SECURITY MODELS IN HEALTHCARE CLOUD COMPUTING : A REVIEW

[1]J.Leelavathy, [2]Dr.S.selvabrunda
[1]Research Scholar, [2]Professor & Head
[1]Bharathiar University, Coimbatore.
[2] Department of Computer Science and Engineering,
Cheran college of Engineering, Karur.

Abstract: Cloud Computing is an emerging technology, where the reality is acquiring more sense and computing power is very low. This makes cloud computing more popular among entrepreneurs, especially medium size organizations. Cloud computing is a set of services which are provided to a client over a internet on usage basis and pay as per usage where the network has the ability to balance their service requirements. The information available in cloud can be shared without space constraint. The progressed technologies in cloud environment have diverse areas which includes healthcare environment. The demand of delivering a quality medical service has increased comparatively between the health care oriented service providers. This healthcare data is considered as very sensitive as well as confidential which can accessed by the authorized persons who have privileges to access and modify the records. The importance of security and privacy to Electronic Health Record (EHR) is gaining importance for accessing over Internet. The paper mainly emphasize on the needs of cloud computing in healthcare sector and the review of certain security measures adopted for maintaining EHR and that private data can be preserved for future use.

IndexTerms **- Cloud computing, Healthcare security, EHR, Security models**

Introduction

Cloud computing is a technology which uses a set of resources and services and maintains data in central server offered through the Internet. The data and other applications can be maintained without any installation of new hardware or software which are maintained by cloud vendors (Third parties). The rapid growth in cloud computing and the development of medical field supports the doctors and patients to maintain the EHR in a centralized location which benefits the global access, storage management and increases the business flexibility of healthcare service providers.

Data security plays a vital role when the data is stored in some location without any direct intervention of the user under a third party control. Moved medical data and private information can be accessed in a wide range of devices from various locations using various cloud architectures. The primary issue is transferring the data to centralized server or an outsourced third party cloud vendor without changes or hacker's intrusion.. The data can be secured when using some encryption methods on EHR and the security measures and parameters provided by the vendors should be clearly defined well in advance makes the data reliable and the confidentiality can be maintained.

NEED FOR CLOUD COMPUTING IN HEALTHCARE SERVICES

Cloud technology is used to create network between patients, doctors, and healthcare service providers by providing storage space, applications and services on a different environment. The patient records can be maintained centrally provides improved delivery of health services and medical processes. The cost of enrolling a new patient and the claims processing and patient management becomes uncomplicated. The data can be shared with enhanced security and authorized access of information using point-of-care service delivery by using mobile devices through internet for collaboration and sharing of data. The risk of data loss is too low where the centralized data is not only maintained in single location. The redundancy check and disaster recovery is provided as an in-built feature provided by the vendor. The agility of information in medical field helps the doctor in time.[1]

RELATED WORKS

Authenticating Identity

Web based systems provides access to the stored data from anywhere at any time using any secured devices by an authenticated user using registered username and encrypted key password. The key is built directly by two-factor authentication and trusted device access. The transaction should be verified and protected from the malware and intruders.

Data classification

The data classification is done based on the sensitive level of confidential patient record. More importance is given to higher confidential data. Various cryptographic and hashing techniques can be used. The digital signatures can be proposed as a next step of authentication. This cryptanalysis increases the security factor of EHR.[2]

Encryption and Decryption

Two-layer protection can be given for the input data. The captured images and text files are encrypted and the second layer divides the encrypted files into n number of files and stored in cloud. The original data can be decrypted only when the n files are merged correctly by using certain algorithms. The generation of sequence key is used for encryption and decryption of cipher text. The decryption can be done with the help of private key to the registered doctor and authorized persons.[3]

Existing algorithms for cloud security

The security can be provided to cloud as a service by using certain algorithms. Some of the algorithms are Data Encryption standard(DES), Advanced Encryption algorithm (AES), Triple DES are considered as symmetric algorithm where the encryption can be done by single key. Algorithms like RSA, Diffie-Hellman Key Exchange and Homomorphic equations are asymmetric where encryption and decryption can be done by using two different keys. The enhancement in these algorithms makes the cloud service as more reliable.[4]

User Authentication using keystroke dynamics

The typing rhythm of user is measured as behavioral biometric. The dwell time and flight time are measured to identify the user real user and fake user. Multilayer perceptron network and radial basis function network are used for receiving input and performing classification. New users are registered and the authenticated users are verified by the previously stored data. Multilevel of security can be obtained without much cost for hardware.[5]

EHR Secure integration model

The authenticity and integrity of EHR is verified by the authenticated person by attaching legitimate digital signatures. The data formats from these models are integrated and the encryption carried out by ensuring the data without loss and without changes. Attribute-based composite model and Role-based composite model has been proposed for maintaining authentication and access control. Logical division of components into sub-components such that fine-grained authorization can be done by individually labeling each subcomponent without affecting its properties of privacy sensitivity, intended purpose, and object type as well as the authorization policies and the limitation for changing or extending the content can be checked.[6]

Security Models

The data security and system security can be achieved by using different level of security phases. The sensor data are collected and migrated for secure transmission. The level of confidentiality and access control were ensured. The Integrity can be checked by various secure hash algorithms. [7] The availability can be enrolled by taking the multiple copies of migrated data, so that single point loss could be retained by the copies from other locations. When heterogeneous network integrates, the network security becomes indispensible. The network can be safe guarded from local security threats, global security threats and network vulnerabilities can be avoided by using attack graph method. The graph method defend against various known attacks when used with the available tools in market.[8]

CONCLUSION

As healthcare organizations give the impression of being secured in integrating their collected EHR information and adopt to the new business structures in the cloud. New demanding technologies are keep on emerging to make hardware-enhanced security technologies and software solutions that protect privacy, identities of individuals, migrated data, and infrastructure in the cloud. These advancements in this field will further boost the confidence and accuracy of information in the healthcare cloud and availability of data by providing progressively more robust methodologies to enable automation of healthcare cloud environment as well as for the service providers to better manage, monitor, and enforce security policies to meet compliance requirements. The focus on cloud computing is gradually increasing due to less cost and less implementation of hardware and software. Thus the various security algorithms and security models are analyzed for privacy issues and the management of EHRs in a strong way.

REFERENCES

[1] Sushma S.A, Priyadarshini D.Kalewad, " Survey on Cloud Computing In Health Care Systems", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume - 3 Issue – 8,2014 Page No. 7841-7845

[2] Rizwana Shaikh , Jagrutee Banda, Pragna Bandi, "Securing E-healthcare records on Cloud Using Relevant data classification and Encryption", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 6 Issue 2, 2017, Page No. 20215-20220

[3] Intel IT centre, "Healthcare Data Security in Cloud Computing" 2013

[4] G. Rathi, Abinaya. M, Deepika. M¸ Kavyasri. T, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, 2015

[5] T.Ramaporkalai , "Security Algorithms in Cloud Computing", International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Apr 2017

[6] Manpreet Kaur, Rajinder Singh Virk, " Security System Based on User Authentication Using Keystroke Dynamics", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, 2013

[7] Rui Zhang and Ling Liu, "Security Models and Requirements for Healthcare Application Clouds" pdfs.semanticscholar.org

[8] Sayantani Saha, Rounak Das, Suman Datta, Sarmistha Neogy, "A Cloud Security Framework for a Data Centric WSN Application

[9] Mrs. D. Shanmugapriya, Dr. G. Padmavathi, "A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges", International Journal of Computer Science and Information Security,Vol. 5, No. 1, 2009