ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

Lightweight Sharable and Traceable Secure Mobile Health System

[1]Dr.A.Chinnasamy [2]N.Akilandeswari [3]P.Anitha [4]G.Jaya bharathi
[1]Associate Professor Department of Computer Science and Engineering at Sri Sai Ram Engineering College, Chennai.
chinnasamy.cse@sairam.edu.in.
[234]UG Students Department Computer Science and Engineering at Sri Sai Ram Engineering College, Chennai.
akilapooja2511@gmail.com. anipalani.678@gmail.com.
jayabharathi2502@gmail.com

ABSTRACT:

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 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 random oracle.

We also conduct extensive experiments to access the system's performance.

KEYWORDS:

List, HER, ABE, Financial Gains, Malicious users, Secret Keys

Copyright © 2019 Authors

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

INTRODUCTION:

Health is one important factor for a person's good living. Every human needs to take care of their health in a proper manner. We are designing a light weight sharable and traceable secure mobile health system to trace the health of a person and store them in the cloud. Through various experiments we could determine the performance and efficiency of the system.

LITERATURE SURVEY:

Online search network such as Facebook, Myspace and twitter has experienced a increased growth because of the high security and privacy design bought by the core functionalities of the OSN by utilizing network theory from the paper "Privacy and security for online social networks(1)" The usage of electronic health data from different sources for statistical analysis requires a toolset should cover a wide range of data analysis with different data distributions where the legal, security and privacy concerns have been taken into consideration. The health data are typically located at different general practices and hospitals from the paper "Privacy preserving health data processing(2)".

This paper presents an efficient large-scale data collection in wireless body area network (WBAN) in the presence of cloudlet-based prototype system. The key contribution of this paper is to collect the observed data of WBANs in a large-scale and convey it in consistent manner to the other end of service providers and the result was up to the expectations from the paper "Cloudlet-based efficient data collection in wireless body area networks," Simulation Modeli "Cloudlet-based efficient data collection in wireless body area networks(3)".

WORKING:

The working of the system is as follows:

The user's basic health conditions like Blood pressure, Pulse rate, Body Temperature, Waist-hip Ratio, Sugar, and Humidity are being checked with their respective sensors which entirely contribute to the body sensors. These values are noted and then send to the Electronic health record. These are then assigned with some keywords. Once keyword is obtained it's given in the encrypted health record. From this the doctor could take in any details regarding the patient. For this initially the doctor's identity is being checked with a sell key. If the key given matches with that of the doctor then they would take in the patients information and then retrieve the information about the patient and treat them. Else they would not be able to view it and they would be a traitor.

EXISTING SYSTEM:

In that existing mobile health system, Patient sensible medical related information (Bp value, pulse value, humidity value, and temp value) etc.., should be sense and send to the cloud via mobile. And the doctor should get the patient

 Copyright ⓒ 2019 Authors

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

medical record from cloud.



In that system architecture should not be secure because the cloud is third party vendor, everyone has access the cloud at the time the patient information should be monitor or modify to some malicious users and also the cloud is going to read the patient information and change the values, at the time the user privacy should be affect and the doctor receive the corrupted values..

PROPOSED SYSTEM:

In `our proposed system we have to improve the more security and identify the traitor. First the patient needs to read the medical related values EHR i.e. Electronic Health Records. Patient having read the number of sensor values that's mean (Bp sensor, sugar sensor, temp sensor, pulse sensor, humidity sensor). All the sensor values should be collected and aggregate to EHR. To mitigate security and privacy concerns about EHRs, a common solution is to provide end-to-end encryption by storing EHRs in encrypted form so that they remain private and secure, even if the cloud is not trusted or compromised. The encrypted EHRs, however, must be amenable to sharing and access control.



Attribute based encryption (ABE) is an effective mechanism to provide fine-grained access control on encrypted data, in which secret keys of users and cipher texts are dependent

Copyright ⓒ 2019 Authors

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

upon attributes. In cipher text-policy ABE, which we will adopt, an access policy is associated with a cipher text and a user's secret key is associated with a set of attributes. The cipher text can be decrypted only if the set of attributes associated with the user's secret key satisfies the policy. In addition to fine-grained access control, effective keyword search over encrypted EHRs is an extremely useful feature in practice.

The high value of EHRs might motivate certain rogue healthcare staff, called traitors, to sell their secret keys for financial gains. Hence, it is imperative that the identity of a key owner who maliciously sells his/her secret key in the black market be traceable in mHealth systems. Furthermore, a mHealth system should be able to block the particular healthcare staff.

CONCLUSION:

Thus the proper monitoring of the patients health system could be properly monitored and checked without any type of malpractices in it. Much more security would be given to the data's in it. A high secure cloud is being maintained using the Encrypted electronic health records.

REFERENCE:

[1]Lightweight Sharable and Traceable Secure Mobile Health System
Yang Yang, Member, IEEE, Ximeng Liu, Member, IEEE, Robert H. Deng, Fellow, IEEE, Yingjiu Li, Member, IEEE,

[2] 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, India1 Student, Department of Computer Engineering, MMIT Engineering College, Lohegaon, Maharashtra, India2 3 4 5

[3] Survey on Lightweight Secured Data Sharing Scheme for cloud computing Shubham Chandugade1, Prachi More2, Shaikh Mohammad Shafi Rafiq3 1,2,3 Indira College of Engineering and Management, Dept. of Computer Engineering, Maharashtra, India

[4] Lightweight Traceable Smart Health Care System using Cloud Computing Rani Chouhan1, Kamini Jagtap2, Priyanka Ransing3, Ritesh Thakur4 1,2,3UG Student, Dept. of Computer Engineering, Institute of Knowledge College of Engineering, Maharashtra, India. 4Associate

 Copyright ⓒ 2019 Authors

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

Professor, Dept. of Computer Engineering, Institute of Knowledge College of Engineering, Maharashtra, India.



Dr.A.Chinnasamy born on 26th Nov 1981 in Salem district, Tamilnadu, India. He obtained his Bachelors degree (B.E) in Computer Science and Engineering from Anna University in 2005, Master degree (M.E) in Computer Science and Engineering from Anna University in 2008 and Ph.D., Information and Communication Engineering, Anna University, Chennai, 2017. He is currently working as Associate Professor in the Department of Computer science and Engineering at Sri Sairam Engineering College affiliated to Anna University, Chennai, (INDIA). He research interest is Wireless Communication. He is a life member of the Computer Society of India (CSI), ISTE, IAENG. Reviewer in Measurement and control Journal

Copyright ⓒ 2019 Authors