that will provide secure, trustful and reliable communication for different communities in healthcare area.

IV. PROPOSED SYSTEM

In the system, a node has attached on human (Patients) body and this node collect all the signals from the wireless sensors. After collecting the signals it sends them to the base station. The attached sensors on patient's body form a wireless body sensor network (WBSN) and they are able to sense the heart rate, blood pressure and so on. This system can detect the abnormal conditions, issue an alarm to the Patient and send a SMS/E-mail to the physician. 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. We have developed this system for managing multi-patient architecture for hospital healthcare. In the above architecture four types of parties are consists: Wireless Body Sensor Network, Health care staff, Public cloud, Key generation algorithm.

The main role of WBSN is like data owner. This sensor embedded inside or outside the body of patients. This sensor continuously monitoring patients parameters like chronic diseases such as diabetes, asthma and heart problems. This patient information are collected and transmitted to a mobile device via wireless interface such as Bluetooth or WLAN. Patients assign such keyword to find out health information from record. Healthcare staff is act as a data user in mHealth network. Each data user or Healthcare staff has a set of attributes like affiliation, department and type of healthcare staff. Data user or healthcare staff is authorized to search encrypted HER based on his set of attributes. The mHealth system generate keyword trapdoor and send it to cloud. Public cloud has unlimited storage. KGC algorithm generates public parameter for the system and distributes secret key to data users.

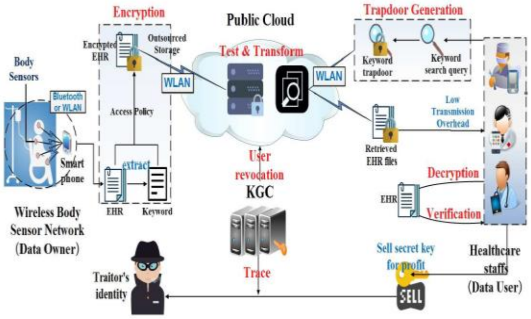
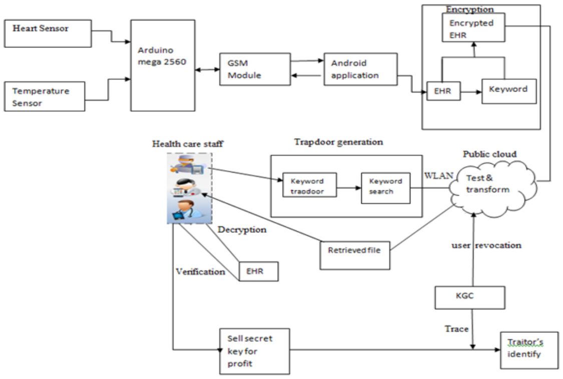


FiG : LiST System Architecture

V. METHODOLOGY



1. WBSN (data owner):

WBSN involves tiny wireless sensors that are embedded inside or surface-mounted on the body of a patient. These sensors continuously monitor the vital physiology parameters of the patient suffering from chronic diseases such as diabetes, asthma and heart problems. Collected personal health data are aggregated and transmitted to a mobile device via wireless interface, such as Bluetooth or WLAN. Keyword to depict the health information is extracted from the health record. Then, the keyword and EHR are encrypted into a cipher text under a specific access policy.

2. Healthcare Staff (data user):

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.

3. Public Cloud:

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.

4. KGC:

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.

VI. SYSTEM REQUIREMENTS

A. Software Requirement

1) Technology used: Java
2) Tools: Jdk 1.5 or above
3) IDE: Netbeans
3) Operating System: Windows 7 or above

B. Hardware Requirement

1) Hard Disk: 80 GB
2) Ram: 2 GB
3) Processor: Intel Pentium 4 and above
4) Android Mobile

VII. MATHEMATICAL MODEL

- Let S be the whole System,

S= {I, P, O}
I=input
P=procedure
O= Output
• Users U = {owner, doctor, health care staff}
U = {U1, U2... Un}
Keywords k = {k1, k2...kn}
H = heart sensor T = temperature sensor
D = details
HER = Electronic Health Record Trapdoor generation t = {t1, t2, tn}
• I = {I0, I1, I2, I3}
I0 = {H, T, D}
I1= U
I2= k
I3 = HER
• P = {P0, P1, P2, P3, P4, P5}
P0 = EHR encrypted (AES algorithm used)
P1 = k
P2 = t
P3 = key generate
P4 = sell secrete key
P5 = KGC
• O = {O0, O1, O2}
O0 = EHR decrypted
O1 = User revocation
O2 = Traitors identify

VIII. ALGORITHM

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

2. InitialRound
- 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.

VIII. 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.

REFERENCES

[1] L. Guo, C. Zhang, J. Sun, Y. Fang. “A privacy-preserving attribute based authentication System for Mobile Health Networks”, IEEE Transactions on Mobile Computing, 2014.

[2] A. Abbas, S. Khan, “A review on the state-of-the-art privacy preserving approaches in e-health clouds”, IEEE Journal of Biomedical Health Informatics, 2014.

[3] J. Yang, J. Li, Y. Niu, “A hybrid solution for privacy preserving medical data sharing in the cloud environment”, Future Generation Computer Systems, 2015.

[4] V. Goyal, O. Pandey, A. Sahai, B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data”, Proc. 13thm ACM Conf. Computer and Comm. Security (CCS06), 2006.

[5] R. Ostrovsky, A. Sahai, B.Waters, “Attribute-based encryption with no monotonic access structures”, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007.

[6] J. Han,W. Susilo, Y. Mu. "Improving privacy and security in decentralized cipher text-policy attribute-based encryption", IEEE Transactions on on Information Forensics and Security, 2015.

[7] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption", IEEE transactions on parallel and distributed systems, 2013. "Secure Mobile Health System with Sharable and Traceable Features"

[8] M. Green, S. Hohenberger, B.Waters, "Outsourcing the decryption of ABE cipher texts", in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

[9] J. Lai, R. H. Deng, C. Guan, J. Weng, "Attribute-based encryption with verifiable outsourced decryption", IEEE Trans. Inf. Forensics Security, Aug. 2013.

[10] B. Qin, R. H. Deng, S. Liu, S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption", IEEE Trans. Inf. Forensics Security, JULY. 2015.