ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

PRIVACY-PRESERVING CIPHER TEXT MULTI-SHARING CONTROL FOR MOBILE HEALTH MONITORING SYSTEM

* Seljo Jose**Nijin Jolly Christ the King Engineering College
seljoalapattu@gmail.com, nijinjolly@outlook.com

ABSTRACT- Cloud-assisted mobile health (mHealth) monitoring,which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. The concept of BIG DATA is used here to provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share a cipher text of data among others under some specified conditions. This paper, for the first time, proposes a privacy-preserving cipher text multi-sharing mechanism to achieve its properties which also address this important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. It combines the merits of proxy re-encryption with anonymous technique inwhich a cipher text can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of cipher text senders/recipients. Furthermore, this paper shows that the new primitive is secure against chosen-cipher text attacks in the standard model.

Key Terms: Encryption, Decryption, Privacy-Anonymity,Mobile health (mHealth), Healthcare.

1. INTRODUCTION

Wide deployment of mobile devices, such as smart phones equipped with low cost sensors, has already shown great potential in improving the quality of healthcare services. Remote mobile health monitoring has already been recognized as not only a potential, but also a successful example of mobile health (mHealth) applications especially for develop-ing countries. The Microsoft launched project [Medi Net] is designed to realize remote monitoring on the health status of diabetes and cardiovascular diseases in remote areas.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 (SpO2) and blood glucose. Such physiological data could then be sent to a central server, which could then run various web medical applications on these data to return timely advice to the client. These applications may have various functionalities ranging from sleep pattern analyzers, exercises, physical activity assistants, to cardiac analysis systems, providing various medical consultation. Moreover, as the emerging cloud computing technologies evolve, a viable solution can be sought by incorporating the software as a service (SaaS) model and pay-as-you-go business model 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 decision support algorithms in the cloud-assisted mHealth monitoring has been considered as a future trend.

Unfortunately, although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is a stumbling block in making this technology a reality. Without properly addressing the data management in an mHealth system, clients' privacy may be severely breached during the collection, storage, diagnosis, communications and computing. Security is the most important concern for any type of services like this, which provides storage for data. Due to its efficient data processing capability, cloud play a vital role in keeping big data. Many individuals and organizations can view, modify and update their data stored in the cloud through remote accessing. During remote accessing there is an possibility for some common issues like privacy, security, dataintegrity, dynamic updates etc… every time it is not possible to check the data for consistency, as trillions of individual and organizations data are flooding over the internet. As increase in number of individual users and medical organizations, they choose to upload their data in cloud, force us to keep the data more securable from being hacked. The data of an individual user or patient should be kept confidential and it should be accessed only by the authenticated users. While providing security, the most important aspect to be considered before storing the data is that, the anonymity of the service providers. The services which are used for data storage should provide a high quality encrypted data sharing. These services provides the way that, only the cipher text of the data is shared to the authorized individuals by the data owners under some restricted and specified conditions. The features mentioned above are commonly required to maintain secure processing, and these features are achieved by employing a new technique called cipher text multi sharing mechanism. In this mechanism a proxy re-encryption technique are employed in which only the cipher text to be shared securely and conditionally over multiple times. It also ensures that, original message and information identity of cipher text senders and receivers is not leaked and it also ensures it is not vulnerable to cipher text attacks.

2. BIG DATA

Big data is a concept which is used to describe a huge amount of both structured and unstructured data that is so large. It becomes very difficult to process such data using traditional database models like (DBMS, RDMS) and software methodologies. A most important concern is that, if the volume of data is too big or it moves too fast or it exceeds current processing capacity, then it becomes a risky one.

Big data has the ability to provide, improve operations and it makes process faster, and take more intelligent decisions for the organizations. It gets origin from Web search companies who had the problem of querying very large distributed aggregations of loosely-structured data (XML, XHTML, and web based document).

A. Characteristics:

Big data can be characterized as 3v's

x Volume: big data doesn't sample. It just observes and tracks what happens

x Velocity: big data is often available in real-time

x Variety: big data draws from text, images, audio, video; plus it completes missing pieces through data fusion But, the challenge of keeping those huge amounts of structured and unstructured data leads to the change in 3v's. As a result of increase in number of data sharing devices, it alternates the traditional 3v's definition.

B. Importance of Big Data:

When big data is effectively captured and analyzed efficiently, it can lead to efficiency improvements, increased sales, lower costs, better customer service, and improved products service. Companies are able to gain a more complete understanding of their business, and their customers.

1.Effective use of big data exists in the following areas:

x Using information technology (IT) logs to improve IT troubleshooting and security breach detection, speed, effectiveness, and future occurrence prevention.

x Use of voluminous historical calls centre information more quickly, in order to improve customer interaction and satisfaction.

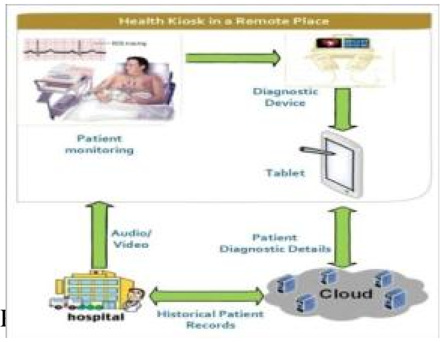
x Use of social media content in order to better and more quickly understand customer sentiment about you/your customers, and improve products, services, and customer interaction.

x Fraud detection and prevention in any industry that processes financial transactions on-line, such as shopping, banking, investing, insurance and health care claims.

x Use of financial market transaction information to more quickly assess risk and take corrective action.

3. SYSTEM MODEL AND ADVERSARIAL MODEL

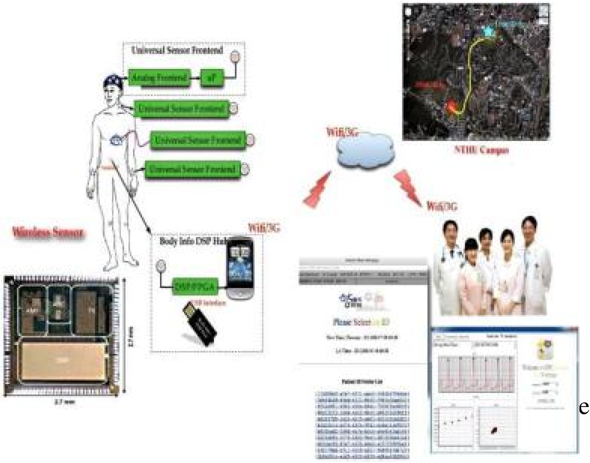
To facilitate our discussion, we first elaborate our cloud-assisted health monitoring system (CAM). CAM consists of four parties: the cloud server (simply the cloud), the company who provides the health monitoring service (i.e., the healthcare service provider), the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device.


Health Kiosk in a Remote Place
Patient monitoring
Diagnostic Device
Tablet
Audio/ Video
Patient Diagnostic Details
hospital
Historical Patient Records
Cloud

A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors. We assume a neutral cloud server, which means it neither colludes with the company nor a client to attack the other side. This is a reasonable model since it would be in the best business interest of the cloud not to be biased. We admit that it remains possible for the cloud to collude with other malicious entities in our CAM, and we leave the CAM design under these stronger models as future work. We also do not assume that an individual client colludes with other clients. Our security model does not consider the possible side-channel attack due to the co-residency on shared resources either because it could be mitigated with either system level protection or leakage resilient cryptography. CAM assumes an honest but curious model, which implies all parties should follow the prescribed actions and cannot be arbitrarily malicious.

In the following, we briefly introduce the four major steps of CAM: Setup, Store, TokenGen and Query. We only illustrate the functionality of these components in this section while leaving the details in later sections.

At the system initialization, TA runs the Setup phase and publishes the system parameters. Then the company first expresses the flow chart of the mHealth monitoring program as a branching program, which is encrypted under the respective directed branching tree. Then the company delivers the resulting cipher text and its company index to the cloud, which corresponds to the Store algorithm in the context.



4.CLOUD COMPUTING

Cloud computing is a technology to access the resources available in the servers through Internet. Cloud computing technology becomes popular in the recent years due to its several advantages over traditional methods,like flexibility, scalability, agility, elasticity, energy efficiency, transparency, and cost saving. Cloud resources are shared resources which can be accessed by any one, anytime and anywhere. It is accessible through any devices like mobile, desktops, laptops, tablets etc… The resources and information are provided for the users based on ondemand services. It allows the users to pay only for the resources and workloads they use. Cloud is nothing but a server and a number of servers interconnected through it. Cloud providers are the one who own large data centers with massive computation and storage capacities. They sell these capacities on-demand to the cloud users who can be software, service, or content providers for the users over the internet. In the recent years the major cloud providers are Google, Microsoft, and Amazon etc...

A. Architects to Be Factor in Cloud computing Designs:

Infrastructure as a Service:

Infrastructure as a Service is a form of cloud computing service which provides virtualized resources which are required over the Internet. Among many services it is an important one because, it provides, server spaces, bandwidth requirement, internet connections, load balancing etc…

Platform as a Service:

Platform as a service is a form of cloud computing services which provides a platform which allows customers to develop, run, and manage their web applications without the necessity of developing and maintaining the infrastructure which is required for developing and launching an application.

Software as a Service:

Software as a Service is a form of cloud computing services which provides the software's in which the developed applications are hosted by the service provider. Further, a service provider gives access for those applications to the customers through Internet by terms of pay per use.

Network as a Service:

Network as a Service is a type of business model which allows us to access the network functionalities directly and securely.

B. Virtualization:

Virtualization is the key concept in sharing the resources. It allows the single instance of resources to share among multiple customers or among different organizations. Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization. Virtual Machines provide an environment that is logically separated from the existing hardware.

C. Big Data in cloud:

Most of the technologies are closely associated with the cloud. The products and platforms mentioned are either entirely cloud-based or have cloud versions themselves. Big Data and cloud computing go hand-in-hand. Cloud computing allows organizations of all sizes to get more value for their data than ever before, by enabling fast analytics at a minute of previous costs. This, in turn drives companies to acquire and store even more data, creating more need for processing power and driving a virtuous circle.

5. SECURITY TECHNIQUE

A. Cryptography:

Cryptography is the study and practice of techniques which is used for storing and retrieving information securely and privately, by protecting the data from third parties. To provide security, it involves the processes of encryption and de-encryption.

It serves wide range of applications such as online banking, ticket reservation, logging in to Facebook, Gmail,Twitter etc… where user personal identities are protected confidentially.

1.1 Terminologies:

x *Encryption:* It is the process of converting the original data into some unreadable form to protect the data while transferring from sender to receiver.

x *Authentication:* It ensures that the message was sent from the sender by verifying sender information associated with the message.

x *Integrity:* It ensures that, information received by the receiver is not modified anywhere during transfer.

B. Types of cryptography:

Secret key cryptography:

It is a type of cryptography which uses a single key for encryption and de-encryption. A key used by the sender for encryption is used by the receiver for de-encryption.

Public key cryptography:

It is a type of cryptography which uses two keys to provide security. In this sender and receiver has a separate private key as a secret key and a public key is shared between them for communication.

Hash function:

It is a type of cryptography which does not involve any key. Instead of using keys, it uses hash values of fixed length. Hash values are calculated depending on the text message.

6. TRADITIONAL METHOD

Traditional Cryptography encryption techniques such as identity based encryption, public key encryption etc… are used to provide security to the data from third party hackers. Christo Ananth et al. [12] discussed about an eye blinking sensor. Nowadays heart attack patients are increasing day by day."Though it is tough to save the heart attack patients, we can increase the statistics of saving the life of patients & the life of others whom they are responsible for. The main design of this project is to track the heart attack of patients who are suffering from any attacks during driving and send them a medical need & thereby to stop the vehicle to ensure that the persons along them are safe from accident. Here, an eye blinking sensor is used to sense the blinking of the eye. spO2 sensor checks the pulse rate of the patient. Both are connected to micro controller.If eye blinking gets stopped then the signal is sent to the controller to make an alarm through the buffer. If spO2 sensor senses a variation in pulse or low oxygen content in blood, it may results in heart failure and therefore the controller stops the motor of the vehicle. Then Tarang F4 transmitter is used to send the vehicle number & the mobile number of the patient to a nearest medical station within 25 km for medical aid. The pulse rate monitored via LCD .The Tarang F4 receiver receives the signal and passes through controller and the number gets displayed in the LCD screen and an alarm is produced through a buzzer as soon the signal is received. Traditional encryption mechanisms are applicable only for small amount of data. If the encrypted data is large, encryption and de-encryption process might be a time consuming and a costlier one.

Drawbacks:

x Encryption and de-encryption process is time consuming and cost effective.

x Security is less.

x Update of cipher text recipient is not possible. x Anonymity is not considered.

A. Anonymity and Multi-Hop (AMH):

To solve these problems a new technique known as AMH-IBCPRE is proposed. It is a unidirectional approach which achieves multiple receiver cipher text updates; consider anonymity, enables conditional data sharing etc…

Anonymity: Anonymous communication is required for the users to send messages to other users without revealing their identities.

Multi-Hop: Receiver can be updated multiple times for a given cipher text.

Proxy Re-encryption (PRE) technique is proposed which allows a semi trusted party known as proxy, which converts an encrypted cipher text of particular key into an encryption of the same message by using another separate key, which leads to decrease the workload of the data owner.

Identity-Based Cryptography (IBC) is a form of public key cryptography in which recipient identities such as email address, id, and name can be used to evaluate a public key.

Identity-based conditional proxy re-encryption (IBCPRE) technique is a form of PRE method. It focuses on two aspects.

1. To extend the proxy re-encryption method to identity-based encryption method.

2. To extend the proxy re-encryption method to support conditional proxy re-encryption method.

Advantages:

x Enable anonymity.

x Multiple receiver update. x Conditional data sharing. x Less workload.

x Free from chosen cipher text attacks (CCA). x Free from collusion attacks.

7. CONCLUSION

In this paper, we design a cloud-assisted privacy preserving mobile health monitoring system, called CAM, which can effectively protect the privacy of clients and the intellectual property of mHealth service providers. This paper have introduced a new mechanism known as Anonymity Multi Hop Identity Based Conditional Proxy Re-Encryption for secure data sharing in cloud computing. To protect the clients privacy, we apply this AMH-IBCPRE technique. This work specially focused on anonymity of the recipient and multiple cipher text of recipient which is required for protecting some sensitive confidential information while transferring the information. This mechanism also ensures consistency and efficiency of data sharing in a time consuming way and in a cheaper way. It is the first time this new mechanism is approached to ensure security against chosen cipher text attack primitives.

8 .FUTURE ENHANCEMENT

The new mechanism proposed in this paper called AMH-IBCPRE has a problem that, it provides security against some of the chosen cipher text attacks because of its unidirectional property. This unidirectional IBCPRE scheme in which a hacker is not able to identify the source properties from the encrypted destination cipher text. To safeguard the information of both sender and the receiver, a new scheme called, Anonymous-PRE (ANOPRE) was developed. This scheme guarantees that the hacker cannot identify the sender of original and re-encrypted cipher text even the re-encryption is provided. This scheme also ensures security from most of the chosen cipher text attacks. Even there are lots of models proposed for providing security, this is the only scheme that achieves all the properties, even it combine some important features of standard models.

9. REFERENCES

[1] G. Ateniese, K. Benson, and S. Hohenberger, 2009 ,"Key-private proxy Re-encryption," in *Topics in Cryptology–CT-RSA* (Lecture Notesin Computer Science), vol. 5473. Berlin, Germany: Springer-Verlag, pp. 279-294.

[2] J. Shao, 2012, "Anonymous ID-based proxy re-encryption," in *Information Security and Privacy* (Lecture Notes in Computer Science), vol. 7372. Berlin, Germany: Springer-Verlag, pp. 364–375.

[3] Sun Microsystems, 2009, "Introduction to Cloud Computing Architecture", Sun Microsystems Inc., white paper, pp. 1-17.

[4] MELL, P. and GRANCE, T, 2009. “Definition of Cloud Computing”, Draft NIST working, vol.5, pp. 7-19.

[5] Magoulas, Roger; Lorica, Ben (February 2009), “Introduction to big data”, vol. *Release 2.0* (Sebastopol CA: O'Reilly Media), pp.1-7.

[6] Bellare, Mihir; Rogaway, Phillip (21 September 2005), “Introduction *to Modern Cryptography*, by random grids, vol.1, pp.10-21.

[7] D.Boneh and X.Boyen, 2007, “Introduction”. “ID secures identity-based encryption”, Berlin, Germany: Springer-Verlag, 2007, vol.3027, pp. 223–238.

[8] C.K.Chu and W, .G.Tzeng (August 2006), “Identity-based proxy re-encryption”, (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, 2006, vol. 4779, pp. 189–202.

[9] 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.” *Conference Proceedings of theInternational Conference of IEEE Engineering in Medicine and Biology Society*, vol. 2008, no. 3, pp. 755–758.[Online]. Available:http://www.ncbi.nlm.nih.gov/pubmed/ 191627 65

[10] A. Tsanas, M. Little, P. McSharry, and L. Ramig, “Accurate telemoni-toring of speech tests,” *Biomedical Engineering, IEEE Transactions on*, vol. 57, no. 4, pp. 884–893, 2010.

[11] G. Clifford and D. Clifton, “Wireless technology in disease management and medicine,” *Annual Review of Medicine*, vol. 63, pp. 479–492, 2012.

[12] Christo Ananth, S.Shafiqa Shalaysha, M.Vaishnavi, J.Sasi Rabiyathul Sabena, A.P.L.Sangeetha, M.Santhi, “Realtime Monitoring Of Cardiac Patients At Distance Using Tarang Communication”, International Journal of Innovative Research in Engineering & Science (IJIRES), Volume 9, Issue 3,September 2014,pp-15-20

[13] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, and P. D. Stefanis, “End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust,” in *PervasiveHealth*, 2011, pp. 478–484.

[14] M. Delgado, “The evolution of health care it: Are current u.s. privacy policies ready for the clouds?” in *SERVICES*, 2011, pp. 371–378.

[15] N. Singer, “When 2+ 2 equals a privacy question,” *New York Times*, 2009.

[16] E. B. Fernandez, “Security in data intensive computing systems,” in *Handbook of Data Intensive Computing*, 2011, pp. 447–466.

[17] A. Narayanan and V. Shmatikov, “Myths and fallacies of personally identifiable information,” *Communications of the ACM*, vol. 53, no. 6,24–26, 2010.P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, “Coun-tering gattaca: efficient and secure testing of fully-sequenced human genomes,” in *ACM Conference on Computer and CommunicationsSecurity*, 2011, pp. 691–702.

[18] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, “Remote home health care technologies: how to ensure privacy? build it in: Privacy by design,” *Identity in the Information Society*, vol. 3, no. 2, pp. 363–378, 2010.

[19] A. Narayanan and V. Shmatikov, “Robust de-anonymization of large sparse datasets,” in *Security and Privacy, 2008. SP 2008. IEEE Symp*