IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Facilitating Secure Cloud Based Mobile Healthcare Application using Encryption Techniques

Praneeta K. Maganti[1*], Pushpanjali M. Chouragade[2]

[1,2] Dept. of Computer Science and Engineering, Government College of Engineering Amravati, Amravati, India

[*]*Corresponding Author: praneetamaganti@gmail.com, Mob.: +91-9921371259*

DOI: https://doi.org/10.26438/ijcse/v7i4.973977 | Available online at: www.ijcseonline.org

Accepted: 17/Apr/2019, Published: 30/Apr/2019

***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

I. INTRODUCTION

Mobile healthcare applications let patients avail the benefit of receiving consultation from healthcare service providers from anywhere and at any point of time by sharing their health information with them in cloud environment. To protect the health record from falling into wrong hands, it must be encrypted before setting it in transit for cloud storage, sharing and processing.

The proposed mobile healthcare application lets a patient share his/her health record with doctors of his/her choice using IBBE scheme. Here the patient has to pick the health record and select doctors from the list available with the application to share his/her health information. The input given by patient to the IBBE scheme is the health record for encryption and list of identities of doctors, who are authorized to access the health record. The IBBE scheme then outputs the encrypted health record.

The authorized doctors can download and decrypt the health record and provide consultation to patient. The doctor might require a negotiation with a specialist, if he/she is unable to attend the patient or require some specialist advice. In such cases the health record which can be accessed only by doctors mentioned by patient has to be re-encrypted, so that the specialist can download and decrypt it.

Here the CP-ABPRE scheme is propounded, where the doctor has to generate the key which re-encrypts and outsource it to cloud which acts as proxy along with the encrypted health record. The proxy then re-encrypts the health record for the specialists whose attributes are chosen by the doctor, without realizing the actual health information being shared. The doctor's end is relived from the re-encryption computation burden. Then the authorized specialists can obtain the health record and provide suggestion to doctor.

The patient may wish to discuss about the treatment, prescription, advantages and side affect with other patients suffering from similar symptoms. For patients to avail this service, the proposed application provides list of patients suffering from similar symptoms after proxy conducts a symptom matching over the encrypted health information using IBEET scheme, after the patient sends a trapdoor consisting of the symptoms he/she wishes to match.

The proposed application lets doctors and specialists to check if the patient's health record is the one originally shared by the patient or is modified or replaced for another by using integrity check. The patient here shares the secret hash key generated by SHA 256 with the central authority, which verifies the integrity of health record. Integrity verification of

health record using SHA 256 is important as encryption is responsible for providing confidentiality.

The contributions are aimed at providing integrity and confidentiality to the health records of patients which are shared, processed and stored on cloud using identity-based and attribute-based schemes. Also patients can receive consultation from doctors remotely and are allowed to chat anonymously with the patients suffering from similar heath problems. The proposed application helps healthcare service providers to have faster access to patients' health information. It provides security which works efficiently for mobile devices which have less computation power.

The organization of the rest of the paper is as follows, Section I provides the introduction to the secure health record storing, sharing and processing over cloud using encryption techniques. Section II encompasses the related works of various encryption techniques. Section III provides the methodology where proposed work's implementation explained. Section IV includes the results of the experimental analysis. Section V covers the conclusions and the possibilities and scope of the propounded work in future.

II. RELATED WORK

To overcome the security threats faced by cloud computing and to enable strict access restrictions over the data, various researchers have made their contributions.

The computation wise efficient and faster SKE schemes use same keys for enciphering and decryption are known to suffer from the drawback of secure distribution of key. The problem was overcome by PKE schemes which used two separate keys for enciphering and deciphering of data. Though it became successful in overcoming the SKE's lack of key transferring security, but it involved operations which slowed the system.

Hence hybrid approach was welcomed which involved the enciphering of data using SKE and the key to be shared was encrypted using PKE thereby providing a computationally efficient and faster method. But above scheme requires key distribution which is very complex as it involves certificates for ensuring the certainty of identity of the entities involved [3]. Hence to ease the complexity involved in PKE scheme, IBE was introduced where the publicly accessible key of the user is any arbitrary string which recognizes the user uniquely [1].

Also as an advancement aimed at providing one-to-many transfers ABE was propounded where the attributes replaced the identity. ABE comes in two types, one involves inclusion of access policy in secret key and attributes in cipher-text and the other is vice versa [2]. The idea of broadcast encryption scheme was pioneered by A. Fiat et al. [4], which involved transmission to some arbitrary no. of recipients.

Further advancements were introduced by applying it with identity-based [5] and attribute-based [6] cryptosystems. ABE involves huge computations which results in the draining of batteries of the portable devices like mobile phones. Hence identity based schemes gained preference [7].

In a scenario where a user has to authorize another user to access the encrypted data, either the user has to encrypt the data all over again with a new set of receivers or simply generate a key that is sent to a proxy to conduct re-encryption over the enciphered data without knowing the plaintext for the specified receivers' set. This idea was first given by M. Blaze et al. [8]. Variants like IBPRE [9] and ABPRE [10] were further introduced to achieve re-encryption at more fine level.

ABPRE can benefit low computation devices as the proxy is responsible for carrying out re-encryption and it provides access control at fine grained level. Conditional PRE was also introduced, where conditions involving either attributes or access policy were used with an objective to let delegator control which cipher-texts must be encrypted by the proxy. This was useful where the delegator has many data records like in mailing system [11]. Further IBCPRE and ABCPRE were also recommended for implementation.

To process data which is encrypted over cloud is possible by delegating authority to proxy. Reference [12] proposed the mechanism of searching keyword where the proxy is authorized by sending a trapdoor to perform equality test over the enciphered data. As an improvement over the setbacks of PKEET [13] scheme IBEET [14] was introduced.

III. PROPOSED METHODOLOGY

In Figure 1 DFD of the propounded system is shown. The central authority (CA) is the trusted entity. It carries out the initial setup and generates two keys, one of the two is called public parameter (PP) and the other key is kept privately with CA (MSK). CA sends the public parameters to the entities on request. The health record selected by the patient is encrypted by feeding the identities of the doctors selected by the patient and PP to the IBBE algorithm. The output of which is uploaded to cloud.

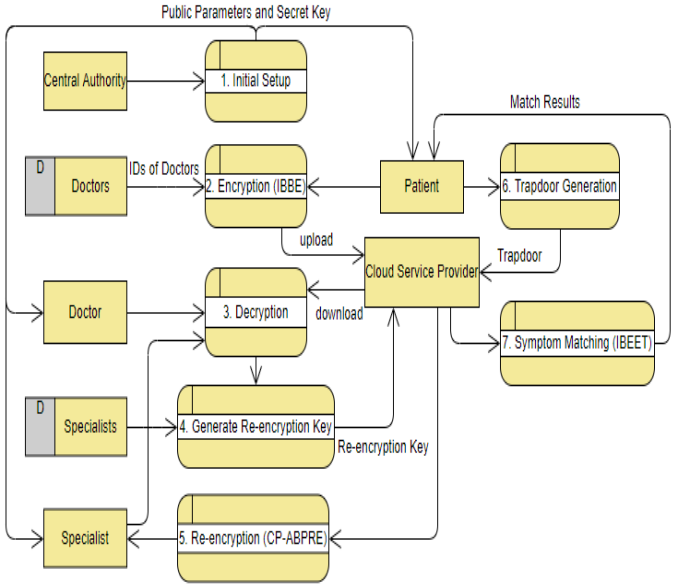

Figure 1. Data flow diagram of proposed system.

The authorized doctors can download and decrypt the file by first claiming their secret key from CA. CA calculates the secret key using MSK and doctor's identity and sends it to the doctor. Upon which he/she can decrypt and avail the health record. The doctor is further allowed to share it with specialists.

Here the doctor has to calculate the key that performs re-encryption using PP, his/her secret key and access policy, and then send it to CSP. CSP applies the received key to the encrypted health record, there by performing re-encryption using CP-ABPRE. The specialists satisfying the access policy are authorized to decrypt using their decryption key generated and sent by CA using specialist's attributes and MSK.

The patient has to send a trapdoor (one-way function) generated by using his/her secret key, PP and the symptoms, to the proxy, to find patients suffering from same symptoms by carrying out the equality test using IBEET. The proxy sends back the match results, upon which the patient can chat anonymously with the fellow patient.

Also to protect the integrity of the health record, the patient calculates the hash function over the enciphered data and sends the hash key to the CA, thereby delegating the integrity checking to the CA. CA provides the integrity check results when requested by the doctor or specialist. Figure 4 shows the integrity check result where the hash is matched.

The proposed work is implemented on Win 10 platform, using Eclipse JEE photon with MySQL community 8.0 serving as backend. The server used is Apache Tomcat 9.0.

The application is created in Android Studio IDE. In Figure 2 homepage consisting of the login page is shown.

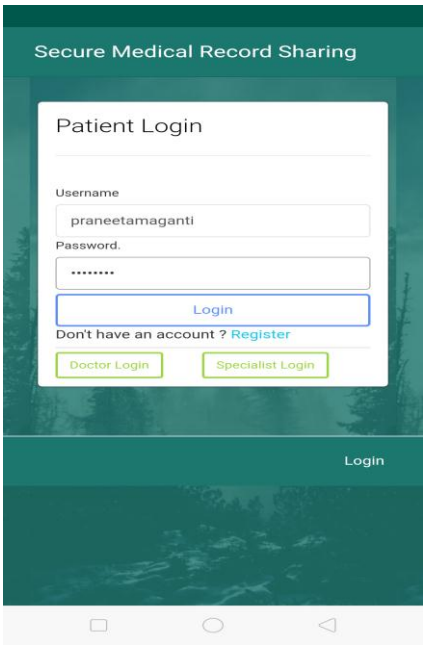

Figure 2. Users login page.

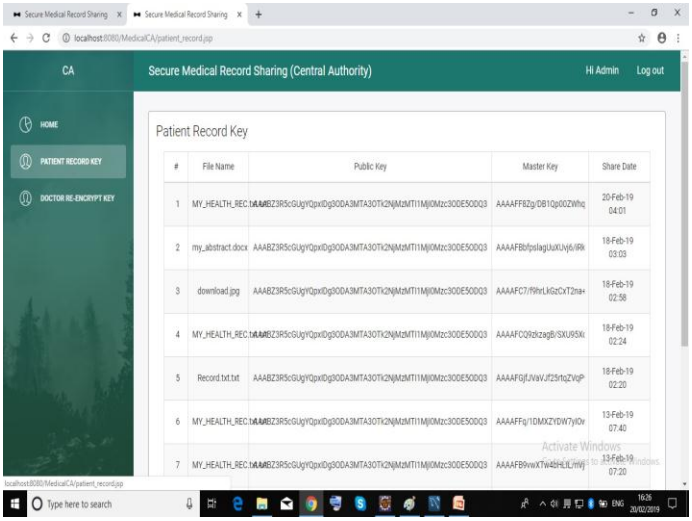

Figure 3. Medical CA portal.

The above Figure 3 shows the web page of the CA, which initialize the system by generatong the PP and MSK, generate keys for the system users and check integrity of patient's health record.

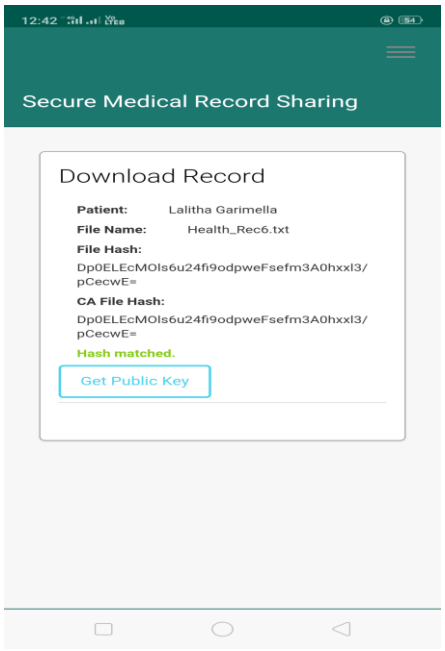

Figure 4. Integrity check.

IV. Results And Discussion

The results of the experiments have been deduced by considering the file size taken and number of doctors selected against the time taken for the IBBE scheme. And for the CP-ABPRE scheme the file size and number of attributes are considered against time taken. It can be observed from Figure 5 that the time required for encryption using IBBE scheme increases as the file size increases. Although time required for decryption is very small i.e. around 50 ms, a constant increase in time can be noticed as the file size grows.

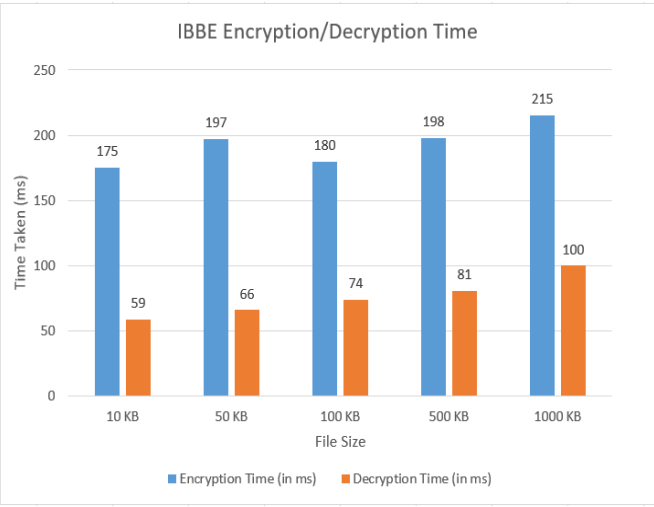

Figure 5. Encryption and decryption time for IBBE w.r.t. file size.

The time taken for re-encryption is around 125 ms, also it can be seen that as the file size grows, the re-encryption time has no major effect which can be noticed in Figure 6 that the growth in the time taken is very small. Same is observed with decryption. It takes very less time and also the growth is very small. Also the re-encryption process is outsourced to the proxy, which relives the burden at the user end.

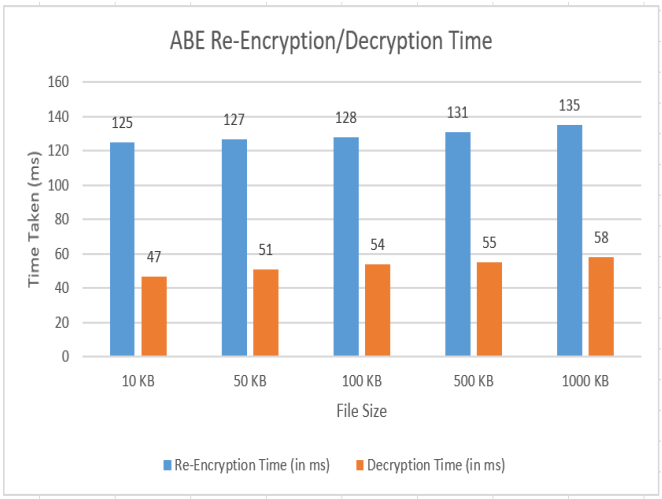

Figure 6. Re-encryption and decryption time for ABPRE w.r.t. file size.

Also, it is observed that as the number of doctors selected increases, the re-encryption time increases in IBBE scheme. For CP-ABPRE scheme as the no. of attributes selected increases, the re-encryption time increases. This causes no extra computational burden over the system as the process is carried out by the proxy. The decryption time is almost always constant for both the cases. The proposed secure system is suitable for the portable mobile devices with less power of computation.

V. Conclusions And Future Scope

Security for a mobile healthcare application is proposed using efficient encryption schemes, which being cloud based is accessible from anywhere and at any time and is prone to compromise confidentiality and integrity which may lead to the misuse of the sensitive information related to the patient. Implementation of encryption schemes for the proposed work is suitable for the portable devices with low computational power. A mobile healthcare framework which securely lets patients share their data with healthcare providers and in turn receive consultation via chat system is implemented, which also lets patient anonymously chat with other patients suffering from similar symptoms. It can be observed from experimental results that the cost of computation is reduced on user side. Further developments can be made by outsourcing the decryption and enabling revocation.

REFERENCES

[1] D. Boneh and M. Franklin, "*Identity-based Encryption from the Weil Pairing*", In. Kilian J. (eds) Advances in Cryptology, CRYPTO 2001, Lecture Notes in Computer Science, Vol.**2139**, pp.**213-229**, **2001**.

[2] R. Lakshmi, R. Lavanya, M. Meenakshi, Dr. C. Dhas, "*Analysis of Attribute Based Encryption Schemes*", International Journal of Computer Science and Engineering Communications, Vol.**3,** Issue.**3**, pp.**1076-1081**, **2015**.

[3] Abbas and S. U. Khan, "*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,** Issue.**4**, pp.**1431-1441**, **2014**.

[4] A. Fiat and M. Naor, "*Broadcast Encryption*", In. Stinson D. R. (eds) Advances in Cryptology, CRYPTO 1993, Vol.**773**, pp.**480-491**, **1993**.

[5] C. Delerablee, "*Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys*", In. Kurosawa K. (eds) Advances in Cryptology, ASIACRYPT 2007, Lecture Notes in Computer Science, Vol.**4833**, pp.**200-215**, **2007**.

[6] D. Lubicz and T. Sirvent, "*Attribute-Based Broadcast Encryption Scheme Made Efficient*", In. Vaudenay S. (eds) Progress in Cryptology, AFRICACRYPT 2008, Lecture Notes in Computer Science, Vol.**5023**, pp.**325-342**, **2008**.

[7] Q. Huang, W. Yeu, Y. He and Y. Yang, "*Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing*", IEEE Access Special Section on Cyber-Threats and Countermeasurs in the Healthcare Sector, Vol.**6,** pp.**36584-36594**, **2018**.

[8] M. Blaze, G. Bleumer and M. Strauss, "*Divertible Protocols and Atomic Proxy Cryptography*", In. Nyberg K. (eds) Advances in Cryptology, EUROCRYPT'98, Lecture Notes in Computer Science, Vol.**1403**, pp.**127-144**, **2006**.

[9] M. Green, G. Anteniese, "*Identity-based Proxy re-encryption*", In. Katz J., Yung M. (eds) Applied Cryptography and Network Security, ACNS 2007, Vol.**4521**, pp.**288-306**, **2007**.

[10] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, y. Yu and A. Yang, "*A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing*", Future Generation Computer System, Vol.**52**, pp.**95-108**, **2014**.

[11] J. Weng, R. H. Deng, X. Ding, C. Chu and J. Lai, "*Conditional Proxy Re-Encryption Secure against Chosen-Ciphertext Attack*", Proceedings of the 4th International Symposium on Information, Computer, and Communication Security,ASIACCS'09, pp.**322-332**, **2009**.

[12] D. Boneh, G. D. Crescenzo, R. Ostrovsky and G. Persiano, "*Public Key Encryption with Keyword Search*", Proceedings of EUROCRYPT, Interlaken, pp.**542-545**, **2004.**

[13] G. Yang, C. Tan, Q. Huang and D. Wong, "*Probabilistic Public Key Encryption with Equality Test*", In. Pieprzyk J. (eds) Topics in Cryptology-CT-RSA 2010, Lecture Notes in Computer Science, Vol.**5985**, pp.**119-131**, **2010**.

[14] S. Ma, "*Identity-based encryption with outsourced equality test in cloud computing*", Information Sciences, Vol.**328**, pp.**389-402**, **2016**.

Authors Profile

P. K. Maganti pursued Bachelor of Engineering from Sant Gadge Baba Amravati University, Amravati, Maharashtra, India in 2017 and is currently pursuing Master of Technology in Computer Science and Engineering from Sant Gadge Baba Amravati University, Amravati, Maharashtra, India, from 2017. Her main research work focuses on Cryptography Algorithms, Network Security,Cloud Computing and Cloud Security and Privacy, based education.

P. M. Chouragade pursued Bachelor of Technology from Sant Gadge Baba Amravati University, Amravati, Maharashtra, India in year 2011 and Master of Technology from Sant Gadge Baba Amravati University, Amravati, Maharashtra, India in year 2013. She is currently working as Assistant Professor in the Department of Computer Science and Engineering at Government College of Engineering Amravati, Amravati since 2013. She has published research papers in reputed international journals and conferences including IEEE and it's also available online. Her main research work focuses on Web Mining, Image Processing and IoT based education. She has 6 years of teaching experience.

