New Secure Healthcare System through Cloud of Things

Mr. Kshirsagar S. B.[1] Prof. Rokade M. D.[2]
[1]ME Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]Sharadchandra Pawar College of Engineering, Dumbarwadi (OTUR), India

Abstract— Mobile health system has a new patient centric model. In this system patients data are collected through wearable sensors, aggregation and encryption of these data at mobile devices. This encrypted data uploaded to the cloud. This data are stored on the cloud. This data are access by healthcare staff and researcher also.

Keywords: encryption, decryption, cloud, user, mobile health system

I. INTRODUCTION

Wearable devices or cloud of things of modern healthcare services are serving patient's needs by using new technologies. 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. we introduce wearable devices to the health care service However, there are many security issues such as privacy and security of health care data which need to be considered once 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. There is very challenging problem however, efficient and scalable sharing of encrypted data. 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. The end user devices Performed LiST is lightweight in the sense that it offloads most of the heavy cryptographic computations to the cloud while only lightweight operations. We 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, health care domain mainly devolved countries were using computers and their devices within the 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 10 years the uses of smart phones drastically increased. Due to this change, user community is pushful for development of mobile applications. Today most of user use mobile application instead of personal application. Even health care service providers and patients are feeling comfortable to use mobile devices for patient records and/or patient diagnostic process. Smart phone with application for health care is known as M-health care application. M-healthcare application is useful for patients and physicians.

II. LITERATURE SURVEY

Electronic healthcare (eHealth) systems mostly used by people instead of paper based medical system because attractive features such as universal accessibility, high accuracy and low cost. As a major component of eHealth systems, mobile healthcare (mHealth) applies mobile devices, such as smartphones and tablets, to enable patient-to physician and patient-to-patient communications for better healthcare and quality of life (QoL). Unfortunately, patients' concerns on potential leakage of personal health records (PHRs) is the biggest stumbling block. In current eHealth/mHealth networks, patients' medical records are usually associated with a set of attributes like existing symptoms and undergoing treatments based on the information collected from portable devices. To guarantee the authenticity of those attributes, PHRs should be verifiable. However, due to the link ability between identities and PHRs, existing mHealth systems fail to preserve patient identity privacy while providing medical services. To solve this problem, this paper proposed a decentralized system for user. Moreover, this design authentication strategies with progressive privacy requirements in different interactions among participating entities. Finally, this system have thoroughly evaluated the security and computational overheads for this proposed schemes via extensive simulations and experiments.

A. 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. [2]

Cloud computing is emerging as a new computing technology in the healthcare sector besides other business domains. Now a day's large numbers of health organizations turns towards e- health information to the cloud environment. M-health clouding provides services like medical records. It works as medical record storage center. Nonetheless, storing the patient health data in the third-party servers also entails serious threats to data privacy. For privacy of the health information of the cloud environment various approaches are used. The Privacy preserving approaches are classified into two types cryptographic and non-cryptographic approaches. Taxonomy of the approaches is also presented.

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

Service provide storing and sharing of medical data in the cloud environment, where computing resources including storage is provided by a third party, raise serious concern of individual privacy for the adoption of cloud computing technologies. Existing privacy protection researches can be classified into three categories, i.e. privacy by policy, privacy by statistics, and privacy by cryptography. However, the

privacy concerns and data utilization requirements of the medical data can be quite different. The solution for medical database sharing in the cloud environment should be support multiple database paradigms. In the real-world cloud multiple privacy demands, which blocks their application. In this paper a practical solution for privacy preserving medical record sharing for cloud computing has been proposed. Based on the classification of the attributes of medical records, it uses vertical partition of medical dataset to achieve the consideration of different parts of medical data with different privacy concerns.

III. PROPOSED SYSTEM

A coordinator node attached on patient body to collect all signals which is send by wireless sensors. This signal send to the base station. Sensors attached on patient's body. Sensor able to sense the patient blood pressure, heart rate through WBSN (Wireless Body Sensor Network). This system can detect the abnormal condition of patients and send SMS or email to 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 in multi-patient architecture for hospital healthcare and compared it with the other existing networks based on multi-hop relay node in terms of coverage, energy consumption and speed.

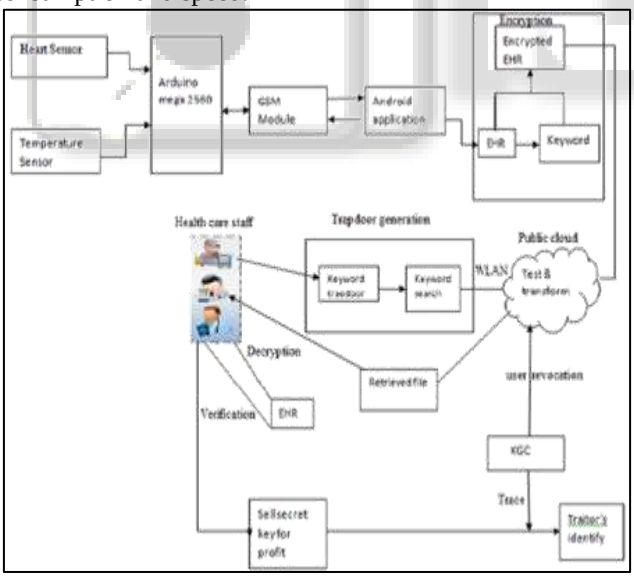

Fig. 1: System Architecture

The flow of the system is given in below:

A. EHR

EHR is generated from a wireless body sensor network. The data owner use such extracted keyword to describe the EHR. Then EHR and keyword both are encrypted. For the encryption the lightweight encryption algorithm are used.

B. Healthcare staff

The main aim of Healthcare staff is to find out query and generate a keyword trapdoor using lightweight trapdoor generation algorithm. This trapdoor is send to public cloud.

C. Public Cloud

The trapdoor generation algorithm send trapdoor to public cloud. Public cloud receive this trapdoor and executes a lightweight test generation algorithm. Lightweight test algorithm is used to find the match cipher text. Public cloud send this matched cipher texts to outsource cipher text. Then this send to the healthcare staff.

D. KGC

KGC stands for key generation algorithm. KGC generate public parameters. This secrete key is distribute to data users. KGC is able to trace the identity of user. KGC trace the user key and revoked his secret key.

IV. CONCLUSION

In this paper, The LiST is proposed. LiST is a Lightweight Sharable and Traceable used to analyze the cause and effects the patients issues. LiST is used to provide a security to patients information. The main features of LiST is sharing data with traceable for mHealth systems. We formally defined the security of LiST and proved its security without random oracle.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] Arindam Banerjee, Prateek Agrawal, R. Rajkumar, "Design of a Cloud Based Emergency Healthcare Service Model", Spvryans International Journal of Engineering Sciences & Technology, 2017.

