OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

ELECTRONIC HEALTHCARE SYSTEM

Deepali Gholap[1], Priya Surve[2], Purvi Thale[3], Vaishnavi Saswade[4], Prof. Sharad Adsure[5]
Student, Department of Computer Engineering, BSIOTR, Pune. [1,2,3,4]
Asst. Professor, Department of Computer Engineering, BSIOTR, Pune. [5]

Abstract: **Portable well-being health system 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 portable devices, 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 an Electronic Healthcare System (EHS) secure versatile wellbeing framework in which tolerant information are scrambled end-to-end from a patient's device to information clients. EHS enables fine-grained access control of encrypted information, supports tracing of double crossers who offer their look and access benefits for money related pick up, and permits on-request user revocation. EHS is lightweight in the sense that 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 EHS and demonstrate that it is secure without irregular prophet.**

Keywords: Access control, Searchable encryption, Tractability, User revocation.

---∴∴∴---

I INTRODUCTION

Electronic Healthcare System Modern health care 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. Electronic health (eHealth) 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 website, 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. We propose an Electronic Healthcare System in which patient data are encrypted end-to- end from a patient's to data users. Electronic Healthcare System enables efficient keyword search and ne-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. Electronic Healthcare System 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 EHS 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 developed 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 and Broadband in most of all areas in a country makes everyone interested to use mobile phones and laptops. Due to this change, user community is pushing for development of web applications.

II LITERATURE SURVEY

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 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. [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 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, 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 EXISTING SYSTEM

In the existing system patient personally has to go the hospital for his check-up or doctor has to visit the patient at his home which consumes lot of time as well as energy. Also, there are some systems existing such as Fitness band which may display us our pulse rate, body temperature, etc. but won't provide us with option to remotely share it with anyone. One of the existing systems also introduced a distributed attribute-based encryption technique because cipher text 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.

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 patient's body form a wireless body sensor network (WBSN) and they are able to sense the heart rate, blood pressure and temperature. 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.

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. 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.

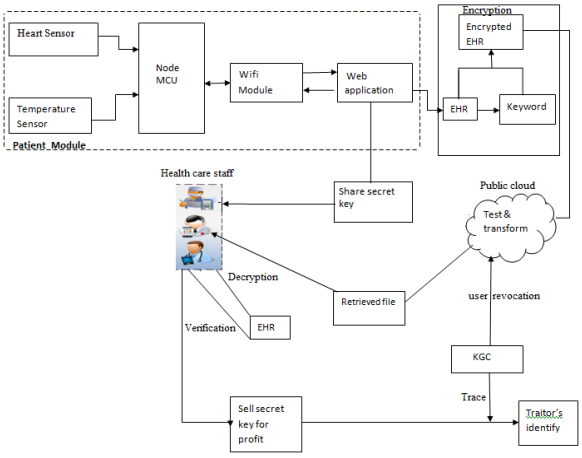


Figure 1: System Architecture

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.

V SYSTEM REQUIREMENTS

Software Requirement

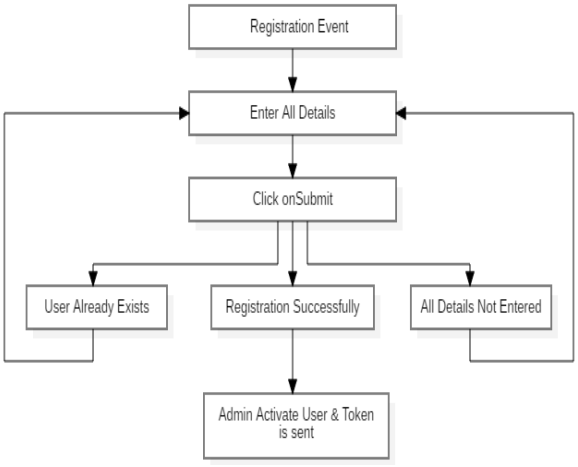
- Operating System: Microsoft Windows 7 or Above
- Front End: HTML, JSP, Java
- Back End: MySQL
- Tools: JDK 8, Netbeans
- Online-Storage: Adrive

Hardware Requirement

- Processor: Intel Core I3 or Higher
- RAM: 4 GB or Higher
- Hard Disk: 100 GB (min)\
- Sensors: Temperature, Heart Rate
- Microcontroller : NodeMCU

VI ALGORITHM

Registration Algorithm



This algorithm specifies the flow of system when the user clicks on Registration button. There can be different cases after clicking the submit button which are specified in the algorithm.

There can be different cases such as-

i) User already registered.

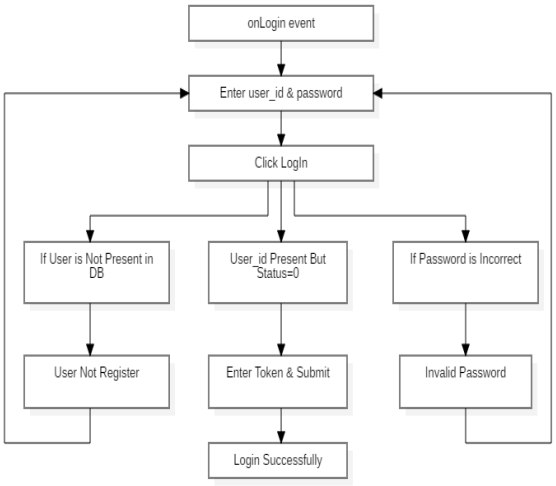
ii) All fields not entered.

iii) Successful registration.

After successful registration first Admin has to activate the user then only the user can login in for first time in the system.

Login Algorithm

This algorithm specifies the flow of system when the user clicks on Login button.



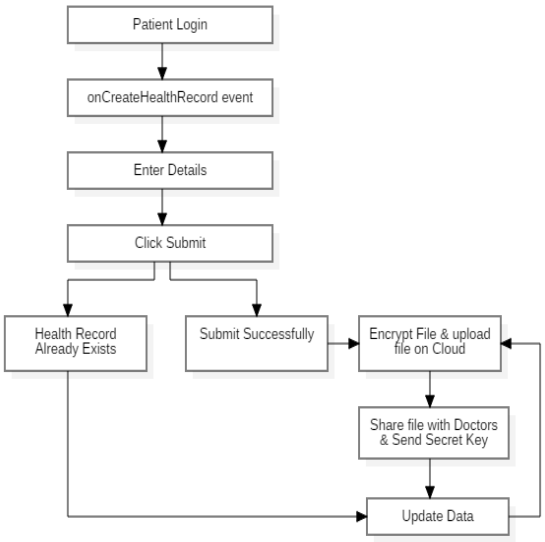
There can be different cases after clicking the submit button such as-

i) User not registered.

ii) Incorrect Password.

iii) Successful logged in

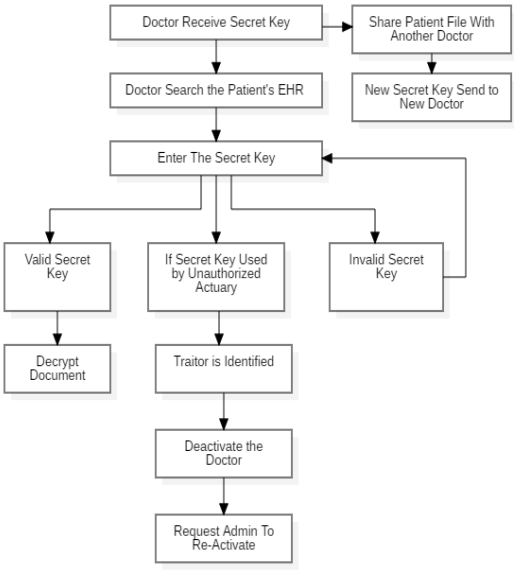
Patient's Algorithm



This algorithm includes the flow of the Patients module.

It specifies the different action performed by patient while creating and sharing his health record with his doctor.

Traitor identification algorithm



This algorithm includes the flow of the Doctors module.

It specifies the different action performed by doctor and also includes traitor identification module.

Encryption Algorithm

AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric block cipher algorithm used for encryption and decryption. The encryption process of AES uses a set of specially derived keys called round keys. These are applied, along with other operations, on a matrix of data that holds exactly one block of data-the data to be encrypted. This array is called as the state array. Following are the steps of AES encryption for a 128-bit block:

Step 1: Derive the set of round keys from the cipher key.

Step 2: Initialize the state array with the block data (plaintext)

Step 3: Add the initial round key to the starting state array.

Step 4: Perform nine rounds of state manipulation.

Step 5: Perform the tenth and final round of state manipulation.

Step 6: Copy the final state array out as the encrypted data (ciphertext).

The reason that the rounds have been listed as “nine followed by a final tenth round” is because the tenth round involves a slightly different manipulation from the others.

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations which are shown in Figureure below.

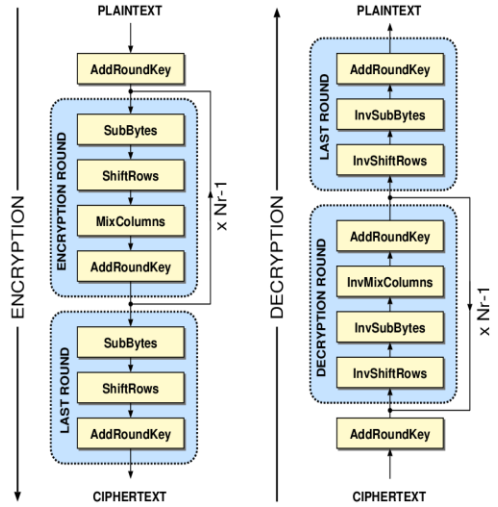


Figure 6: AES working

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 = EHR

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

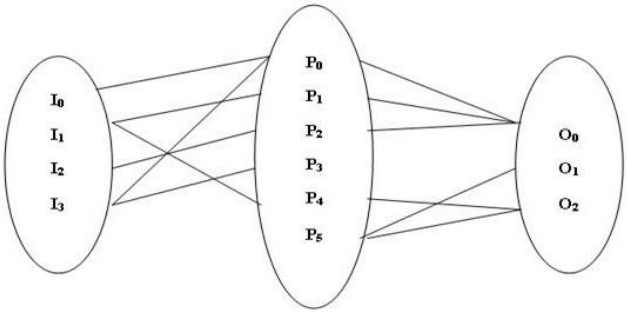
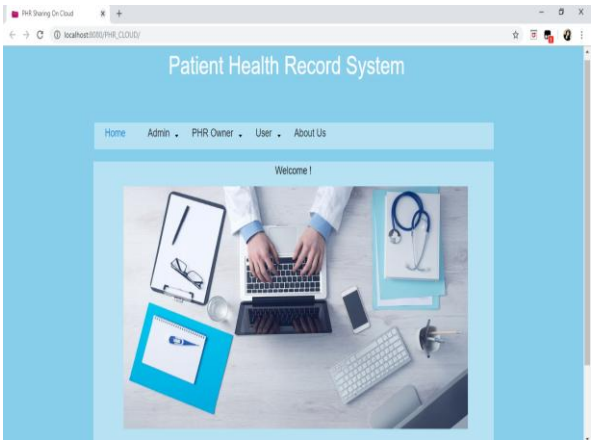


Figure 7: Venn diagram

VIII APPLICATIONS

This modern 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, security and privacy of data is a very serious issue to be considered.

IX OUTPUTS AND RESULTS



X ADVANTAGES

- The purpose is to develop a 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 CONCLUSION

We proposed EHS, a lightweight secure data sharing solution with traceability for Health care systems. EHS continuously 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 rational system design. We formally defined the security of EHS and proved its security without random oracle. The qualitative analysis showed that EHS is superior to most of the existing systems.

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] Deepali Gholap, Priya Surve, Purvi thsle, Vaishnavi Saswade, Prof. Sharad Adsure Electronic Healthcare System, OAIJSE Vol 3, Issue 11, November 2018.

[3] Amruta Shete R , S.D.Satav Survey on Medical Data Sharing Systems with NTRU, IEEE Journal of Biomedical Health Infor-matics, 2017, vol. 4, pp. 1431-1441.

[4] M.P. Radhini, P.Ananthaprabha, P.Parthasarathi3 Secure Sharing of Medical Records Using Cryptographic Methods in Cloud 2014, vol. 43-44, pp. 74-86.

[5] Aakanksha Maliye, Sarita Patil Scalable and Secure Sharing in Cloud Computing Using Data Manipulation & Encryption, IEEE transactions on parallel and distributed systems, 2013, 24(1): 131-143.

[6] 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.

[7] 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.