An Efficient Approach for Secured E-Health Cloud System Using Identity Based Cryptography Techniques in Cloud Computing Environment

Shikha Mittal¹, Paramjeet Singh², Rahul Malhotra³

¹Ph.D Scholar, Dept. of CSE, IKGPTU, Kapurthala
²Associate Professor, Dept. of CSE, GZSCCET, Bathinda
³Director-Principal, SDDIET, Barwala

E-mail: shikhs.mittal@gmail.com

https://doi.org/10.26782/jmcms.2019.06.00010

Abstract

Nowadays, cloud computing is an interesting research area among the researchers. It is an internet-based pool of heterogeneous resources. Cloud environment is very much reliable to make availability of resources when required to online users. Reliable computing services can be handled without any own infrastructures, so it would be considered as an alternate cost effective technique. Most of the organizations utilized the technique of cloud computing to host their applications. The service of the health care unit is the most essential service for the people. There is a necessity to store the sensitive information related to the patient’s medical history in a secure way. Therefore, the research and development in the Personal Health records and Electronic Health records is negligible area. Thus the most robust encryption and decryption should be encountered. One among the advanced technology in cloud computing is the maintenance of Electronic Health Records (EHR). The main objective of this paper is to propose and implement a methodology to exchange the health information about a particular person in a secured cloud environment. The medical information about a patient from distributed manner is also maintained in EHR by cloud environment. The stored information of the user provides the facility of collecting, sharing, exchanging and organizing that information through users. Therefore, an efficient approach for securing e-health cloud system using identity based cryptography techniques is presented in this research study.

Keywords: Cloud computing, EHR, Data Privacy, Key Management

I. Introduction

In the recent years, for storing the data or the information via web, the only most famous application is Cloud computing. Within the last past years, cloud computing has developed from being a promising business plan to at least one of the fastest developing fragments of the IT business [III]. Because of the ability of cloud
computing, the users are increasing vastly in the recent years. The cloud computing also provides the better effective application with the adequate cost in a satisfied way for the users. Through the virtualization the cloud computing also fulfills the different tasks related to the computational. The management of the huge data and provide the light weight services, the industries and the university are encouraged to employ the cloud computing at their place. Even in the small and medium scale industries are fascinated towards the cloud computing. Because it does not need the major funds for the infrastructure, the license for the software and for the other application oriented requirements. Due to its minimized maintenance fund and the strong capability of the cloud computing in the government organizations. The security is one among the chief objectives of cloud providers providing cloud computing services. If data kept in cloud resources are taken or inaccessible for many days because of the deteriorating network connection, the commercial loss to the user is not only be that one specific service unavailable, but it causes a comprehensive risk of the company’s presence, due to the sudden unavailability of IT services. The comprehensive investigation of cloud computing safety hazards, probable mitigation methods and superior cloud security systems is essential for establishing trust in technology and rising security. Cloud computing is used to stock, manage, and progress the data by using the network of remote servers presented on the internet.

The rest of the paper is organized into different sections as follows: Section-II presents a brief background of e-health systems in cloud computing and its services. Section-III discusses a brief summary of related works done. Section-IV covers proposed methodology. Section-V presents simulation results and discussion of the proposed work. Conclusion is shown in Section-VI while references are mentioned at the last.

II. E-Health Systems in Cloud Computing—Background

The improvisation and enhancement in the medical services the modern Information technology is applied in the healthcare field. This may reduce the costs. The new possibilities are offered by the E-health clouds for achieve the quick and the global access to the medical data. This provides the innovative business model opportunities. This E-health system also includes the issues and the growth restrictions in the area of privacy and security aspects. In the recent years the in the field of healthcare the development of information technology is widely increased in many countries. The standardization of national and the international level there is an ongoing effort for the exchange of data. So there are so many various application situations are imagined in the electronic healthcare. For example-

- Medical research
- Accounting and billing
- Electronic health record
- Trading intellectual property

The costs in the healthcare are believed to minimum in the e-health systems such as the electronic health records. In general the personal health management is improved in the electronic health records. In some of the country the every insured person used to have the smartcard which does not containing the administrative data such as the
name and the health insurance organization, then the following medical data are easy to access as well as store:

- Electronic prescriptions
- Blood group
- Medication history
- Electronic health records

This smartcard also comprises the keys for the cryptographic and the functions which is used to recognize the patient and to process the encryption for the sensitive data. The other countries have the consistent file for the data which is easy to share the information. The data in the EHRs are used to share and securely transfer by the similar organization according to the smartcards. All the above mentioned methods are mainly used to store the medical information in the central data storage centers. This infrastructure is made with centrally managed healthcare concepts. It is essential to keep health data as safe because the exposure of the health data may cause the severe effects mainly for the patients. So the employment of the framework for the security and the privacy is must to store and process the extreme sensitive data. Simply says, the bank or the organization may reject the job if the health information to that related person was leaked. If the health data was leaked from the system intentionally or unintentionally, the answerable professionals in the health field or the IT providers may face the penalties for not obeying the privacy laws.

The following difficulties are generally faced by the E-health systems when considering the privacy regulations:

- The E-health systems not only handle the patient medical data, it also carried out the several works like billing and accounting of the treatments, medicine list etc.
- Additionally the solution based on the smartcard, the system has to authenticate in some manner to recover the data even when the smartcard holder was not able to verify the system if he/she is in very critical health condition.
- In some other cases, the data have to be accessed even when the smartcard holder is not at that time; example the patient relative buys the medicine for the particular patient at a pharmacy.
- These above mentioned problems are really difficult to overcome for the industry and the industry. Now days the solution and standards mostly concentrated on the network security and access control polices. Though, they are not address the security for the consumer platform properly such as the health specialists are used the security of the hardware and the software.

An overview of E-health system is shown in figure 1 below.
A. E-Health Cloud Model

The overview of sample e-health arrangement is explained here, which is organized in the national level healthcare IT applications. In previous years, the doctors usually stored the patient’s medical history in the paper with the written form. This is a way of keeping the information in the closed location at doctor’s cabin. Even though the vast use of computers as well as the updated Information technology in the healthcare organizations permitted for a reasonable effort to accomplish the secrecy and security of the separated medical records. This is because of the distributed and the self-managed organization of every institution.

The very sensitive data processing and storage is leads the crucial issues such as deploying the IT infrastructure outsources such as cloud computing and the various related services such as the accounting and the billing in the medical surroundings in various places. The health professionals are the person who carries the health care services such as the dentist, Physician, pharmacists, Lab technician, etc. The health care providers are the institute which is delivering the services to the patients such as Hospital, Medical institutions.

Normally theses medical records are classified into two categories:

- Personal Health Record (PHR)
- Electronic Health Record (EHR)

a. Personal Health Record (PHR)

This is the record which is managed by the patient, that comprises the patient’s health related data and the medical related data object database.

b. Electronic Health Record (EHR)

This is the record which is usually managed by the health professionals, that comprises the patient’s health related data and the medical related data object database.
database. Most of the time the both are not accurately varied. But in some of the countries both the terms are taken as the different credentials because of the numerous legal suggestions.

III. Related Works

A number of research works have been carried out by many researchers in the domain of e-health cloud computing on basis of past research papers and literatures. Some of them are as under:

(Huang, et al. 2018) have been proposed profile matching techniques and secure data sharing in the Mobile Healthcare Social Networks (MHSN) cloud computing. However, the social networks and cloud computing have been changed the via of healthcare to provides the real phase data sharing in the effect method. The data security has some issues with main difficulties from the wide applications of Mobile Healthcare Social Networks (MHSN). So the patients have encrypted health records to outsource the storage with IBBE (Identity based broadcast encryption) techniques and they shared with group of surgeons in the effective and secure manner. In far they presented the attribute based data re-encryption which permitted the clinicians to satisfy the pre defined conditions in cipher text to be authorized in the cloud environment to convert them into new cipher text of identity based encryption structures without leaked any delicate information by the specialist [VI].

(Li, et al. 2018) aimed to tackle the efficiency and the pathetic information in cloud data sharing have some security problems. so far they proposed the attribute based data sharing methods for the suitable manner of mobile resource users in clouds. Also they supported the offline and online encryption though they allow anyone to checked the validity of ciphertexts before they decrypt. The scheme secure provened and the selective chose the attributes set and chose the security model with DBDH assumption. Even though the task computation in the offline mode it reduced by adding the public parameters. The results with data sharing were extremely suitable for resources mobile users [IX].

(Kalaiprasath, et al. 2017) developed the cloud security with ontology to control, compliances and threat. They have offer the classifiers in security model of threat had faced by cloud operators. The users have high level security were automatically determined and the activated threats have defiance of cloud providers. So the cloud consumers used to formulate the security policies and to find the compliance providers with technology. So they semantically developed the ontology to the security threats models, controls, providers data have expressed and the cloud security policies. They used as easy manner in cloud security policies also they recommended the consumers were planned to move their data to the cloud and the secure the concerns. They developed the rules in ontology as the reason that better matched of compliant providers [VII].

(Luna, et al. 2017) stated to improve the cloud security plan necessities have introduced the simple methodology and flexibility. Then the customer allows classifying and represented the needs of security. So far they extended the techniques as state of the art security evaluated and accessed the security level by cloud secSLA’s. Hence the secSLA’s defined the standardization and works in the state of the art. The techniques validated through the real world data of cloud service
providers to acquire from the cloud security alliance. They presented the main thing of decision making as security in pattern and they implemented the results techniques of visually matched the CSP based their secSLA’s to customers. However, the technique used some drawbacks in security to solved these future work going to suggest as advanced of secSLA’s and notations like end-to-end process, uncertainty and dependencies in secSLA’s are involved for the better evaluation to improve the security assurance [XI].

(Aljawarneh and Yassein 2016) anticipated the effects of the existing techniques to survey the symmetric of the cloud security issues in these environment. They proposed the cloud security software framework as potential development and the concepts of the fuzzy systems to clear the large number of security issues in cloud with the altered level of frameworks [I].

(Almorsy, et al. 2016) suggested the cloud security to analyse the problem in detail with this concepts. So, they examined the main problems of cloud design of perspective, the cloud stakeholder’s perspective, cloud service delivery models perspectives and the cloud offered characteristics perspective. They analysed to derive the detailed things of key features and specification of cloud security problem in the offered cloud security solution [II].

(Samarati, et al. 2016) presented about the security issues and concerns of cloud computing illustrated the impact of availability, confidentiality and integrity as their properties and described the possible challenges, directions and current solutions. Therefore the cloud had been emerged the computing paradigm as successful with the organization and users. Then they depend on external providers to stored, process the data also make them available always to others. Though they presented the concerns and issues raised the scenario as, storage, processing of data and management [XIII].

(Ma 2016) proposed the concepts of Identity Based Encryption (IBE) and Public Key Encryption With Equality Test (PKEET) obtained from Identity Based Encryption With Equality Test (IBEET). Inherited the advantage of PKEET and IBE was simplified the certificate management of PKEET with all the encrypted messages through the receiver public identity. So, the scheme IBEET receives the trapdoor computing were used by secrete values to identify and send the cloud server for the test of equality in ciphertexts. Therefore used the primitive some one have trapdoor to identify could delegate the capability of equal test with ciphertexts and does not require any authority centralized to act as delegator. It very appropriate to client with the minimum computation resource [XII].

(Khan and Tuteja 2015) offered the important cloud computing related with security, privacy, reliability and anonymity. Then the furthermore significant were security and providers in cloud to assure it. So the main concepts of secureness in clouds means calculation of treatment and the storage were hosted in databases by cloud providers. These proposed have security issues in cloud to analysed and the better security mean the dissimilar cryptographic algorithms are used as symmetric algorithms [VIII].

(Fabian, et al. 2015) presented the architecture and implemented the data sharing to provides the high level of privacy and security for the semi trusted of cloud environments to persistent data. They have been manner on features schemes as Attribution Based Encryption (ABE) to select the access of authorization and the
secret sharing of cryptographic to separate the data in multi clouds. So the cloud providers had the curious capability of reduced the adversarial. Therefore the implemented and evaluated of the several researches prove the good performance and viability from this methodology. So far they intended the adding of load balancing and stress tests to simulate the operation and the multi simultaneous client needs [IV].

(Xhafa, et al. 2015) aimed to allow the efficacy storage and sharing of the personal health records to the cloud computing and then they designed the electronic health records were based on the clouds also used the attribute based encryption. So the systems allowed the patients to share their PHR with the surgeon to performed the encryption data to their symptoms. Then they known the precise description for the illness and the physician departments taken the medical treatment [XV].

(Hu Y and Bai G 2014) suggested that the single superiority to processing the ability and the big data storage and the cloud platform have hybrid to the access control and the security protection of main mechanisms to developed the healthcare home based systems. They reviewed the pinpoint of the hybrid cloud platform with thee mechanisms of security protection and the media access control. Cloud computing had the e-health to emerged area. So they needed the pin point challenges and state of the art, possible directions have an application and reasearch development. They reviwed the e-health in cloud computing have some security problems to solve with them encryption mechanisms [V].

(Shen, et al. 2014) offered the e-health monitoring system with privacy preservation and minimum service delay have exploited the geo-distributed clouds. Thus the system have resources sharing scheme it enabled to distribute the cloud servers and assigned the servers to request the user to load balance. The service had delay with the minimize of users. The another thing were proposed the traffic shaping algorithm. It converted the user health data collision to non health data collision have such capability to analzed the traffic attacks to reduced. Thus they shown the efficient for the proposed algorithm of traffic shaping in contain two terms, privacy preservation and service delay [XIV].

(Liang, et al. 2014) anticipated the Identity Based Encryption (IBE) to eliminate the necessity of have the cost certification and verification process. So far the revocation remained that the daunting task to term as, Key update and Ciphertext update. Have these phases due to an lack of the reversal credential grade. As this paper solved the efficiency problem to gain by revocation. They proposed the scheme as Cloud Based Revocable Identity Based Proxy Re-Encryption (CR-IB-PRE) scheme supported the delegate of decryption rights to the user revocation. The methods offered the data sharing mechanism as flexible to the system and supported the properties of re-encryption have traditional IBE methods revocable were compared. Then the paper motivated about the open problems [X].

**IV. Proposed Methodology**

The methodology which is utilized in Electronic Health Record (EHR) had some drawbacks such as scalability in key management, risk of privacy exposure, flexible access and user revocation. Also the main disadvantage is that whether the patients are controlling the sharing of sensitive personal health information specifically when they are stored on the cloud server. The security of the sensitive information is the
main concern to handle it. To overcome these problems, a secure Electronic Health Record (EHR) database storage in cloud infrastructure is proposed in this work. The main objectives of our proposed work are as under:

- To secure the intimate patient information by the deploying the Electronic Health Record
- To provide the better security in the EHRs using Encryption, Re-encryption, Level-I decryption, Level-II decryption

V. Simulation Results and Discussion

This section shows the simulation results of our proposed work. The performance analysis of the proposed algorithm is briefly discussed here.

A. Performance Analysis of Encryption Time

The performance analysis has been made on the basis of encryption time and re-encryption time. Table-1 shows the performance analysis of encryption time of our proposed algorithm.

Table-1: Performance Analysis of Encryption Time

| Data (in GB) | GA07B | LZD | WCW | IBPRE | Proposed |
|--------------|-------|-----|-----|-------|----------|
| 1            | 1000  | 1000| 1000| 1000  | 800      |
| 100          | 2000  | 3000| 3000| 3000  | 1800     |
| 500          | 8000  | 10000| 10000| 10000 | 7500     |
| 1000         | 12000 | 15000| 15000| 15000 | 10000    |

The table-1 and figure 2 shows the encryption time of four existing methods and our proposed method. In this approach the four existing methods such as GA07B, LZD, WCW and IBPRE are taken into account for the comparative analysis to acquire the better results in our proposed algorithm.
The 1 GB data for the existing methods like GA07B, LZD, WCW and IBPRE takes 1000 ms time which is comparatively higher than the proposed method, similarly 100 GB data acquired within 1800 ms in proposed method, however an existing method takes 2000 ms which is not favourable. Thus from the table-1 and figure 2, it is analyzed that the proposed method consumes lesser time for data retrieval than other four existing methods.

**B. Performance Analysis of Re-Encryption Time**

In this section the performance analysis of re-encryption time of the proposed algorithm is discussed.

Table-2 and figure 3 shows the re-encryption time of existing methods and our proposed algorithm. In this manner, the proposed method acquires lesser time than four existing methods in term of data retrieval time. The GA07B, LZD, WCW and IBPRE are existing methods takes 1000 ms and proposed method takes 900 ms for acquiring data size of 1 GB. Likewise for the data size of 500 GB the existing methods GA07B, LZD, WCW and IBPRE consumes 15000, 13000, 10000 and 5000 ms of time which is not more efficient results than proposed method due to its 4800 ms of time for data retrieval. Hence it concludes that our proposed method is much more efficient than the existing methods. Thus our proposed algorithm gives better results in this way.

| Data (in GB) | GA07B (in ms) | LZD (in ms) | WCW (in ms) | IBPRE (in ms) | Proposed (in ms) |
|-------------|---------------|-------------|-------------|---------------|------------------|
| 1           | 1000          | 1000        | 1000        | 1000          | 900              |
| 100         | 4000          | 4000        | 2000        | 2000          | 1900             |
| 500         | 15000         | 13000       | 10000       | 5000          | 4800             |
| 1000        | 23000         | 22000       | 20000       | 19000         | 15000            |

Table-2 and figure 3 shows the performance analysis of checking re-encryption time for different data size. Here, four existing methods such as GA07B, LZD, WCW and IBPRE are utilized for validating the comparing the results. Also the size of the data range from 1 GB to 1000 GB has been used for analyzing the performance of the proposed approach. The graphical representation of this evaluation is shown in fig. 3. The results depicted that the proposed approach offers better performance than the existing methods.
VI. Conclusion

The cloud security plays an important role in the monitoring of patients E-health records. In patient’s health record system a key is used by patients for the process of encryption from which the other third parties like insurance agents, doctors, nurse and others may extract the data which are relevant to them with the help of some encryption key provided them. In this paper, the performance evaluation of the proposed system in terms of encryption time and re-encryption time has been computed. The results of the proposed algorithm is evaluated and compared. The obtained results depicted that the proposed approach offers better performance than the existing methods. In future, we could take other parameters like encryption cost, re-encryption cost, checking cost, level-1 decryption, and the level-2 decryption using the same approach.

References

I. Aljawarneh SA & Yassein MOB (2016), ‘A Conceptual Security Framework for Cloud Computing Issues’, International Journal of Intelligent Information Technologies (JIIT), Vol. 12, No. 2, pp. 12-24.

II. Almorsy M, Grundy J & Müller I (2016), ‘An Analysis of the Cloud Computing Security Problem’, arXiv preprint arXiv:1609.01107.

III. Dhirender Singh, R. K. Banyal, Arvind Sharma, ‘Cloud Computing Research Issues, Challenges, and Future Directions’, Emerging Trends in Expert Applications and Security, Advances in Intelligent Systems and Computing 841, Springer Nature Singapore Pte Ltd. 2018.
IV. Fabian B, Ermakova T & Junghanns P (2015), ‘Collaborative and Secure Sharing of Healthcare Data in Multi-Clouds’, Information Systems, Vol. 48, pp. 132-150.

V. Hu Y & Bai G (2014), ‘A Systematic Literature Review of Cloud Computing in e-Health’, arXiv preprint arXiv:1412.2494.

VI. Huang Q, Yue W, He Y & Yang Y (2018), ‘Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing’, IEEE Access, Vol. 6, pp. 36584-36594.

VII. Kalaiprasath R, Elankavi R & Udayakumar DR. (2017), ‘Cloud. Security and Compliance- A Semantic Approach in End to End Security’, International Journal of Mechanical Engineering and Technology (IJMET), Vol. 8, No.5.

VIII. Khan SS & Tuteja R (2015), ‘Security in Cloud Computing using Cryptographic Algorithms’, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, No. 1, pp. 148-155.

IX. Li J, Zhang Y, Chen X & Xiang Y (2018), ‘Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing’, Computers & Security, Vol. 72, pp. 1-12.

X. Liang K, Liu JK, Wong DS & Susilo W (2014), ‘An efficient Cloud-Based Revocable Identity-Based Proxy Re-Encryption Scheme for Public Clouds Data Sharing’, European Symposium on Research in Computer Security, pp. 257-272.

XI. Luna J, Taha A, Trapero R & Suri N. (2017), ‘Quantitative Reasoning about Cloud Security Using Service Level Agreements’, IEEE Transactions on Cloud Computing, Vol. 5, No. 3, pp. 457-471.

XII. Ma (2016), ‘Identity-based Encryption with Outsourced Equality Test in Cloud Computing’, Information Sciences, Vol. 328, pp. 389-402.

XIII. Samarati P, Di Vimercati SDC, Murugesan S & Bojanova I (2016), ‘Cloud Security: Issues and Concerns’, Encyclopedia on Cloud Computing, pp. 207-219.

XIV. Shen Q, Liang X, Shen XS, Lin X & Luo HY (2014), ‘Exploiting Geo-Distributed Clouds for a E-Health Monitoring System with Minimum Service Delay and Privacy Preservation’, IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 2, pp. 430-439.

XV. Xhafa F, Li J, Zhao G, Li J, Chen X & Wong DS (2015), ‘Designing Cloud-Based Electronic Health Record System with Attribute-Based Encryption’, Multimedia Tools and Applications, Vol. 74, No. 10, pp. 3441-3458.

Copyright reserved © J. Mech. Cont.& Math. Sci.
Shikha Mittal et al.