JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Auditable Health Records Levering DROPS in Cloud

Tejaswi Wani[1]*, Roshani Raut[2]

Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Pune- 412105, Maharashtra, India
Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Pune- 412105, Maharashtra, India

DOI: https://doi.org/10.26438/ijcse/v7i5.10951100 | Available online at: www.ijcseonline.org

Accepted: 15/May/2019, Published: 31/May/2019

***Abstract*—** In this paper, the system proposed a Lightweight Sharable and Traceable (LiST) secure framework in which tolerant information is scrambled end-to-end from a patient's cell phone to clients. In this system, a sensor attached on the patient body to collect all the signals from the wireless sensors and sends them to the base station; 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 an SMS/E-mail to the physician. The main advantage of this system in comparison to previous systems is to reduce energy consumption and security. In this system, DROPS methodology divides a file into fragments and replicates the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. The attribute authorities (AAs) are responsible for performing user legitimacy verification and generating intermediate keys for legitimacy verified users.

***Index Terms*—** Access control, search-able encryption, tractability, user revocation, mobile health system, cloud security, fragmentation, replication, performance, WBSN, EHR

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 the 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 that allows the real-time collection of patient data via wearable sensors, aggregation, and encryption of these data at mobile devices, and then upload 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. The 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 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 a random oracle. We also 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, mainly devolved countries were using computers and their devices within the health care domain. But nowadays developing countries are also moving towards it. The 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 use of smartphones drastically increased. Due to this change, the user community is pushing for the development of mobile applications. Now users can use most of all desktop applications in their smartphones. 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 phones 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. The file blocks, MAC codes, and version numbers are stored at various levels of the tree. The proposed technique heavily depends on the user's employed scheme for data confidentiality. Moreover, the probable amount of loss in the case of data tempering as a result of intrusion or access by other VMs cannot be decreased. Our proposed strategy does not depend on traditional cryptographic techniques for data security. Moreover, the DROPS methodology does not store the whole file on a single node to avoid compromise of all of the data in case of a successful attack on the node. The authors approached the virtualized and multi-tenancy related issues in the cloud storage by utilizing the consolidated storage and native access control. The Dike authorization architecture is proposed that combines the native access control and the tenant name space isolation. The proposed system is designed and works for object-based file systems. However, the leakage of critical information in case of improper sanitization and malicious VM is not handled. The DROPS methodology handles the leakage of critical information by fragmenting data files and using multiple nodes to store a single file.

In this paper Section I contains the introduction of the system, Section II contains the review of the literature, Section III contains the existing system, Section IV, V contains the proposed system and system architecture, section V explains the result of the system and Section VI conclusion.

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 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 ciphertext strategy ABE (CP-ABE) conspire in view of access tree. Ostrovsky et al [6] presented another KP-ABE plan such that the user's private key can speak to any Boolean access recipe over traits. To expel the confided in focal specialist, [7]and [8] display a 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 the ABE framework, which enables an intermediary to change a ciphertext 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 ciphertext 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 to 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.

TABLE 1: LITERATURE TABLE

Title	**Publication Year**	**Author**	**Disadvantages**
1.Survey on Medical Data Sharing With NTRU	Feb-2017	Amruta Shete, S. D. Satav	Does not Cover all aspects and applications.
2. Scalable and Secure Sharing in Cloud Computing using Data Manipulation and Encryption	July-2015	Aakanksha Maliye, Sarita Patil	There is still lack an efficient and on demad user revocation mechanism for ABE & DES with the support for dynamic policy, update, changes which is essential parts of secure PHR sharing.
3. Secure Sharing in Cloud Computing using Cryptographic Methods	April- 2014	M. P. Radhini, P. Parthasarathi	No access control of Data , Descriptive attributes used for control of Data.
4. A Privacy Preserving attribute based system for mobile health networks.	2012	Linke Guiochi, Zhang, Jinyuan Sun and Yuguang Fang.	Integrity of rank Order the search result assuming the cloud server is untrusted.

III. EXISTING SYSTEM

A introduced a distributed attribute-based encryption technique because ciphertext policy attribute-based Encryption allows encrypting 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. 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 system that meets the needs of complex policies is defined and illustrated. Based on the needs of those policies, therefore proposed cryptographic optimizations that vastly improve enforcement efficiency.

IV. PROPOSED SYSTEM

In the proposed system, a coordinator node has attached on the patient body to collect all the signals from the wireless sensors and sends them to the base station. The attached sensors on a patient's 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 an SMS/E-mail to the physician. Also, the proposed system consists of several wireless relay nodes that are responsible for relaying the data sent by the coordinator node and forward them to the base station. We develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes. The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. We do not rely on traditional cryptographic techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the data. We ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.

V. SYSTEM ARCHITECTURE

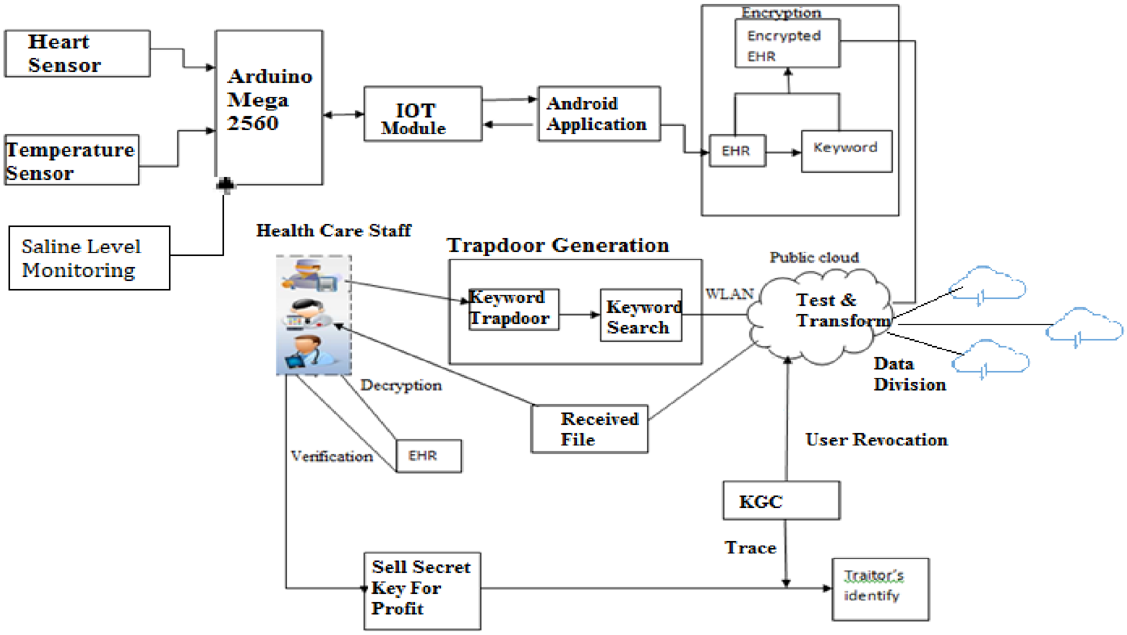
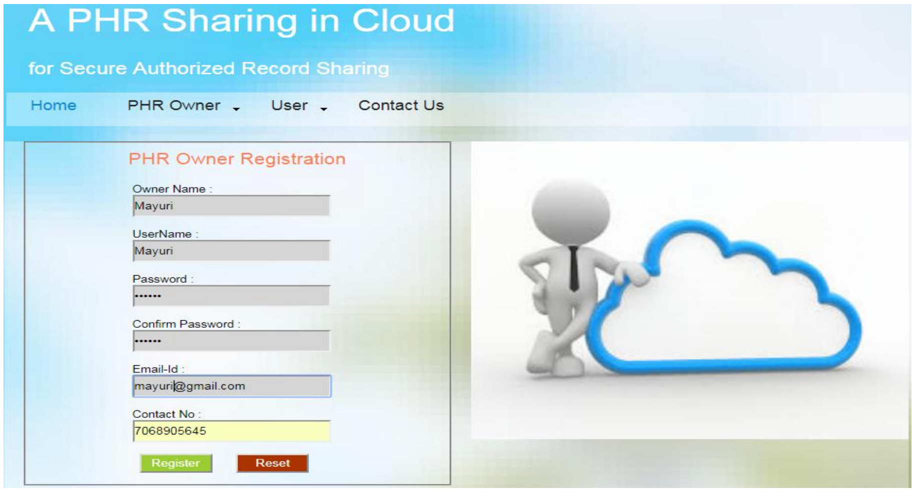


Fig. 1: System Architecture

VI. RESULTS

In our project, the PHR Owner first needs to be register. For registration PHR Owner need to fill the following fields:
The PHR Owner can fill this all fields and click on submit button then you will receive registration is successfully done but if PHR Owner left any field empty then registration is unsuccessful. Numbers of PHR Owners are able to register in the system.



PHR Owner Registration

Owner Name : Mayuri

UserName : Mayuri

Password : ••••••

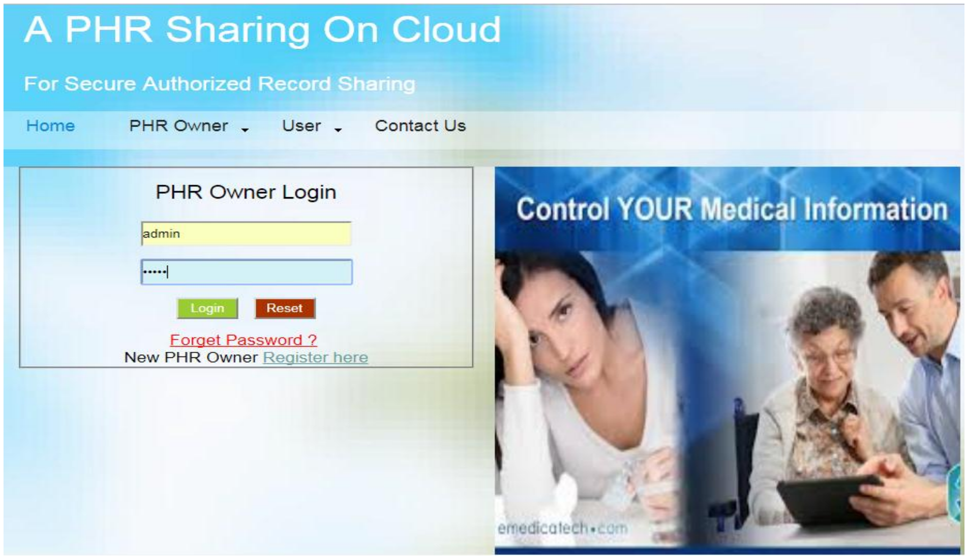
Confirm Password : ••••••

Email-Id : mayuri@gmail.com

Contact No : 7068905645

Fig. 2: Registration of PHR Owner

After registration PHR Owner needs to login to create the health record. In login form, PHR Owner needs to enter username and password then click on login button. If this both fields are correct then the system will login otherwise login will be failed.


A PHR Sharing On Cloud
For Secure Authorized Record Sharing
Home
PHR Owner
User
Contact Us
Login
Reset
Forget Password ?
New PHR Owner Register here
Control YOUR Medical Information
emedicatech.com

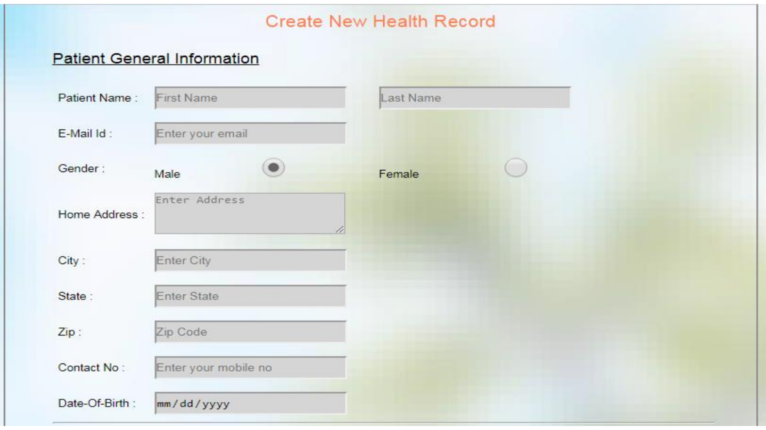
PHR Owner Login

admin

•••••

Fig. 3: PHR Owner Login

After PHR Owner Login to create health records, patient have to fill Personal information like (Patient Name, Email Id, Gender, Address, City, State, Zip, Mobile No, Date of Birth) and health information like (Height, Weight, Body Mass Index, Blood Group, Body Temperature, Blood Pressure, Pulse Rate and Respiratory Rate etc.) after creating health record the text file will be generated.



Create New Health Record

Patient General Information

Patient Name : First Name Last Name

E-Mail Id : Enter your email

Gender : Male ● Female ○

Home Address : Enter Address

City : Enter City

State : Enter State

Zip : Zip Code

Contact No : Enter your mobile no

Date-Of-Birth : mm/dd/yyyy

Fig. 4: Create PHR

In the above Fig. 4 the proposed system will collect the personal health record (body temperature and pulse values) using Node MCU(Marvel Cinematic Universe) which having inbuilt wifi module. The data will be sent on the AWS cloud and on cloud for used machine learning techniques to analyse the patient health conditions. System will helps for continuous monitoring of patient.

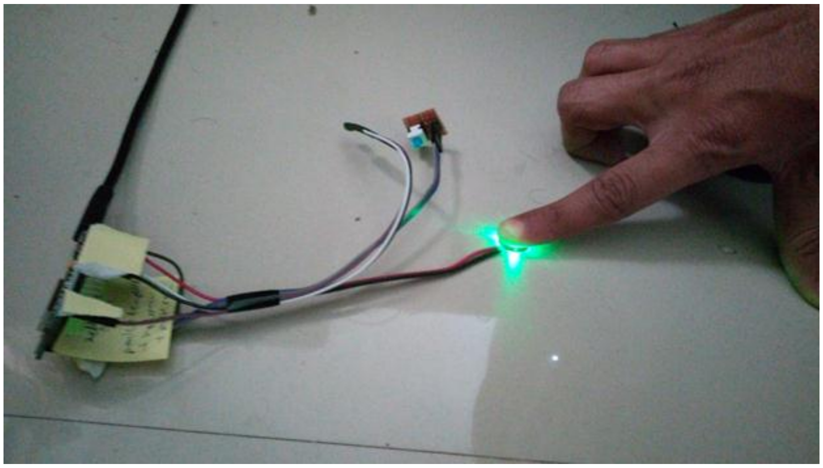


Fig. 5: Collecting pulse and body temperature of patient

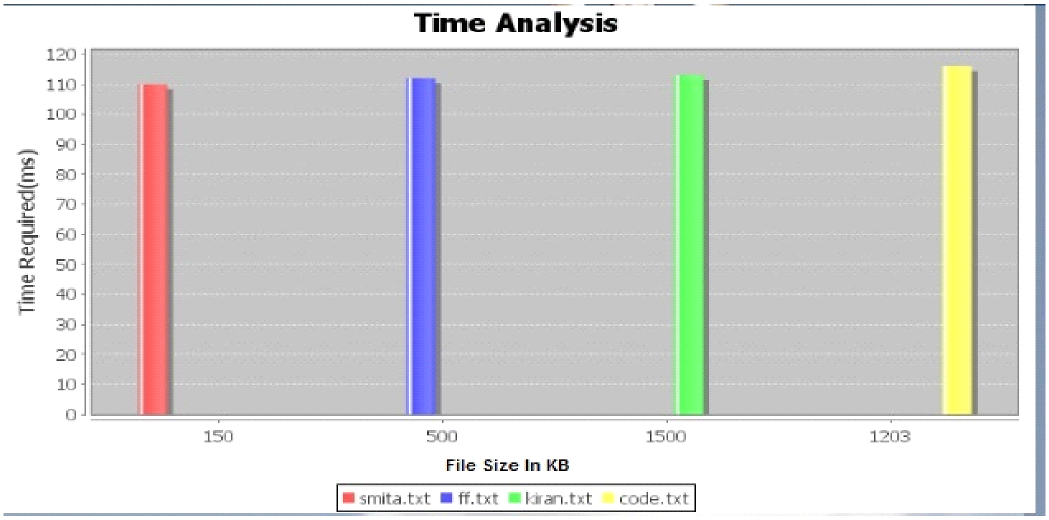


Fig. 6: Experimental Analysis

In the fig. 6 analysis graph shows that to encrypt and partition of our file data does not vary too much with file size. To complete this analysis to perform an execution on different files with different size. In this first file size is very small size till it takes the equal time as the file of size 1500 byte is taken. This time is taken for the operations such as key generation, file encryption, file partition and file upload on the cloud. So analysis result shows that there is no much time variance even if file size increased.

VII. CONCLUSION

In this project, Auditable health records levering DROPS in the cloud. 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. We formally defined security and proved its security without random oracle. The qualitative analysis showed that DROPS is superior to most of the existing systems. Extensive experiments on its performance (on both PC and mobile devices) demonstrated that DROPS 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 Informatics, 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), Vol. 10, 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, Vol.12, 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.

[11] B. Qin, R. H. Deng, S. Liu, S. Ma, Attribute-based encryption with efficient verifiable outsourced decryption, IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1384-1394, JULY. 2015

[12] Spvryans International Journal of Engineering Sciences & Technology (SEST) ISSN : 2394-0905 Design of a Cloud Based Emergency Healthcare Service Model