ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Privacy and Efficiency On Health Care Data Using Private Proxy Reencryption Scheme

S.Kousalya[1]

Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India[1]

ABSTRACT— The health care services are individual people wants to know medical information where who affected in some disease .The privacy of health care services very difficult in the remote processing. Its avoided by the cloud based technologies provides the privacy on the health care data. The cloud assisted privacy preserving mobile health Monitoring system to provide privacy. Under this system the reencryption scheme to reduce the complexity of the encryption. The CAM has three kinds of design for processing. The final design only using the reencryption scheme. In the reencryption four parties for remote processing such as cloud server, individual clients, semi trust authority, mHealth monitoring system. Here implementing two cryptographic building blocks such as holomorphic encryption, multidimensional range queries on anonymous IBE. In final CAM design using the reencryption scheme to encrypt the all the information into one time and produce the token for the information retrieval on cloud. The above work is well for privacy but here work for the cloud more high on information retrieval. Its should be provide the more difficulties for the each and every user's for information retrieval. Its should be avoid by the new scheme called time management. Its automatically generates the certain time slots for the each user for information retrieval and it attached with the token its increase efficient of information retrieval on cloud.

KEYWORDS—Healthcare, key private proxy reencryption, mobilehealth (mHealth), privacy

I. INTRODUCTION

Wide deployment of mobile devices, such as smartphones equipped with low cost sensors, has alreadyshown great potential in improving the quality of healthcareservices. Remote mobile health monitoring has already been recognized as not only a potential, but also a successful exampleof mobile health (mHealth) applications especially for developingcountries. The Microsoft launched project "MediNet" is designed to realize remote monitoring on the health status of diabetes and cardiovascular diseases in remote areas inCaribbean countries [1]. In such a remote mHealth monitoring system, a client could deploy portable sensors in wireless body sensor networks to collect various physiological data, such as blood pressure (BP), breathing rate (BR), Electrocardiogram (ECG/EKG), peripheral oxygen saturation (SpO) and blood glucose. Such physiological data could then be sent to a centralserver, which could then run various web medical applicationson these data to return timely advice to the client.

These applicationsmay have various functionalities ranging from sleeppattern analyzers, exercises, physical activity assistants, to cardiaanalysis systems, providing various medical consultation[2]. Moreover, as the emerging cloud computing technologiesevolve, a viable solution can be sought by incorporating thesoftware as a service (SaaS) model and pay-as-you-go businessmodel in cloud computing, which would allow small companies (healthcare service providers) to excel in this healthcare market.It has been observed that the adoption of automated decisionsupport algorithms in the cloud-assisted mHealth monitoring has been considered as a future trend [3].

Unfortunately, although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcareservices and potentially reduce healthcare costs, there isa stumbling block in making this technology a reality. Without properly addressing the data management in an mHealth system, clients' privacy maybe severely breached during the collection, storage, diagnosis, communications and computing. A recentstudy shows that 75% Americans consider the privacy oftheir health information important or very important [4]. It hasalso been reported [5]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

that patients' willingness to get involvedin health monitoring program could be severely lowered whenpeople are concernedwith the privacy breach in their voluntarilysubmitted health data. This privacy concern will be exacerbateddue to the growing trend in privacy breaches on electronic healthdata.

II. RELATED WORK

1)Wireless technology in disease management and medicine:

Healthcare information, and to some extent patient management, is progressing toward a wireless digital future. This change is driven partly by a desire to improve the current state of medicine using new technologies, partly by supply and demand economics, and partly by the utility of wireless devices. Wired technology can be cumbersome for patient monitoring and can restrict the behavior of the monitored patients, introducing bias or artifacts. However, wireless technologies, while mitigating some of these issues, have introduced new problems such as data dropout and "information overload" for the clinical team. This review provides an overview of current wireless technology used for patient monitoring and disease management. To identify some of the major related issues and describe some existing and possible solutions. In particularly,the rapid evolving fields of telemedicine and mHealth in the context of increasingly resource constrained healthcare systems.

2)Experimentation with personal identifiable Information:

In this framework, actual personal identifiable information (PII) texts are analyzed to capture different types of PII sensitivities. The sensitivity of PII is one of the most important factors in determining an individual's perception of privacy. A "gradation" of sensitivity of PII can be used in many applications, such as deciding the security level that controls ac- cess to data and developing a measure of trust when self-disclosing PII. This experiments with a theoretical analysis of PII sensitivity, defines its scope, and puts forward possible methodologies of gradation. A technique is proposed that can be used to develop a classification scheme of personal information depending on types of PII. Some PII expresses relationships among persons, some specifies aspects and features of a person, and some describes relation- ships with nonhuman objects. Results suggest that decomposing PII into privacy-based portions helps in factoring out non-PII information and focusing on a proprietor's related information. The results also produce a visual map of the privacy sphere that can be used in approximating the sensitivity of different territories of privacy-related text. Such a map uncovers aspects of the proprietor, the proprietor's relationship to social and physical entities, and the relationships he or she has with others

.

3)Stealthmem : System-level protection against cache-based side channel attacks in the cloud

Cloud services are rapidly gaining adoption due to the promises of cost efficiency, availability, and on-demand scaling. To achieve these promises, cloud providers share physical resources to support multi-tenancy of cloud platforms. However, the possibility of sharing the same hardware with potential attackers makes users reluctant to offload sensitive data into the cloud. Worse yet, researchers have demonstrated side channel attacks via shared memory caches to break full encryption keys of AES, DES, and RSA. Here Stealhmem, a system-level protection mechanism against cache-based side channel attacks in the cloud. Stealhmem manages a set of locked cache lines per corewhich are never evicted from the cache, and efficiently multiplexes them so that each VM can load its own sensitive data into the locked cache lines. Thus, any VM can hide memory access patterns on confidential data from other VMs. Unlike existing state-of-the-art mitigation methods, Stealthmem works with existing commodity hardware and does not require profound changes to application software. We also present a novel idea and prototype for isolating cache lines while fully utilizing memory by exploiting architectural propertiesof set-associative caches. Stealthmem imposes 5.9%of performance overhead on the SPEC 2006 CPU benchmark, and between 2% and 5% overhead on secured AES,DES and Blowfish, requiring only between 3 and 34 lines of code changes from the original implementations.

4) Privacy-preserving tele -monitoring for e-health

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Advances in communication technology have opened a myriad of new possibilities for the remote delivery of healthcare. This new form of service delivery not only contributes to the democratization of healthcare, by reaching far-away populations, but also makes it possible for elderly and chronically-ill patients to have their health monitored while in the comfort of their homes. Despite all of these advantages, however, patients are still resisting the idea of medical tele monitoring. One of the main obstacles facing the adoption of medical telemonitoring, is the concern among patients that their privacy may not be properly protected .By propose a privacy-preserving tele monitoring protocol for healthcare. Our protocol allows patients to selectively disclose their identity information, and guarantees that no health data is sent to the monitoring centre without the patients' prior approval. The approval process can be automated, and requires only an initial configuration by the patient.

III. EXISTING SYSTEM

The previous work providing the high privacy of the health care services. The privacy of health care services very difficult in the remote processing. Its avoided by we using the cloud based technologies provide the privacy on the health care data's. Here we using the cloud assisted privacy preserving mobile health Monitoring system to provide privacy. Under this system we using the reencryption scheme to reduce the complexity of the encryption. The CAM have three kinds of design for processing. The final design only using the re encryption scheme. Here we using the four parties for remote processing such as cloud server, individual clients, semi trust authority, mHealth monitoring system.The existing system is follows the HIPAA (Health Insurance Portability and Accountability Act). the current law is more focused on protection against adversarial intrusions while there is little effort on protecting clients from business collecting private information. Meanwhile, many companies have significant commercial interests in collecting clients' private health data and sharing them with either insurance companies, research institutions or even the government agencies. Its provide the protection of the personal records. It
encrypt the user data's. its takes more time for the information retrieval.

Traditional privacy protection mechanisms by simply removing clients' personal identity information (such as namesor SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of mHealth systems due to the increasing amount and diversity of personal identifiable information [9]. It is worth noting that the collected information from anmHealth monitoring system could contain clients' personal physical data such as their heights, weights,and blood types, or even their ultimate personal identifiable information such as their fingerprints and DNA profiles [10].

According to [11], personal identifiable information (PII) is"any information, recorded or otherwise, relating to an identifiableindividual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical transactional,locational,relational, computational, vocational, or reputational" In other words, the scope of PII might not necessarily be restricted to SSN, name and address, which are generally considered as PII in the traditional sense. Indeed, the state of the art reidentification techniques [12], [13] have shown that any attribute could become personal identifiable information in practice [9].

Moreover, it is also noted that although some attribute may be uniquely identifying on its own, "any attributecan be identifying in combination with others, while no single element is a (quasi)-identifier, any sufficiently large subset uniquely identifies the individual" [12]. The proposed mobile health monitoring scenario provides a good opportunity for adversaries to obtain a large set of medical information, which could potentially lead to identifying an individual user. Indeed, several recent works [14]–[16] have already shown that even seemingly benign medical information such as blood pressure can be used to identify individual users.

Furthermore, it is also observed that future mobile health monitoring and decision support systems might have to deal with other much more privacy-sensitive features such as DNA profiles, from which an adversary may be able to reidentify an individual user. Traditionally, the privacy issue is tackled with anonymization technique such as anonymity or diversity. However, it has been indicated that these techniques might be insufficient to prevent reidentificationattack[9]. The threat of reidentification is so serious that legal communities have already been calling

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

for more sophisticated protectioninstead of merely using anonymization. We believethat our proposed cryptographic based systems could serve as a viable solution to the privacy problems in mHealthsystems,and also as an alternative choice for those privacy-aware users

Drawbacks of Existing System

The privacy of the existing system is less amount only high compare with the another approaches. Its take more time for encrypt the user data's.its takes more time for the information retrieval

IV.PROPOSED SYSTEM

In our proposed work implements the two kinds of the schemes called private proxy re encryption and time management scheme. The private re encryption scheme is used to provides the privacy of information on cloud. The retrieval of the information is only handled by cloud. The cloud also done a proxy re encryption.The individual user's are requesting to cloud with the token. Here problem is work load of the cloud is high compare with the existing system. It should be avoid implements the new time management scheme to provides the separates time slots for the individual user. So that user retrieve the information on cloud by using the certain time slots. The following diagrams shows that the authority to each users.

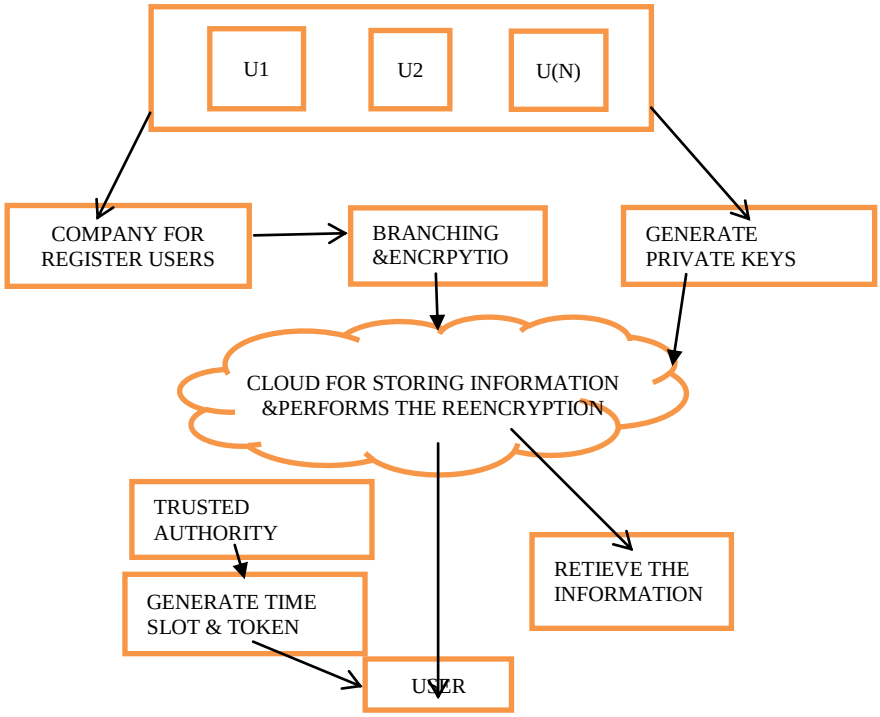

Figure.1. Architecture

Advantages of Proposed System

The privacy of the proposed system is high compare with our existing system.

The cloud assisted privacy preserving system is applicable for cloud environments. using effective cloud systems to provide the privacy. The information retrieval on cloud is high compare with the existing system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The data flow illustrates the following.

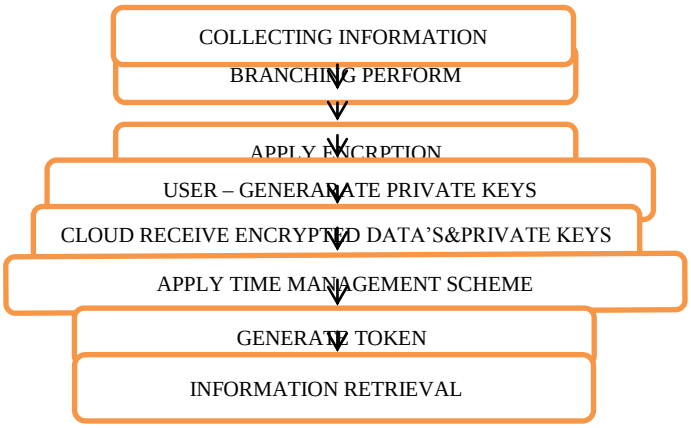

Figure.2.Flow diagram

Required Components

Monitoring System:

The monitoring system is one of the companies for collect the health information about the people. Here it's using the branching programs to collect the information on people. The branching program means its separate information based on tree structure like parent nodes and child nodes. Here its performs the encryption on collected information's.

Client System:

The client system is the user using hand helded systems such as smart phones or laptops. Here using this system to user put the information and retrieve the information from cloud. Its used to get the token from the semi trusted authority. And this token to retrieve the information from the cloud.

Token Generation:

The token is generated by the semi trusted (TA). The tokens are generated by using the private keys and depending upon the user specified information's. Here its using this tokens are partially encrypted and its sends to the cloud. Where the cloud side its again encrypt the token to provide the user specified information's.

Cloud Reterival:

Here we considers the what are the processing in the cloud side. Where here the cloud is a separate place for storing the large amounts of data's.Whereits get the information from the monitoring system and organize the data's.And its receives the token from client and give information depending upon the user specification.

Time Management:

This module we implements the time management scheme to provide the efficient information retrieval on cloud. Here its automatically generates the certain time for the each and every users. Where its attached to the token. This time slots to each and every users retrieve the information on cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V. CONCLUSION AND FUTURE WORKS

To achieve the high privacy on the mobile health care system using the cloud assisted privacy preserving mobile health monitoring system where here implements the three modules such as base cam model, improved cam model and final cam model. That final model is enhancing the high privacy in health care services. Here future enhancement is increase the efficiency of information retrieval on cloud.So provides the token with specified and certain time slots for retrieved information on cloud.

REFERENCES

[1] P. Mohan, D. Marin, S. Sultan, and A. Deen, "Medinet: Personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony," in Proc. 30th Ann. Int. Conf. IEEE Engineeringin Medicine and Biology Society, 2008 (EMBS 2008), 2008,pp. 755–758.

[2] A. Tsanas, M. Little, P. McSharry, and L.Ramig, "Accurate telemonitoringof parkinson's disease progression by noninvasive speech tests,"IEEE Trans. Biomed. Eng., vol. 57, no. 4, pp. 884–893, Apr. 2010.

[3] G. Clifford and D. Clifton, "Wireless technology in disease managementand medicine," Ann. Rev. Medicine, vol. 63, pp. 479–492, 2012.

[4] L. Ponemon Institute, Americans' Opinions on Healthcare Privacy,2010 [Online]. Available: http://tinyurl.com/4atsdlj

[5] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J.vanBeijnum, and P. D.Stefanis, "End-user perception towards pervasive cardiac healthcareservices: Benefits, acceptance, adoption, risks, security, privacy andtrust," in Proc. Pervasive Health, 2011, pp. 478–484.

[6] M. Delgado, "The evolution of health care it: Are current U.S. privacypolicies ready for the clouds?," in Proc. SERVICES, 2011, pp. 371–378.

[7] N. Singer, "When 2 2 equals a privacy question," New
York Times, Oct. 18, 2009 [Online]. Available:http://www.nytimes.com/2009/10/18/business/18stream.html

[8] E. B. Fernandez, "Security in data intensive computing systems,"inHandbook of Data Intensive Computing
NewYork,NY,USA:Springer, 2011, pp. 447–466.

[9] A. Narayanan and V. Shmatikov, "Myths and fallacies of personally identifiable information," Commun.ACM, vol. 53, no. 6, pp. 24–26, 2010.

[10] P. Baldi, R. Baronio, E. D.Cristofaro, P. Gasti, and G.Tsudik, "Countering gattaca: Efficient and secure testing of fully-sequenced human genomes," in Proc. ACM Conf. Computer and Communications Security, 2011, pp. 691–702.

[11] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies:Howto ensure privacy? Build it in: Privacy by design," Identity in the Information Society, vol. 3, no. 2, pp. 363–378,2010.

[12] A. Narayanan and V. Shmatikov, "Robust de anonymization of large sparse datasets," in Proc. IEEE Symp. Security and Privacy, 2008 (SP2008), 2008, pp. 111–125.

[13] A. Narayanan and V. Shmatikov, "De-anonymizing social networks,"in Proc. IEEE Computer Society, IEEE Symp. Security and Privacy,2009, pp. 173–187.

[14] I. Neamatullah,M. Douglass, L. Lehman, A. Reisner,M. Villarroel,W. Long, P. Szolovits, G. Moody, R. Mark, and G. Clifford, "Automated de-identification of free-text medical records," BMC Med. Inform. DecisionMaking, vol. 8, no. 1, p. 32, 2008.

[15] S. Al-Fedaghi and A. Al-Azmi, "Experimentation with personal identifiable information," IntelligentInf.Manage.,vol. 4, no. 4, pp. 123–133,2012.

[16] J. Domingo-Ferrer, "A three-dimensional conceptual framework for database privacy," Secure Data Manage., pp. 193–202, 2007.