OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SURVEY ON AUDITABLE HEALTH RECORDS LEVERING DROPS IN CLOUD

Miss. Tejaswi Wani[1], Prof. Bhagyashree Dhakulkar[2]
PG Students Department of Computer Engineering, D. Y. Patil College of Engineering, Lohgaon, Pune-412207, Maharashtra, India[1]
Assistant Professor, Department of Computer Engineering, D. Y. Patil College of Engineering, Lohgaon, Pune-412207, Maharashtra, India[2]

Abstract: **Portable well-being (Mobile-Health) 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 cell phones, and afterward transferring the encoded information to the cloud for storage and access by human services staff and doctors. In any case, proficient and adaptable sharing of encoded information has been an extremely difficult issue. In this project, we propose a Lightweight Sharable and Traceable (LiST) secure versatile wellbeing framework in which tolerant information are scrambled end-to-end from a patients cell phone to information clients. Rundown empowers productive catchphrase hunt and fine-grained get to control of encoded information, underpins following of double crosser's 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 frameworks execution. In this system, DROPS methodology, divide a file into fragments, and replicate 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**

Keywords: Access control, search-able encryption, tractability, user revocation, mobile health system, cloud security, fragmentation, replication, performance, WBSN, HER.

----------∴∴∴----------

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 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. 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 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 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. The file blocks, MAC codes, and version numbers are stored at various levels of the tree. The proposed technique in heavily depends on the users employed scheme for data confidentiality. Moreover, the probable amount of loss in case of data tempering as a result of intrusion or access by other VMs cannot be decreased. Our proposed strategy does not depend on the 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 successful attack on the node. The authors in 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 file and using multiple nodes to store a single file.

II REVIEW OF LITERATURE

TABLE 1: LITERATURE TABLE

Title	Publication Year	Author	Disadvantages
1. Secure Sharing 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 Systems with NTRU	2012	Amruta Shete, S. D. Satav	Does not cover all the aspects and applications
3.A privacy preserving attribute-based authentication System for mobile health networks.	2012	LinkeGuo, Chi Zhang, Jinyuan Sun and Yuguang Fang.	Integrity of the rank order in the search result assuming the cloud server is unstrusted.
4.Scalable and Secure Sharing in Cloud Computing Using Data Manipulation & Encryption	July-2015	Aakanksha Maliye1, Sarita Patil	There is still lacks an efficient And on-demand User revocation Mechanism for BE & DES With the support for dynamic policy updates/ changes, which is essential parts of secure PHR sharing

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 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 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 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. 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

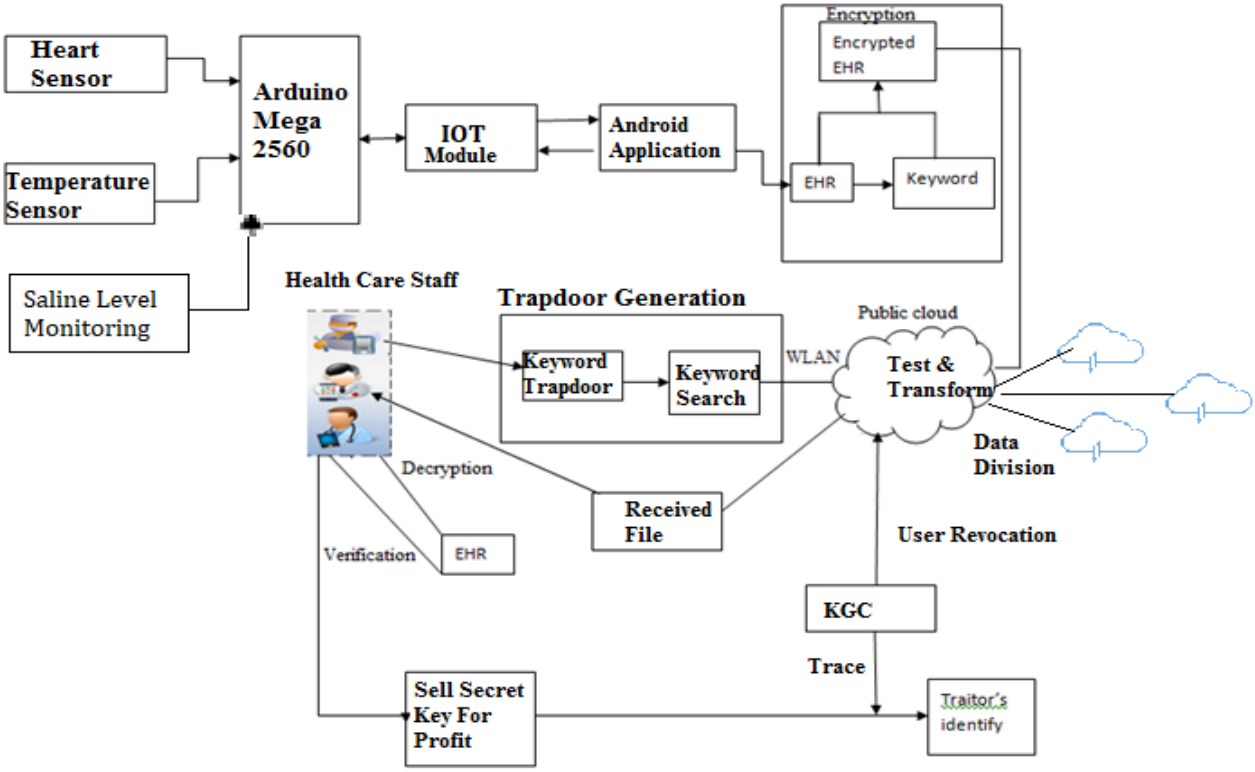

Figure 1. System Architecture

V CONCLUSION

In this project, Auditable health records levering DROPS in 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 the 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 device) demonstrated that DROPS is very promising for practical applications.

REFERENCE

[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.
[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 Health-care Service