International Journal of Combined Research & Development (IJCRD)
eISSN: 2321-225X;pISSN:2321-2241 Volume: 4; Issue: 7; July -2015

Privacy in Electronic Health Care System Using Public and Private Cloud

[1] T.S.Mamatha, [2] Dr.S.N.Chandrashekara, [3]Dr.K.S.JagadeeshGowda, [4]Bharathi.M

1 Student, Dept. of CS&E, SJCIT, Chikkballapur, email:mamathabecs@yahoo.com

2 Professor and Head, Dept. of CS&E, SJCIT, Chikkballapur, email:SNC_chandra@yahoo.co.in

3 Professor and Head, Dept. of CS&E, SKIT, Bengaluru, email:ksj_20012002@yahoo.co.in

4 Associate professor, Dept. of CS&E, SJCIT, Chikkaballapur

Abstract- Inspired by the security issues, controlling the reception of electronic healthcare frameworks and the wide achievement of cloud administration models, we propose to incorporate protection in electronic health care system with the assistance of the private cloud and public cloud. Our system offers remarkable components including privacy preserving data storage, retrieval, and monitoring and audit ability of users. Proposed system also incorporate the idea of symmetric and asymmetric encryption and decryption techniques with limit marking for giving part based access control based on the role of the users whether he/she is a doctor or patient in both normal and emergency cases. Anytime anywhere accessibly electronic health care system works assume a crucial part in our everyday life. Administrations upheld by cell phones, for example, home care and remote observing, empower patients to hold their living style and reason negligible interference to their every day exercises. Furthermore, it altogether decreases the hospital occupancy, permitting patients with higher need of in-doctor's facility treatment to be admitted.

Keywords-Access control, auditability, ehealth, Privacy, EMT, MIPA, PHR.

1.0 INTRODUCTION:

Better health service provisioning can be provided by having fast access to the health data of the patient so need for 24/7 anywhere accessible electronic healthcare system is required in our daily life. Hospital occupancy can be reduced by using mobile devices services like home care and remote monitoring. Electronic healthcare systems are more popular in today's world. There are many drawbacks of electronic healthcare system, large amount of personal data of patients for medical use is involved in electronic healthcare system and people completely lose control over their personal data once it is in internet. Personal data can be easily hacked by hacker once it is in internet, when others can access the personal data of patients there are so many drawbacks like no employer will be willing to hire a person with some disease and insurance company may not provide the insurance to the person by knowing his health history. So one of the challenge is protecting privacy for health data in cyberspace is very difficult. So there is a need for development of feasible set of rules, architecture and system that provides high and security to protect the health data access from unauthorized users.

Using cloud based architecture we can save the total claims, capture and control of the company's that is by outsourcing the computation to the cloud. Using cloud infrastructure we can save the cost of buying and maintain the servers needed for health data management. The proposed hybrid cloud architecture model is stimulated by power, cost, flexibility, convenience, efficiency of cloud based computations outsourcing technique.

Outsourcing data storage and computational tasks becomes a popular trend as we enter the cloud computing era. A wildly successful story is that the company's total claims capture and control (TC3) which provides claim management solutions for healthcare payers such as Medicare payers, insurance companies, municipalities, and self-insured employer health plans. TC3 has been using Amazon's EC2 cloud to process the data their clients send in (tens of millions of claims daily) which contain sensitive health information. Outsourcing the computation to the cloud saves TC3 from buying and maintaining servers, and allows TC3 to take advantage of Amazon's expertise to process and

analyze data faster and more efficiently. The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm.

In this paper we have private cloud that is a cloud owned by a single party, this is treated as a service offered to the users. In this model by making use of infrastructure of the public cloud from public cloud providers the private cloud provider provide software as a service to the users.

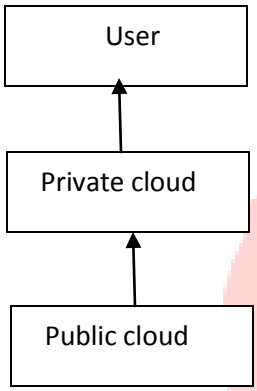

Fig 1: Public and Private Cloud Service Model

2.0 RELATED WORK:

2.1 Android Enabled Mobile Cloud Framework Development Of Electronic Healthcare Monitoring System:

In [1] traditional healthcare system healthcare professionals, hospital and insurance agencies maintain paper based record so in those days there is no privacy for the health information of the patients. Later the traditional healthcare system depends on the centralized server which is unreliable and insecure. Considering these issues in mind there are so many existing systems to provide privacy for the health information stored on the internet. Let us consider the some of the system first system is "android enabled mobile cloud framework development of electronic healthcare system" focus is to reduce health care differences and ensure adequate security and privacy. To address these issues cloud computing concept used in electronic healthcare system. One of the important operating system android is used as a client application which mainly focus on availability of health information on 24/7 basis and invisibility of computing mobile applications.

Open source cloud computing technologies provides this application to build secure electronic healthcare system to build secure electronic healthcare system using virtual private networks. By making use of VPN technology in public networks in cloud infrastructure we can ensure security to protect the personal health data. So this system is using android enabled healthcare system, cloud server and virtual private network to provide privacy for the health data stored in the cloud. This system is based on android open source, which has advantages like fast retrieval and cost effective. Disadvantage of this system is might be improve security and implementing user authentication techniques for both patients and administrator. Medical billing insurance claims can be included to the existing system as future enhancement that will eliminate spurious claims. This system is only designed for the concept of virtual private network in cloud infrastructure.

2.2 A Cryptographic Key Management Solution For Health Information Privacy Preserving And Accounting Regulation:

Here [2] they present management of key to provide privacy regulations. This system has some roles like:

(i)A trusted server of government healthcare office
(ii)A server of healthcare service provider
(iii)Patients

In this system there will be a certification authority which acts as the agent between the patient and healthcare service provider. First patient has to get request the certification authority for smart card so that he or she can get services from healthcare providers. Again there are drawbacks in this system is trusted server ids able to access the health data at any time which could be a privacy threat.

2.3 Cryptography Based Secure Electronic Health Record For Patient Privacy And Emergency Healthcare:

There [3] are three important components in this system:

(i) P-device
(ii) S-server
(iii) A-server

Patient interacts with his family and Patient-device to assign privilege that will be used for retrieving the patient's personal health information. S-server interacts with all the entities in patient local area network for personal health data retrieval. Authentication-server is used for authenticating doctor and inform P-device regarding doctor authentication. The disadvantage of this system is the backup mechanism used for emergency access relies on someone or something whose availability cannot be guarantee at all the times.

2.4 Secured Patient Healthcare Monitoring In Cloud Infrastructure:

Protecting integrity [4][5] of data in cloud assisted privacy preserving health monitoring. Using low cost sensors in mobile devices we can lower the cost of the service provider. Cloud assisted service model consists of 4 parties they are:

(i) Cloud server
(ii) Healthcare service provider
(iii) Client
(iv) Trusted Authority

Cloud server acts as offline storage. All data are saves in encrypted format even the passwords of users. Ages, gender, emails of the users are not encrypted. Mobile Healthcare service provider stores data on the cloud in encrypted format.helathcare provider provides username and password. Using that username and password user (patient) can add medical data onto the cloud. Semi trusted authority activate user account of multiple users. Semi trusted authority generates token for user. Clients register with mobile healthcare service provider. The future improvement of this system is on client privacy using outsourcing decryption technique, improvement in bilinear pairing, encryption, identity based encryption, decryption outsourcing, re-encryption.

2.5 Body Sensor Network Security:

In this paper [6] on person's body network of sensors is deployed for health information monitoring. Sensors deployed on the person's body collects the health information of the patient. Security and privacy are the important factors in a body sensor networks. This system is a new way to provide quality health care to patients. Sensors deployed on the person's body collect physiological information and collected data is readily available in the event of emergency. Disadvantage in this system is sensors can be lost or stolen, data stored on the third party storage site we cannot trust the storage site with health data of the patient.

2.6 Existing System Disadvantages:

- Difficult for Long Term Medication. Several Kinds of Medicine Diagnosing, Frustration of missing Doses.
- Manual Insurance Climbing Patients could actually control the sharing of their sensitive PHI, especially when they are stored on a third-party server which people may not fully trust.
- Because a third-party server inside hackers can able to leak the patient's information and security records to other peoples so this scheme is not fully trust.
- The ABE important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date.

3.0 PROPOSED SCHEME:

All the above system which we discussed till now have the disadvantages one common disadvantage we are facing in every system is privacy for health data which can be overcome in our proposed paper, in this paper we are using identity based encryption for role based cryptographic access control. That is based on the role we are giving the access to the health information stored on the cloud. Whether the person is emergency medical technician or patient (owner) based on his or her role access will be given. Among the previous efforts for the privacy on the electronic health care system, medical information privacy assurance showed the importance of privacy for the medical information. Privacy providing infrastructure and technologies for health information system is first developed by MIPA .in the proposed system patients encrypts their own data and store it on the third party server. We use symmetric encryption to encrypt the health data and keyword to search the file stored in the cloud that is called keyword search where keyword is also encrypted. There are three modules mobile, private cloud, public cloud.

Following are key features of proposed system:

- The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the Cloud-based data/computation outsourcing paradigm.
- We introduce the private cloud which can be considered as a service offered to mobile users.
- The result indicates that the proposed scheme is efficient as well as scalable.
- Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud.
- The cloud-assisted service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks.
- Our proposed pattern hiding scheme just slightly increases the computation and storage costs at the public cloud compared to the most efficient construction.

The main entities involved in our system are depicted in Fig. 2. Users collect their health data through the monitoring devices worn or carried, e.g., electrocardiogram sensors and health tracking patches. Emergency medical technician (EMT) is a physician who performs emergency treatment. By user and EMT, we refer to the person and the associated computing facilities. The computing facilities are mainly mobile devices carried around such as Smartphone, tablet, or personal digital assistant.

Each user is associated with one private cloud. Multiple private clouds are supported on the same physical server. Private clouds are always online and available to handle health data on behalf of the users. This can be very desirable in situations like medical emergencies.

The private cloud will process the data to add security protection before it is stored on the public cloud. Public cloud is the cloud infrastructure owned by the cloud providers such as Amazon and Google which offers massive storage and rich computational resource.

We assume that at the bootstrap phase, there is a secure channel between the user and his/her private cloud, e.g., secure home Wi-Fi network, to negotiate a long-term shared-key. After the bootstrap phase, the user will send health data over insecure network to the private cloud residing via the Internet backbone.

Fig 2: Hybrid Cloud Mobile Health Network

Encryption and Decryption algorithm used here is asymmetric RSA algorithm.

RSA algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of a integer is hard (the factoring problem). RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.

Encryption and decryption are of the following form:
Encryption C= Md (mod n)
Decryption M= Cd (mod n)

The public key is made of n and e that is public key KU= {e, n} which known to everyone.

The private key is made of d and n that is private key KR= {d, n} which must be kept secret.

Encrypting messages

Message is encrypted at the sender side using public key which can be decrypted at the receiver using private key. Message before encryption is called plain text after encryption it is called cipher text.

Plain text message is represented as M (M<n)

Cipher text can be calculated using the relation C= Md (mod n)

Decrypting messages

Once message is received at receiver side (cipher text message) it has to be converted to its original form so that receiver will understand. To decrypt the message to original form private key is required at the receiver side.

Cipher text message represented as C

Plain text can be retrieved from the cipher text using the relation M= Cd (mod n)

Threshold signing between the private cloud and emergency medical technician is done using Diffie - Hellman key exchange algorithm. Threshold signing is a two step process between EMT and cloud to access health data.

The first published public key algorithm appeared in the seminal paper by Diffie and Hellman that defined public key cryptography and is generally referred as Diffie- Hellman key exchange. The purpose of this algorithm is to enable two users to exchange secret key securely that can be used for subsequent encryption of messages. This algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

3.1 Proposed System Advantages:

We provide a thorough analysis of the complexity and scalability of our proposed secure PHR sharing solution, in terms of multiple metrics in computation, communication, storage and key management.

Data Confidentiality and On-Demand Revocation. Write Access Control and Scalability and Usability.

We proposed to build privacy into mobile health systems with the help of the private cloud.

We provided a solution for privacy-preserving data storage by integrating a private and public cloud based key management for unlink ability.

4.0 SECURITY REQUIREMENTS:

In this paper, we strive to meet the following main security requirements for practical privacy-preserving mobile healthcare systems.

1) *Storage Privacy:* Storage on the public cloud is subject to five privacy requirements.

   a) *Data confidentiality:* unauthorized parties (e.g., public cloud and outside attackers) should not learn the content of the stored data.

   b) Anonymity: no particular user can be associated with the storage and retrieval process, i.e., these processes should be anonymous.

   c) Unlinkability: unauthorized parties should not be able to link multiple data files to profile a user. It indicates that the file identifiers should appear random and leak no useful information.

   d) Keyword privacy: the keyword used for search should remain confidential because it may contain sensitive information, which will prevent the public cloud from searching for the desired data files.

   e) Search pattern privacy: whether the searches were for the same keyword or not, and the access pattern, i.e., the set of documents that contain a keyword [15], should not be revealed. This requirement is the most challenging and none of the existing efficient SSE [14]–[17] can satisfy it. It represents stronger privacy which is particularly needed for highly sensitive applications like health data networks.

2) *Audit ability:* In emergency data access, the users may be physically unable to grant data access or without the perfect knowledge to decide if the data requester is a legitimate EMT. We require authorization to be fine-grained and authorized

parties' access activities to leave cryptographic evidence.

5. 0 CONCLUSION

In this paper, we proposed to incorporate protection in mobile health care system with the assistance of the private cloud. We gave a solution for security saving information by utilizing symmetric key encryption and utilizing arbitrary string as key to store and recover health information to and from public cloud. here we are also given solution to which provides access for health data stored on the cloud in both normal and emergency cases. proposed system provides audit ability of the user to prevent unauthorized access of health data.

REFERENCES:

[1] R.parameshwari, Dr.N.Prabakaran "An Android enabled mobile cloud framework development of electronic healthcare monitoring system". International journal of advanced research in computer science volume 1, issue 7, December 2013.

[2] Wei-Bin Lee and Chien-Ding Lee, "A Cryptographic Key Management Solution for HIPPA Privacy/Security Regulations", IEEE, volume 12, number 1, January 2008.

[3] Jinyuan Sun , Xiaoyan Zhu , Chi Zhang , and Yuguang Fang "HCCP: Cryptography Based Secure HER for Patient Privacy and Emergency Healthcare" 2011 31st international conference on distributed computing systems.

[4] Vaishnavi B and Yogeshwari R, "A Secured Patient Healthcare Monitoring in Cloud Infrastructure", International Journal, volume 2 issue 1, January 2014.

[5] Shantanu Shankar Pawar and R.N. Phursule, "Protect Integrity of Data in Cloud Assisted Privacy Preserving Mobile Health Monitoring", International Journal, volume 4, number 13(2014).

[6] Chiu c tan and Haodong Wang "Body Sensor Network Security: An Identity –Based Cryptography approach" March 2008.

[7] Huang Lin, Jun Shao, Chi Zhang, Yuguang Fang and Fellow, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring".

[8] Giuseppe Ateniese , Reza Curttmola , Breno de Medeiros "Medical Information Privacy Assurance : Cryptographic and System Aspects" February 2003.

[9] Marco Casassa Mont, Pete Bramhall and Keith Harrison, "A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care" Yue Tong, Jinyuan Sun, Sherman S.M. Chow and Pan Li "Cloud-Assisted Mobile-access of Health Data With Privacy and Auditability", IEEE paper vol 18, no 2, march 2014

[10] George Hsieh and Rong-Jaye Chen "Design for a secure interoperable cloud-based Personal Health Record service" 2012 IEEE 4th International Conference on Cloud Computing Technology and Science.

[11] Kirill Belyaev, Indrakshi Ray, Indrajit Ray, and Gary Luckasen "Personal health record storage on privacy preserving green clouds" 9th IEEE international conference on collaborative computing.

[12] G.Logeswari, D.Sangeetha, V.Vaidehi "A cost effective clustering based anonymization approach for storing PHR's in cloud" 2014 International Conference on Recent Trends in Information Technology.

[13] Assad Abbas and Samee U. Khan, Senior Member, IEEE "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds" IEEE journal of biomedical and health informatics, vol. 18, no. 4, July 2014.