OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

ELECTRONIC HEALTHCARE SYSTEM

Deepali Gholap[1], Priya Surve[2], Purvi Thale[3], Vaishnavi Saswade[4], Sharad Adsure[5]
Student, Department of Computer Engineering, JSPM's B.S.I.O.T.R., Wagholi, Maharashtra, India[1,2,3,4]
Asst. Professor, Department of Computer Engineering, JSPM's B.S.I.O.T.R., Wagholi, Maharashtra, India [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 these 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 a Electronic Healthcare System (EHS) secure versatile well being framework in which tolerant information are scrambled end-to-end from a patient's device 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 EHS 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.*

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. Electronic Health care 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 base 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 Electronic Healthcare System (EHS) secure mobile health system in which patient data are encrypted end-to-end from a patient's device to data users. EHS 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. EHS 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 REVIEW

To acknowledge fine-grained access 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. 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 speciaEHS, [7]and [8] display multi-expert framework to acknowledge decentralized ABE.

TABLE 1: LITERATURE TABLE

Title	**Publication Year**	**Author**	**Disadvantages**
1.Secure Sharing of Medical Records Using Cryptographic Methods in Cloud.	April-2014	M.P. Radhini, P.Ananthaprabha, P.Parthasarathi	No full access control of the data, descriptive attributes are used to encrypt the data.
2.Survey on Medical Data Sharing Sysytems with NTRU	February-2017	Amruta Shete, S.D.Satav	-
3.A privacy preserving attribute-based authentication system for mobile health networks	2012	Linke Guo, Chi Zhang, Jinyuan Sun and Yuguang Fang	Integrity of the Rank order in the search result assuming the Cloud server is untrusted.
4. Scalable And Secure Sharing in Cloud Computing Using Data Manipulation And Encryption	July-2015	Aakanksha Maliye, Sarita Patil,	There is still lacks an efficient and on-demand user revocation mechanism for ABE and DES with the support for dynamic policy updates/changes which is essential parts of secure PHR sharing.

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 operation. 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.

III EXISTING SYSTEM

An existing system 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. 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 cipher text 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 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 ablation, department and type of healthcare, and is authorized to search on encrypted EHRs based on his set of attributes.

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.

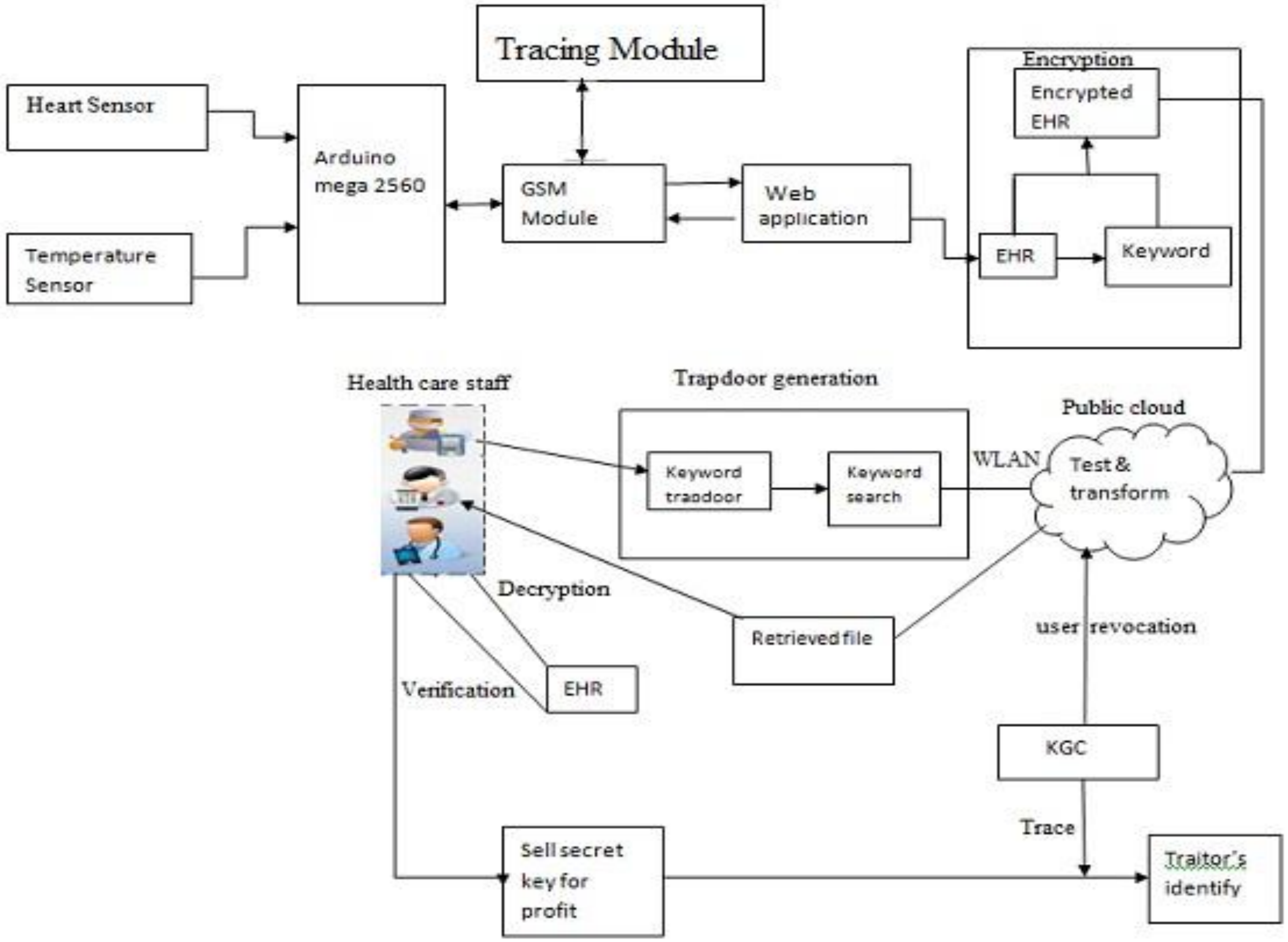

Figure 1. System Architecture

V SYSTEM REQUIREMENTS

Software Requirement

1. Technology Used : Java-JSP
2. Tools : JDK 1.7 or above, Netbeans
3. Operating System : Windows XP or above

Hardware Requirement

1. Hard Disk : 80 GB
2. RAM: 512 MB
3. Processor : Intel Pentium 4 and above
4. Sensors : Temperature , Heart-rate
5. Microcontroller : Arduino mega 2560

VI ALGORITHM

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an 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:

Derive the set of round keys from the cipher key.
Initialize the state array with the block data (plaintext).
Add the initial round key to the starting state array.
Perform nine rounds of state manipulation.
Perform the tenth and final round of state manipulation.
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. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes.

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

SubBytes
ShiftRows
MixColumns
AddRoundKey

Each one of these operations is applied to the current state array and produces a new version of the state array. In all but the rarest cases, the state array is changed by the operation.

Decryption Process:

Decryption involves reversing all the steps taken in encryption using inverse functions:

InvSubBytes
InvShiftRows
InvMixColumns

XorRoundKey doesn't need an inverse function because XORing twice takes you back to the original value. InvSubBytes works the same way as SubBytes but uses a different table that returns the original value. InvShiftRows involves rotating left instead of right and InvMixColumns uses a different constant matrix to multiply the columns.

The order of operation in decryption is:

Perform initial decryption round:
XorRoundKey
InvShiftRows
InvSubBytes
Perform nine full decryption rounds:
XorRoundKey
InvMixColumns
InvShiftRows
InvSubBytes
Perform final XorRoundKey

The same round keys are used in the same order.

VII 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, se-curity and privacy of data is a very serious issue to be considered.

VIII ADVANTAGES

The purpose is to develop an 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.

IX 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] 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.

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

[4] 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.

[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.