International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 9, Issue 5, May 2020||

Secure Report Sharing Platform for Healthcare System

Snehal Pandharpatte[1], Shubham Jadhao[2], Suraj Shelkikar[3], Prof. B.C.Julme[4]

BE Students, Department of Computer Engineering, Pune Vidyarthi Grih's College of Engineering & Technology, Pune, Maharashtra, India[1,2,3]

Professor, Department of Computer Engineering, Pune Vidyarthi Grih's College of Engineering & Technology, Pune, Maharashtra, India[4]

ABSTRACT: Cloud computing comes with higher potential in improving the healthcare services provided to patients and also promises increase in the access of qualitative healthcare services and reduction in the healthcare expenses. Even though cloud computing puts an end to the concerns regarding investment in hardware infrastructure and its maintenance by hospitals, expenses by patients and faster access of health records by both patients and doctors without interruption in service, it is still discerned as unsafe because of the security threats it faces. The patient's health information is prone to loss, unauthorized access, misuse, coercing and altering. This can be avoided by encrypting the data before handing it over for cloud storage. This paper comprises the study of various encryption schemes which can be put to use for securing the patient's sensitive health information on cloud along with the implementation and performance analysis of a mobile healthcare application which encrypts the health records of patients before outsourcing it for storage over cloud and ensures effective access control, secrecy and integrity of health information.

KEYWORDS: Cloud computing, healthcare, encryption, mobile healthcare application, integrity, security.

I.INTRODUCTION

As an emerging paradigm, smart cities leverage a variety of promising techniques, such as Internet of Things, mobile communications, and big data analysis, to enable intelligent services and provide a comfortable life for local residents. The smart city is an urbanized area where multiple sectors cooperate to achieve sustainable outcomes through the analysis of contextual, real-time information, which would produce massive opportunities for mobile healthcare social network (MHSN). Mobile healthcare is an innovative combination of mobile devices and mobile communication technologies, for it can provide necessary health information, routine care improvements, potential infectious disease prevention, health interventions, etc. It is getting more and more widely to apply the emerging cloud computing technology into the fields of mobile healthcare. By using mobile healthcare system, the electronic health record (EHR) can be transmitted over the network to the cloud service provider (CSP) for remote storage. Moreover, the healthcare providers can read it from an end device or access it remotely using a mobile device to provide real-time medical treatment. Meanwhile, people tend to share and disseminate the healthcare information via social networks, since social media is an extension of the healthcare professional and patient relationship. Consequently, mobile healthcare social networks (MHSN) are created for connecting patients so that they could share healthcare information using their mobile devices, and also connecting doctors and specialists for better healthcare. For example, people in MHSN can communicate and interact with each other before making healthcare decision. However, data security issues are the major obstacles to the application of MHSN. MHSN extends the traditional centralized healthcare system, in which the patients stay at home or in hospital environment and the professional physicians in the healthcare center take responsibility of generating medical treatment. Compared to traditional hospital-centric healthcare which not only lacks efficiency when dealing with identifying some serious diseases in early stages but also suffers from limited healthcare information, MHSN enables continuous health monitoring and timely diagnosis to the patients in the smart city. It relies on wearable devices and medical sensors to measure the patients' health conditions and sends health data to the processing unit for doctors' further diagnosis and analysis and provides easy access to a patient's historical comprehensive health information. Additionally, the patients wearing body sensors continuously monitoring their health conditions are assumed to walk outside, moving from time to time and place to place. However, MHSN may suffer from a series of security and privacy threats due to the vulnerabilities of personal health and social data. The collected private information is stored and processed in the honest but curious health and social cloud servers, which may be directly revealed during the storage and processing phases. Moreover, the adversary can intercept the sessions between patients to get their health and social data. Hence, the underlying security and privacy requirements, including confidentiality and access control, should be satisfied in MHSN.This paper comprises the study of various encryption

schemes which can be put to use for securing the patient's sensitive health information on cloud along with the implementation and performance analysis of a mobile healthcare application which encrypts the health records of patients before outsourcing it for storage over cloud and ensures effective access control, secrecy and integrity of health information.

II.MOTIVATION

Consequently, mobile healthcare social network are created for connecting patients so that they could share healthcare information using their mobile devices, and also connecting doctors and specialists for better healthcare. For example, people in mobile healthcare social network can communicate and interact with each other before making healthcare decision.

III.RELATED WORK

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.
In this section, we briefly review the related work on Secure Identity-based Data Sharing in Healthcare Social Network in Cloud Computing.

In this paper, the author proposed a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption techniques to encrypt each patient's PHR file. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. They utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. Further, uses different algorithms to enhance the security and efficiency. [1]

In this paper, the author proposed Lightweight Sharable and Traceable, a lightweight secure data sharing solution with traceability for mHealth systems. Lightweight Sharable and Traceable seamlessly integrates a number of key security functionalities, such as fine-grained access control of encrypted data, keyword search over encrypted data, traitor tracing, and user revocation into a coherent system design. Considering that mobile devices in mHealth are resource constrained, operations in data owners' and data users' devices in Lightweight Sharable and Traceable are kept at lightweight and provide security. Further, extensive experiments on its performance (on both PC and mobile device) demonstrated that Lightweight Sharable and Traceable is very promising for practical applications. [2]

In this paper the author proposed a method that, given a query submitted to a search engine, suggests a list of related queries. The related queries are based in previously issued queries, and can be issued by the user to the search engine to tune or redirect the search process. The method proposed is based on a query clustering process in which groups of semantically similar queries are identified. The clustering process uses the content of historical preferences of user's registered in the query log of the search engine. The method not only discovers the related queries, but also ranks them according to a relevance criterion. Finally, we show with experiments over the query log of a search engine the effectiveness of the method.[3]

In this paper, author presented a middleware solution approach to support data and network security over e-Healthcare system sing medical sensor networks. It has been shown that a masquerade attack can be launched to the system and patients 'data are in danger. We proposed this middleware to counter this kind of attack where a user and all devices into the healthcare network are mutual authenticated. Finally a performance analysis has been done with regard to masquerade attack and the result reveals the efficient of the proposed solution.[4]

In this paper, author design an inference attack-resistant e-healthcare cloud system with fine-grained access control. We first propose a two-layer encryption scheme. To ensure an efficient and fine-grained access control over the EHR data, we design the first-layer encryption, where we devise a specialized access policy for each data attribute in the EHR, and encrypt them individually with high efficiency. To preserve the privacy of role attributes and access policies used in the first-layer encryption, we systematically construct the second-layer encryption. To take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of data attributes in the EHR, we further construct a blind data

retrieving protocol. We also demonstrate that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations, which confirm the efficacy and efficiency of our schemes.[5]

In this paper, the author describes many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers. To access the data stored in cloud, existing work usually apply cryptographic methods such as attribute-based encryption. However, in doing so, these solutions inevitably leak the attribute and identity information of the users. For the purpose of secure access control in cloud computing while keeping the user's privacy, we propose the notion of identity-based group signature and apply it to realize the anonymous authentication to the cloud servers. Furthermore, both the user grant and revocation are supported by using the group techniques. [6]

In this paper the author first implement forward secure identity based ring structure by the use of HMAC algorithms. The model also comes in with the trendiest notion of forward security. The proposed model can be implemented by both, either with or without random oracles depending on the need of the system design. Also, the key can be entered manual by the receiver or queried from the system as automated. We have tried to cover and show different comparisons of different ways a system can be designed and implemented. There is always a room for improvement, so we believe more secure implementation with similar features can be done, also by giving more ease to the end user. We consider the same as open problem and motivation for future work. [7]

In this paper, the author proposes a Highly Available, Scalable and Secure distributed data storage system for high performance and secure data management. Distributed and parallel data storage or file systems such as Object-based Storage Devices and flexible key distribution schemes Data at rest (static) and in transit (dynamic) are protected with different encryption strategies for privacy and integrity. Secret sharing and replication support both security and availability. Encryption and key management are not necessary in data at rest protection. The future work includes a detailed simulation and further performance analysis. [8]

In this the author proposed a security scheme for users.This scheme provides storing and sharing their intricate data inthe Cloud environment. This scheme provides vital encryptionand decryption technique for achieving security on cloudapplication. The revocation procedure is an explicitperformance destroyer within the access control method incryptography. In this scheme, the unique data is firstly separated into numerous parts. Then these parts are sent to the cloud server. Whenever a user revocation happens, the data owner desires merely to retrieve one part and re-encrypt it. This scheme is based on cryptographic storage application. Furthermore techniques are implemented to improve the security of the data. [9]

In this paper, the author have proposed a protected multiple owner data sharing system. This system is used for dynamic groups in the cloud environment. Any Cloud user can unidentified person distribute data with other users in order to improve the signature of group and dynamic broadcast encryption techniques. For this, the storage transparency and encryption calculation cost are self governing with respect to the number of users that are revoked. Furthermore, the protection and investigation system with exact proofs is analyzed. [10]

IV.PROBLEM STATEMENT

However, data security issues are the major obstacles to the application of mobile healthcare social network. As we all know, health information such as treatment and drug information is considered to be highly sensitive. If these data are outsourced to the cloud service provider, the patient can't directly control the software or hardware platform for storing data. Without careful consideration patient may suffer serious medical information leakage from the cloud. For example, millions of electronic healthcare records have been compromised in recent years. Hence, it is significant that the electronic healthcare records should be stored in an encrypted form. Even if the cloud service provider is untrusted or compromised, the data maintains security and privacy. Simultaneously, the encrypted records should be shared and access in a reasonable way.

V. PROPOSED METHOD

We proposea secure identity based data sharing in Mobile Healthcare Social Network, which allow patient to outsource their encrypted health records to CSP with IBBE technique, and share them with a group of doctors in a secure and efficient manner. We present the attribute based conditional date re-encryption construction, which permits doctors who satisfy the pre-defined condition in the cipher text to authorize the CSP to re-encrypt the cipher text for specialist,

without leaking the sensitive information of the patient. We provide an efficient profile matching mechanism in MHSN based on the IBE with equality test that helps patients to find the friends in a privacy preserving manner and achieve flexible authorization on the encrypted health records with resisting the keywords guessing attack.

In the proposed model there are 5 modules:

CSP, CA, Doctor, Specialist, Patient

Central Authority: The CA is trusted for initializing the system and generating attribute keys and secret keys for participating users.

Cloud Service Provider: The CSP is responsible for the data storage and can be acted as a proxy as it is semi-trusted. Beside, this CSP also perform profile matching for the patients.

Doctor: The authorized Doctors can decrypt the patient's ciphertexts that stored in the CSP. When encountering a problem that needs to negotiate with the specialist, the doctor can generate a re-encryption request, thus the CSP converts the cipher text into an IBE-encrypted data for specialist if the doctor satisfies the pre-defined condition in the cipher text.

Specialist: The Specialist could decrypt the re-encrypted cipher text with the secret key and then assist doctors for advice.

Patients: The Patients register the system to obtain their secret keys with their identities. They encrypt the EHRs using algorithm and outsource the ciphertexts to CSP. Hence only authorized doctors could decrypt them. Simultaneously, patients with the same symptom can generate trapdoors and form social relationships according to their wills.

Architecture

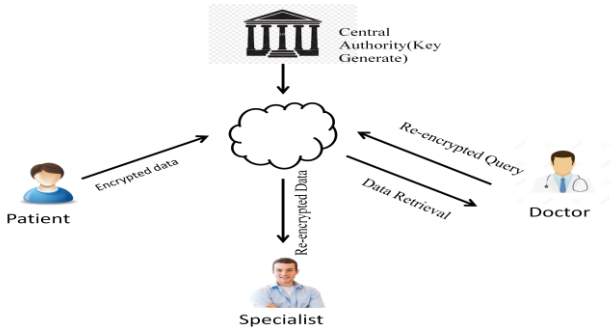


Fig.1 System Architecture

ALGORITHM

Algorithm for Encryption and Decryption.

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algorithm is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.

Vincent Rijmen and Joan Daemen was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input (0,1)

Secret key (128_bit) + plain text (128_bit).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 9, Issue 5, May 2020||

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

Xor state block (i/p)

Final round: 10, 12, 14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

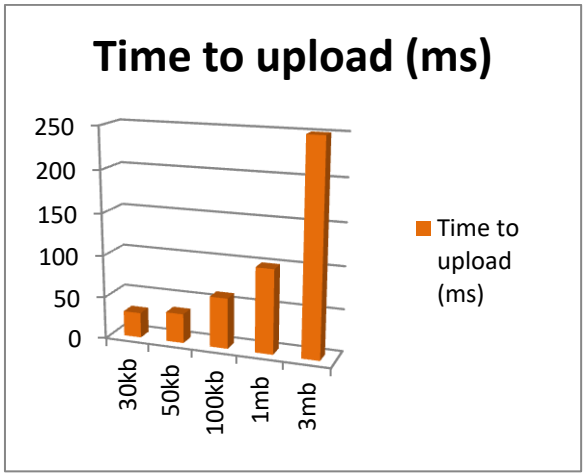
Ciphertext (128 bit)

Mathematical Equation:

The algorithm implemented in this project is describe as:
Initialization: password,key,time,salt:string
time ⟵ get time
input ⟵ (password)
key ⟵ salt + time
Encryption:
Ciphertext ⟵ AESEncrypt(password; key)
output(ciphertext)
Decryption:
key ⟵ salt ⟵ time
forasmuchtolerancegiventime
if key = get time
key ⟵ salt + time
plaintext ⟵ AESDecrypt(ciphertext; key)
endif
endfor
output(plaintext)

VI.EXPERIMENTAL SETUP

For proposed system jdk 8 used and IDE is NetBeans 8.1. Server is Apache tomcat 7. The data will store on cloud.



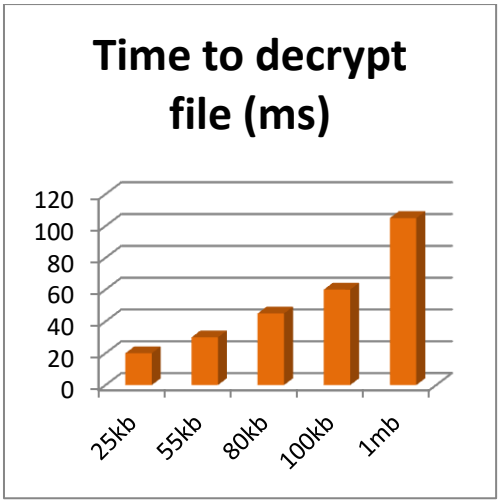
Graph:1Shows file size on x axis and time (ms) to upload on Y-axis

Explanation: Graph shows size of file and time to upload that file after performing fragment and t-coloring .As size of file increases the time will increase.

ID	File size	Time to upload (ms)
1	30kb	30
2	50kb	35
3	100kb	60
4	1mb	100
5	3mb	250

Table 01: Time to upload file

Above table 01 gives the information of uploading time for 30kb, 50kb, 100kb, 1mb and 3mb file size.



Graph:2 Shows file size on x axis and time (ms) to decrypt on Y-axis

ID	File size	Time to decrypt (ms)
1	25kb	20
2	55kb	30
3	80kb	45
4	100kb	60
5	1mb	105

Table 02: Time to decrypt and share file

Above table 02 gives the information of decrypting and sharing time for 25kb, 55kb, 80kb, 100kb, and 1mb file size.

VII.CONCLUSION

The MHSN has improved the healthcare through its convenient data sharing. For the purpose of guaranteeing data confidentiality and availability in MHSN, we propose a secure identity-based data sharing and profile matching scheme in cloud computing. We first realize secure data sharing in MHSN with cryptographic technique, which allows the patients to store EHRs to cloud securely and share them with a group of doctors efficiently. Then we present an attribute-based mechanism in MHSN, which allows doctors who satisfy the pre-defined conditions to authorize the cloud to convert a stored cipher-text into a new cipher-text under IBE for the specialist, without leaking any sensitive information. Further, we provide a profile matching mechanism based on IBEET, which can achieve flexible authorization on encrypted EHRs and help patients to find friends in a privacy-preserving and efficient way. The analysis and results show that the computation cost on patient side is reduced.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 9, Issue 5, May 2020||

REFERENCES

[1] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems Volume: 24 , Issue: 1 , Jan. 2013.

[2] Yang Yang, Ximeng Liu, Robert H. Deng, Yingjiu Li, "Lightweight Sharable and Traceable Secure Mobile Health System", IEEE Transactions on Dependable and Secure Computing, 2017.

[3] R. Baeza-Yates, C. Hurtado, and M. Mendoza, "Query recommendation using query logs in search engines," in Proc. Int. Conf. Current Trends Database Technol., 2004, pp. 588–596.

[4] Ndibanje Bruce, Mangal Sain, Hoon Jae Lee, "A Support Middleware Solution for e-Healthcare System Security", IEEE 16th International Conference on Advanced Communication Technology.

[5] Wei Zhang, Yaping Lin, Jie Wu, Fellow and Ting Zhou "Inference Attack-Resistant E-Healthcare Cloud System with Fine-Grained Access Control", IEEE Transactions on Services Computing 2018.

[6] Zhusong Liu, "A Secure Anonymous Identity-based Access Control over Cloud Data", 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies.

[7] Vivek Pandey, Umesh Kulkarni, "Effective Data Sharing with Forward Security Identity based Ring Signature using different algorithms", 2017 International Conference on Intelligent Computing and Control (I2C2).

[8] Zhiqian Xu, Hai Jiang, "HASS: Highly Available, Scalable and Secure Distributed Data Storage Systems", 2009 International Conference on Computational Science and Engineering.

[9] Kamara, S., Lauter, K. Sion, R., Curtmola, R., Dietrich, "Cryptographic Cloud Storage", 2010 Workshops of LNCS Springer, Heidelberg, vol. 6054, pp. 136-149, 2010.

[10] Bethencourt, J., Sahai, A.,Waters, B., "Ciphertext policy attribute-basedencryption", 28th IEEE Symposium on Security and Privacy, pp. 321-334, 2007.