OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

LIGHTWEIGHT SHAREABLE AND TRACEABLE SECURE MOBILE HEALTH SYSTEM

Sonali Muley [1],Dhamdhere Anand [2],Sunil Ghige [3],Omkar Mele [4] ,Vishal Yele [4]

Assistant Professor, Department of Computer Engineering, MMIT Engineering College, Lohegaon, Maharashtra, India[1]

Student, Department of Computer Engineering, MMIT Engineering College, Lohegaon, Maharashtra, India[2 3 4 5]

Abstract: **Mobile Health (mHealth) is a patient driven model used to collect patient information using wearable sensors and cell phones. After collecting the information it is encrypted and encoded and sent to the cloud for storage And accessed by healthcare staff and researchers. In this project, we propose a Lightweight Shareable and Traceable (List) secure versatile well-being framework in which tolerant information are scrambled end-to-end from a patients cell phone in secured manner. List not only concentrates on health but also it concentrates on data security and performance which had been major hurdle in past systems. It enables efficient keyword searching and efficient access control of encrypted data. List offloads the majority of the substantial cryptographic calculations to the cloud while just lightweight operations are performed towards the clients end. We formally characterize the security of List and demonstrate that it is secure without compromising systems performance. To secure patient's private health related data we have proposed Lightweight Shareable and Traceable Secure Mobile Health System.**

Keywords: *Access control, Searchable encryption, Traceability, User revocation, Mobile health system.*

----------∴∴∴----------

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 healthcare 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 healthcare data which need to be considered once we introduce wearable devices to the healthcare 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 healthcare staff and researchers. However, efficient and scalable sharing of encrypted data has been a very challenging problem. In this paper, we propose a Lightweight Shareable 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.

The use of information technology within the healthcare domain is increasing day by day all over the world. Previously, mainly developed countries were using computers and their devices within the healthcare 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 healthcare 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 healthcare 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 [4]. 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. Ostro-vsky et al [6] presented another KP-ABE plan such that user's 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 client's gadget, Green et al. [8] 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 [8] cannot be confirmed. Afterward, Lai et al. [9] 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 [10], [11]. 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 System Architecture

In the proposed system, a coordinator node has attached on patient body to collect all the signals from the wireless sensors and sends them to the base station. The attached sensors on patient's body from a wireless body sensor network (WBSN) and they are able to sense the heart rate, blood pressure, temperature and so on.

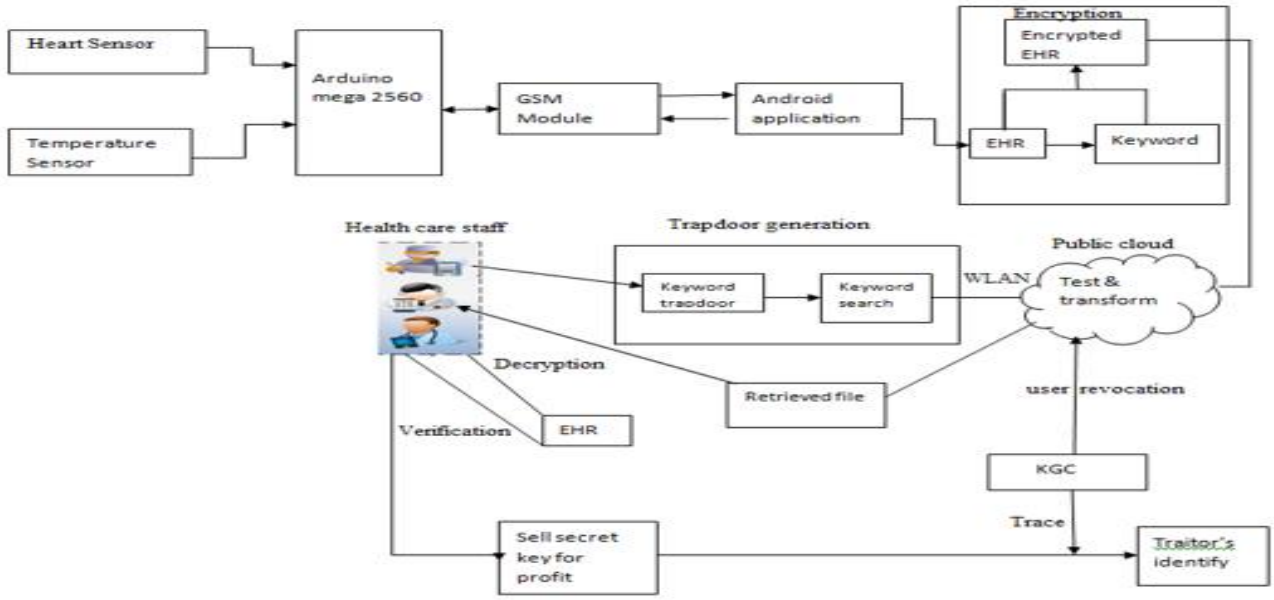

Figure 1: System Architecture

This System creates the patient's health record using that sensors data and user information and accumulated data gives the electronic health record (EHR). 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. Also provide the paperless digital health recode for user can access & send it from anywhere in the environment.

IV 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 fever, 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.

Scheme Description:

This section describes the step by step process of implementation of each and every module of the algorithm.

1.**System Initialization:**

The administrator is responsible for the system initialization.

1. Administrator creates a master key.
2. This Master key is used to access the files.

2. **File Creation:**

Owner of file create health record(EHR).

3.User revocation:

Here, we consider revocation of a data reader or her attributes/access privileges.

There are several possible cases:

1. Revocation of one or more role attributes of a public domain user;
2. Revocation of a public domain user which is equivalent to revoking all of that user's attributes.
3. Revocation of a personal domain user's access Privileges
4. Revocation of a personal domain user. These can be initiated through the PHR owner's client application in a similar way.

4. User Registration:

1. The new users are registered in the cloud.
2. Once the user gets the registration message to the cloud, the cloud sends a private key to the user
3. This private key is associated with a set of attributes.
4. The individual users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy.

5. Write access control:

Prevent the unauthorized contributors to gain write-access to owners PHRs, while the legitimate contributors should access the server with accountability.

File Storing

1. The file which is created is encrypted using attribute based encryption.
2. The cipher-text is stored in the cloud
3. Along with the cipher-text, the file id, the group id, and a group signature is stored.

6. File Read Access:

1. To read the data file in the cloud, the private key of the user is used.
2. This private key is initiated and created by the cloud during user registration.
3. Using this private key, the user can decrypt the files stored in the cloud.
4. Before that, the cloud checks for the revocation list.
5. The user id must not be present in the revocation list.
6. If the user id is present in the list, then the user is not allowed to read the data file in the cloud. The user is considered as an unauthorized user.
7. Else the user is allowed to access and read the cloud.

The users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy.

V CONCLUSION & FUTURE WORK

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. 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, vol. 13, no. 9, pp. 1927-1941.

[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, vol. 18, pp. 1431-1441.

[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, vol. 43-44, pp. 74-86.

[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 (CCS'06), pp. 89-98, 2006.

[5] R. Ostrovsky, A. Sahai, B.Waters, "Attribute-based encryption with nonmonotonic access structures," in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195-203.

[6] J. Han, W. Susilo, Y. Mu. "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," IEEE Transactions on on Information Forensics and Security, 2015, vol. 10, no. 3, 665-678

[7] M. Li, S. Yu, Y. Zheng, K. Ren,W. Lou. "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE transactions on parallel and distributed systems, 2013, 24(1): 131-143.

[8] M. Green, S. Hohenberger, B. Waters, "Outsourcing the decryption of ABE ciphertexts," 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, vol. 8, no. 8, pp. 1343-1354, 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, vol. 10, no. 7, pp. 1384-1394, JULY. 2015

[11] Spvryan's International Journal of Engineering Sciences & Technology (SEST) ISSN : 2394-0905 "Design of a Cloud Based Emergency Healthcare Service Model"