|| Volume 3 || Issue 6 || June 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Electronic Health Care System Using Cloud

Miss. Shamal S. Jamdade[1], Prof.P.D.Lambhate[2]
Department of Computer Engineering Jaywantrao Sawant College of Engineering and Technology
shamaljamdade11@gmail.com[1], jscoeit@gmail.com[2]

ABSTRACT: ***Portable well being (m-Health) has developed as another patient driven model which permits continuous accumulation of patient information by means of wearable sensors, collection and encryption of these information at cell phones, and afterward transferring the encoded information to the cloud for storage and access by human services staff and scientists. In any case, proficient and adaptable sharing of encoded in-formation has been an extremely difficult issue. In this paper, we propose a Lightweight Sharable and Traceable (LiST) secure versatile well being 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 crossers 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 framework's execution.*

Keywords:- *Access control, search-able encryption, tractability, user revocation, mobile health system.*

I INTRODUCTION

Modern health care services are serving patients 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 patients 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 paper, we propose a Lightweight Sharable and Traceable (LiST) secure mobile health system in which patient data are encrypted end-to-end from a patients 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 systems 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-health care. An m-health care application can be used by patients as well as by physicians.

II REVIEW OF LITERATURE

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 shar-ing. 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. 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 ex-perience 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. [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 opera-tion.

TABLE 1: LITERATURE TABLE

Title	Attribute based Encryption, Decryption	Security, Access Control	Ehealth Cloud, AES
1. A privacy preserving attribute based authentication System for Mobile Health Networks IEEE 2013	Y	Y	N
2. .A review on the state-of the- art privacy preserving approaches in e-health clouds IEEE 2014	Y	Y	Y
3. A hybrid solution for privacy preserving medical data sharing in the cloud environment2014	N	Y	Y
4. Attribute based encryption for fine-grained access control of encrypted data 2006	N	Y	Y

The VOD issue is additionally talked about in plans [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. [13].In this paper, we give an answer for lightweight white-box traceability.

III EXISTING SYSTEM

A introduced a distributed attribute based encryption technique because ciphertext policy attribute-Based Encryption allows to encrypt data under an access policy, specified as a logical combination of attributes. Such cipher-texts can be decrypted by anyone with a set of attributes that fits the policy. But in distributed attribute-based encryption (DABE), where an arbitrary number of parties can be present to maintain attributes and their corresponding secret keys. This is in bare difference to the classic ciphertext policy attribute based encryption schemes, where all keys are distributed by one central trusted party. We provide the construction of a DABE scheme; the construction is very efficient for encryption and decryption.

A Secure attribute based systems in which attributes define and classify the data to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In which a novel secure information management architecture is introduced based on emerging attribute-based encryption primitives. A policy sys-tem that meets the needs of complex policies is defined and illustrated. Based on the needs of those policies, therefore proposed a cryptographic optimizations that vastly improve enforcement efficiency.

IV PROPOSED SYSTEM

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 patients 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 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.

V. SYSTEM ARCHITECTURE

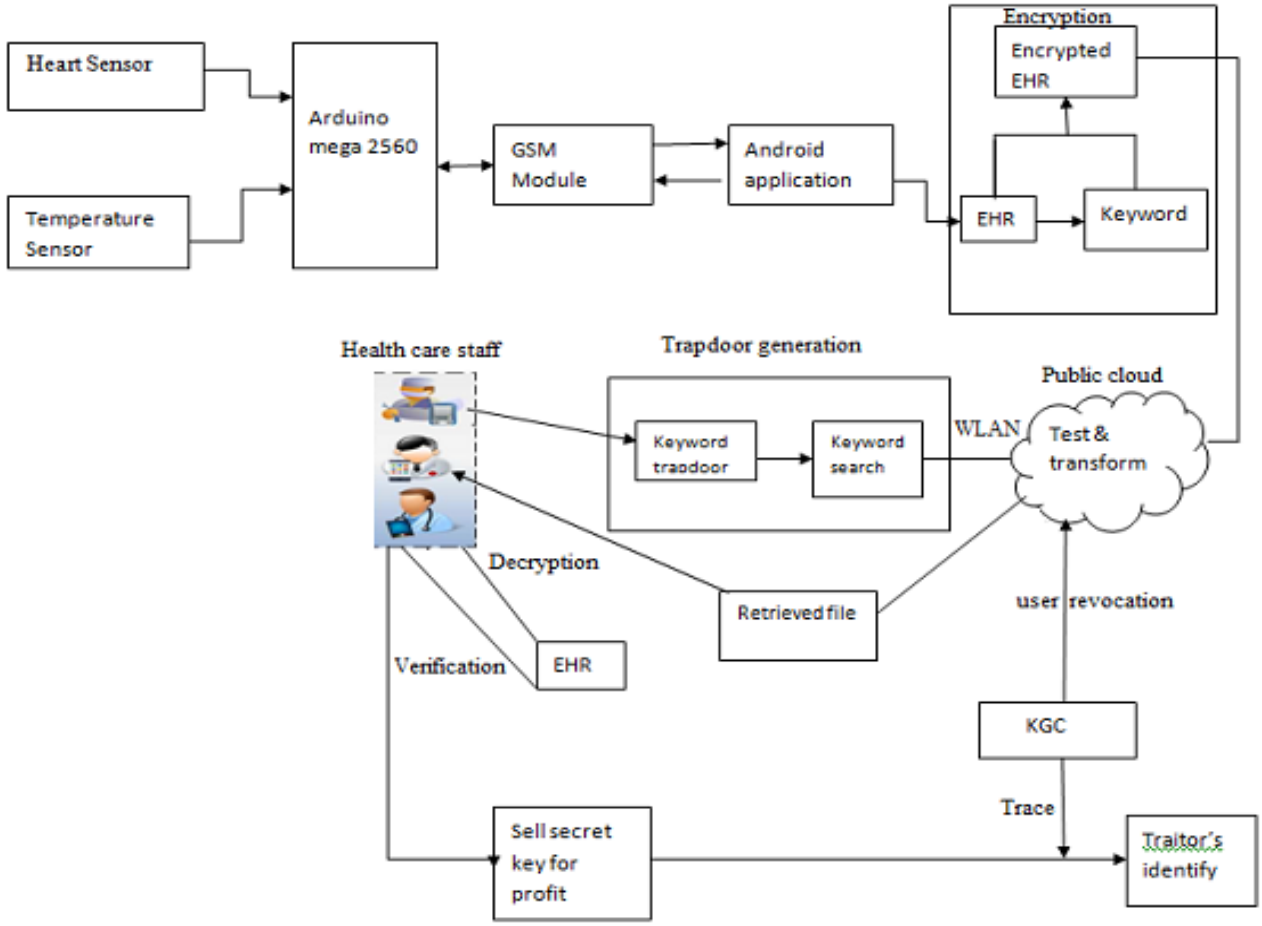

Figure. 1. System Architecture

VI. SYSTEM REQUIREMENTS

Software Requirement

Technology Used : Core Java, Advanced Java
Tools : JDK 1.5 or above, Eclipse
Operating System : Windows XP or above

Hardware Requirement

Hard Disk : 80 GB
RAM: 512 MB
Processor : Intel Pentium 4 and above
Android Mobile
Ardunio Microcontroller
Healthcare Sensors

VII. MATHEMATICAL MODEL

System Description:

Let S be the whole System,

S= {I, P, O}
I=input
P=procedure
O= Output
Users u={owner, doctor, health care staff}
Keywords k= {k1, k2...kn}
H= heart sensor
T= temperature sensor
D=details
HER=Electronic Health Record
Trapdoor generation t= {t1, t2, tn}
I = fI0, I1, I2, I3g I0 = {H, T, D}
I1= u
I2= k
I3 = EHR
P = {P0, P1, P2, P3, P4, P5}
P0 = EHR encrypted (AES algorithm used)
Enc(m,(M,),KW) To CT.
P1 = k
Transform(CT,TKW,PKid,s) To CTout
P2= t
Trapdoor(SKid,s,KW) TO TKW
P3= key generate
KeyGen(MSK,id,S) To (PKid,s,SKid,s)
P4= sell secrete key
KeySanityCheck(SKid,s) To 1/0
P5= KGC
O = fO0, O1, O2g

O0= EHR decrypted
O1= User revocation
O2= Traitors identify

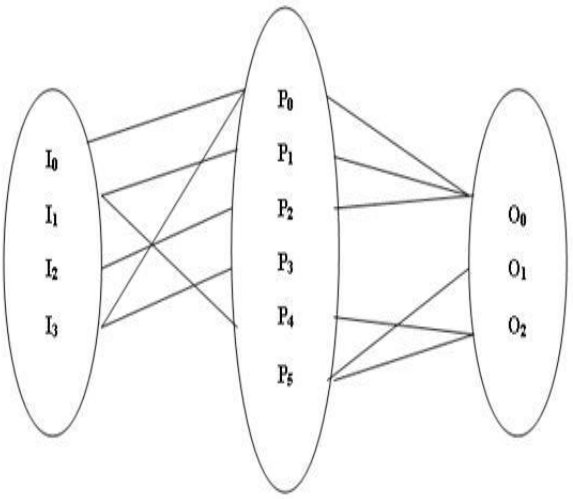

Figure 2 Venn diagram

VIII. ALGORITHM

Key Expansions
For each round AES requires a separate 128-bit round key block plus one more.
Initial Round
Add Round Key with a block of the round key, each byte of the state is combined using bitwise xor.
Rounds
Sub Bytes in this step each byte is replaced with another byte. Shift Rows for a certain number of steps, the last three rows of the state are shifted cyclically.
Mix Columns a mixing operation which operates on the columns of the state, combining the four bytes in each column. Add Round Key
Final Round (no Mix Columns)
Sub Bytes
Shift Rows

IX. APPLICATIONS

This state-of-the-art technology is utilized in vital health-care services to incorporate emerging applications such as remote patient monitoring, electronic health record and collaborative consultation. When we run our applications on the cloud, we are sharing our critical data with cloud and, therefore, se-curity and privacy of data is a very serious issue to be considered.

X ADVANTAGES

The purpose is to develop an m-healthcare application that makes our life easier and saves our time.To provide a secure and trustful m health care application, so that users can use this application for their sensitive data without any doubt of security threat. It is also a user friendly application, so users can easily use the application.

XI. EXPERIMENTAL RESULT

Figure 3. Registration

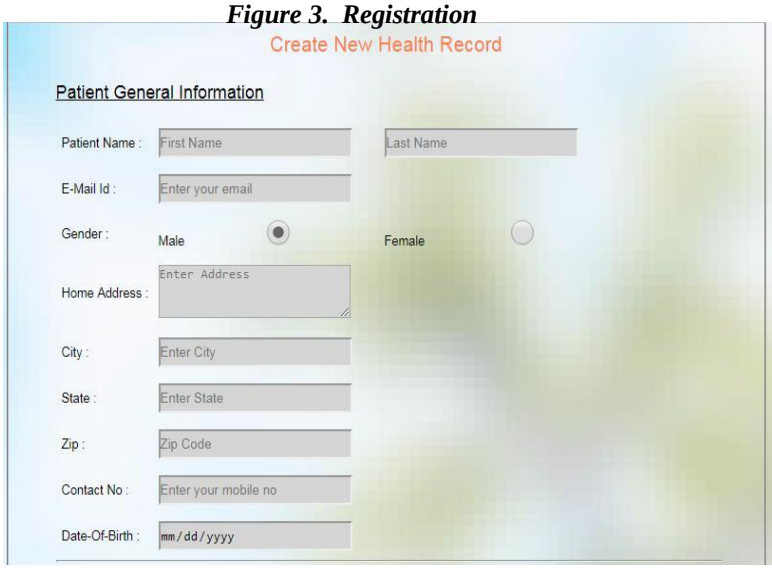

Figure. 4 Create Health Record

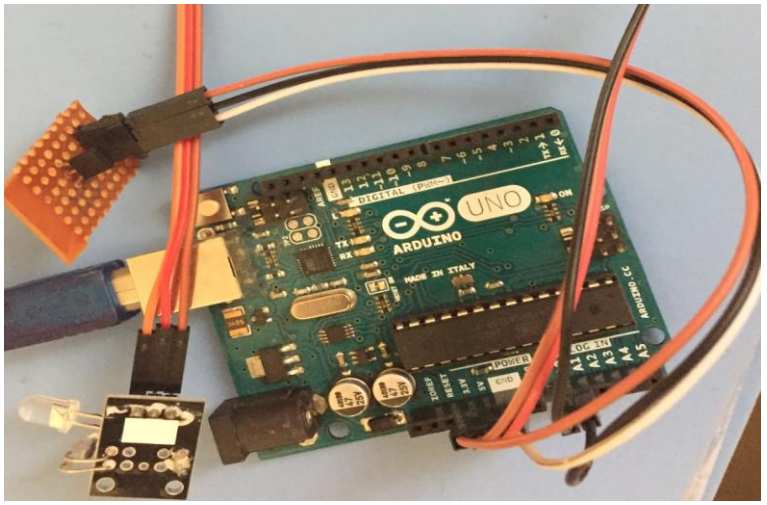

Figure.5 Body Sensor

XII. 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, 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 Infor-matics, 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]http://www.pbs.org/newshour/updates/has-health-care-hacking -become-an-epidemic/.
[5]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), pp. 89-98, 2006.
[6]R. Ostrovsky, A. Sahai, B.Waters, Attribute-based encryption with non-monotonic access structures, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195-203.
[7]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
[8]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.
[9]M. Green, S. Hohenberger, B. Waters, Outsourcing the decryption of ABE ciphertexts, in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.
[10]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.