RESEARCH PAPER | Computer Science | Volume : 5 | Issue : 8 | August 2015 | ISSN - 2249-555X

Secure Key Management for Personal Health Records Using Proxy Server

KEYWORDS: key management, cloud, proxy server

M.Inthumathi
M.Phil Scholar, Department of Computer Science and Engineering,Alagappa University,karaikudi,TamilNadu.

T.Meyyappan
Professor, Department of Computer Science and Engineering, Alagappa University, Karaikudi,TamilNadu.

ABSTRACT *In the emerging patient-centric model of health data is exchange. The Data owner allows a partial control to the proxy server for their medical records and to share health data to their users and emergency staff. This is often outsourced to be stored at a third party, such as cloud provider. It is stimulating to have convenient Personal health record services for everyone. There are more security and privacy risks which could obstruct its broad adoption. In the proposed system, introduce a Proxy Server where maintain the key management based on IBE. And with the data owner support to perform a secure key access in the Proxy server by One Time Password (OTP) Verification. It is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. Further, Data owner always retain the right to, not only permit, but also revoke access privileges through the OTP.*

I. INTRODUCTION

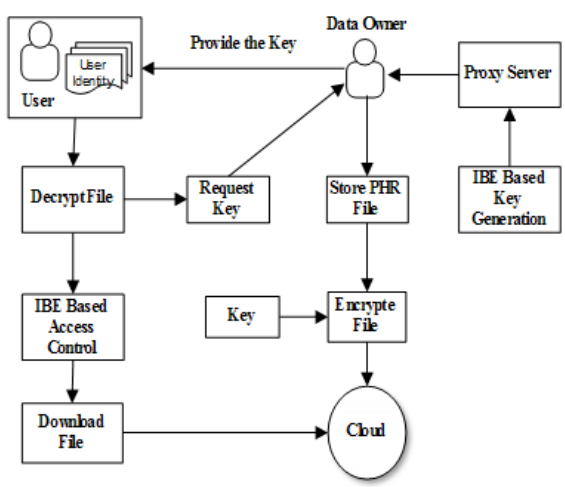
The Personal health record securely shared in cloud there are contain a several issues such as risks of privacy exposure, scalability in key management[1], supple access and proficient user revocation, have been remained the most important challenges toward achieving fine-grained, cryptographically imposed data access control. Healthcare regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not enclosed entities. The high value of the sensitive PHI [10], the third party storage servers are often the targets of various malicious behaviours which may lead to exposure of the PHI. There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

A PHR file should only be available to the users who are given the corresponding decryption key, while stay on confidential to the rest of users. Furthermore, the patient always retains the right to not only grant, but also invalidate access privileges when they feel it is necessary. Each user obtain keys from every owner whose PHR wants to

read would limit the accessibility. A proxy server is employ the key management on behalf of all PHR owners, but this requires too much trust on an authority (i.e., cause the key escrow problem).

The patient-centric [4], secure sharing of PHRs stored on semi-trusted servers, focus on addressing the complicated and challenging key management issues. The complexities of encryption, key generation, and decryption are only linear with the number of attributes involved .However, to integrate IBE into a large-scale PHR system. The verifier is attribute based to verifies the integrity of user data and verifying a data using user location and port number. In an emergency access is to verifying user detail or staff detail used to get the data authentically.

II. SYSTEM MODEL



III. PREVIOUS WORK

Some early works on cryptosystem [1], cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Those demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption [3]. In a PHR multi owner [4] for each patient, the PHR data encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys [1], it is important to reduce the key distribution complexity in such multi-owner settings. In a secure e-health [6] present a security architecture for establishing privacy domains in e-health infrastructures and provides client platform security and appropriately combines this with network security concepts. The APkS [7] are key functionalities of a service such as keyword searches by multiple users become especially challenging with PHRs stored in encrypted form. Basically, users' queries be performed in a privacy preserving way that hides both the keywords in the queries and documents. Shared searchable encrypted data [9] an encryption scheme where each

Volume : 5 | Issue : 8 | August 2015 | ISSN - 2249-555X

authorized user in the system has own keys to encrypt and decrypt data. The scheme supports keyword search which enables the server to return only the encrypted data that satisfies an encrypted query without decrypting it.

IV. PROPOSED WORK

Storing the data in cloud environment becomes natural and also essential. But, security becomes one of the major concerns for all entities in cloud services .In the propose system, introduce a Proxy Server where maintain the key management based on IBE. And with the data owner support to perform a secure key access in the Proxy server by One Time Password (OTP) Verification. It is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. Further, Data owner always retain the precise to not only grant, but also repeal access privileges through the OTP.

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. They require authorization to be fine-grained [5] and authorized parties' access activities to leave cryptographic evidence. The cloud server sends the auditing proof, in the response of that which contains possession of shared data. Than by verifying the correctness of the auditing proof, verifier checks the correctness of the data. There is immediate remediation should be performed upon detection of anomalies.

A. IDENTITY BASED ACCESS POLICY METHODOLOGY

Public-key cryptography offers very strong protection for electronic communications. A large amount of its strength comes from the use of paired keys, which are separate codes that encrypt and decrypt a message; one key is public and one is known only to the recipient.

Identity-based systems allow any party to generate a public key from a User identity value. A trusted third party, called the Private Key Generator (PKG), generates the equivalent private key. To get a corresponding private key, the authorized person to use the identity ID exchanges the PKG, which uses the master private key to generate the private key for identity ID.

Proxy server may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is exceedingly useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical fetters. However, to decrypt messages, the authorized user must get the appropriate private key from the Proxy server.

A sender might specify an expiration date for a message. Appends this timestamp to the actual recipient's identity .Data owner send the health information to proxy server .This generates a key and maintains the encrypted data. Generally, embedding data in the ID corresponds to opening an additional channel between sender and PKG with authenticity guaranteed through the dependency of the private key on the identifier.

B. DATA CONFIDENTIALITY METHODOLOGY

The owners upload IBE-encrypted from Proxy server for the PHR files to the server. Each owner PHR file is encrypted under a certain fine grained and role-based access policy for users from the public or private domain to access, and under a selected set of data Identity that allows access and the OTP (One Time Password) to access the User in the PHR. Only allowed users can decrypt the PHR files Using IBE.

The data owner support to perform a secure key access in the Proxy server by One Time Password (OTP) Verification. It is essential to fine-grained [5] data access control mechanisms that work with semi-trusted servers.

V. Simulation/Experimental Results

In this method is used to get the particular medical data efficiently and quickly. This method is privacy for protecting information. The searching process is very securely processed for hiding data.

FIGURE 1

The figure (1) illustrates a proxy server checks the data owner id and client id. And then generate the one time password using hex digit. In this password send to user for verifying authorised user.

FIGURE 2

The figure (2) illustrates a user receive an otp and send to cloud server. It check

Password and give the data in an encrypted format. For a decryption process user get a secret key view the record.

FIGURE 3

The figure (3) illustrates, the information are encrypted format give a recipient public key and user secret key to decrypt the data and view the detail.

VI.CONCLUSION

In this paper, proposed the privacy for user data and health service providers. The medical care information of user also in emergency cases using Identity based authen-

Volume : 5 | Issue : 8 | August 2015 | ISSN - 2249-555X

tication scheme to avail the information at anytime and anywhere .This system also provide privacy by mean of secure function.

REFERENCE

[1] C.-K. Chu, S. S. M. Chow, W.-G.Tzeng, J. Zhou, and R. H. Deng, "Keyaggregate cryptosystem for scalable data sharing in cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 99, no.PrePrints, p. 1, (2013). | | [2]. J. Sun, X. Zhu, C. Zhang, andY. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEEInt. Conf. Distrib. Comput. Syst., Jun.(2011), pp. 373–382. | | [3].Vipul Goyal, Omkant Pandey,Amit Sahai, Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data"in Proc.13th ACM.Conf.Comput and Commu. secu.,pp 89-98,oct 2006 | | [4].Ming Li, Shucheng Yu, Kui Ren, and Wenjing Lou"Securing Personal Health Records in Cloud Computing: Patient- centric and Fine-grained Data Access Control in Multi-owner Settings"proc.security and privacy.in commu.netw.,Volume 50, 2010, pp 89-106 | | [5].Shucheng_Yu, CongWang,KuiRen and Wenjing Lou "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing",pub.INFOCOM,Proc. IEEEMar 2010,pp 1-9. | | [6].Hons Lohr,Ahmad-Reza Sadeghi,Marcel Winandy,"Securing the E-Health Cloud",Proc. ACM Int .health .informatics .symposium,pp 220-229 | | [7].Ming Li,Shucheng Yu,Ning Cao,Wenjing Lou,"Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing",proc.Int.conf on distrib.comp.sys.pp 383-392,(2011). | | [8]. Melissa Chase Sherman S.M. Chow"Improving Privacy and Security in Multi-AuthorityAttribute-Based Encryption",proc.ACM conf.on compu.and commun.secu.,pp 121-130,(2009). | | [9].Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,by Josh Benaloh , Melissa Chase , Eric Horvitz , Kristin Lauter,proc. ACM workshop on cloud compu.secu.,pp 103-114 ,(2009) | | [10].Barua, M. ,Xiaohui Liang , Rongxing Lu , Xuemin Shen "PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care | ystem",,proc.IEEE Conf.,pp 970-975,(2011)