International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Effective and Secure e-Health Cloud Model using Identity Based Cryptography

Shikha, Paramjeet Singh, Rahul Malhotra

Abstract:- ***Now days for storing the data and information through World Wide Web only and only one of the most popular applications is cloud computing. Due to availability of cloud computing, users are rapidly increasing in recent years. The cloud computing provides better effective application with adequate cost in a satisfied way for users. Therefore it is necessarily to keep health services data as safe and secure because the exposure of health services data may cause severe effects for the patients. Hence, the employment of a framework for security and privacy is must to store and process extreme sensitive data. So far patients had the owner of personal health records, it encrypted and stored with cipher text in the cloud server. To ensure privacy and security in cloud computing environment is a big issue. The medical system has been designed as a standard, access of records and effective use by medical practitioners as required. In this paper, we propose a novel algorithm along with implementation details as effective and secure e-health cloud model using identity based cryptography.***

Keywords: Cloud computing, E-health Cloud Model, EHR Data, Identity Based Encryption

I. INTRODUCTION

Today, the field of health care in India facing major challenges because the technology growth in this field is minimum and it is essential to provide completed history of the patient to the doctor. Doctor required the complete details of patient for proper diagnosis but it is difficult to maintain the record of each patient and their previous treatment details. Many people undergone treatment for different diseases from different field of doctors, so the details of the treatments are scattered among the offices and it is critical to inform treatment details to individual doctors. There are chances of repeating the tests without proper consulting which is waste of time and money. Sometimes various combinations of medicines lead to the serious health issue. So, accurate record keeping is necessary in the field of health care. Information transferred among the health care doctors through the papers or personal communication in the current methodology made the chances of producing death. E-health care provides the chances to keep all the medical records and the records can be accessed by the doctors during the patient visit with the permission of the patient. The service is utilized for effective maintenance of the health record.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
Shikha*, Ph.D Scholar, Dept. of CSE, IKGPTU, Kapurthala E-mail: shikhs.mittal@gmail.com
Dr. Paramjeet Singh, Professor, Dept. of CSE, GZSCCET, Bathinda
Dr. Rahul Malhotra, Director-Principal, SDDIET, Barwala
smoussa@cud.ac.ae

The system also utilized to provide the real time information. Electronic health record (EHR) is also known by the name of Electronic medical record (EMR) and the records utilized cloud servers for high quality infrastructure with cost benefit. Electronic storage system reduces the chances of utilizing hard copies of records and the format of softcopy can be shared among the surgeons, insurance companies and third party administrators. Maintaining the confidentiality and privacy of the patients are the important security issues of electronic health record (EHR) maintenance. Cloud service providers are maintaining and managing the cloud servers, so the environment is a trusty one. 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.

The remainder of paper is as follows: Section-II discusses about cryptography approach in context to cloud computing. Section-III presents literature review. Section-IV covers proposed methodology. Section-V shows implementation details and discussion of the proposed work. Conclusion is shown in Section-VI while references are mentioned at the last.

II. CRYPTOGRAPHY APPROACH

Cryptography is based on complex mathematical issues like prime number factorization and it is a captivating technique to transfer the data progressively without disturbing the quality originality of the secured message. Thus, cryptography is concerned with the mathematical techniques which can propose secure communications in the occurrence of malicious hackers. Only sender and receiver know the plain text by the simple crypto system.

A. Role Based Proxy Decryption Process

Decryption process is also utilized for security purpose and encrypted data is recovered from original data by using decryption algorithm. The decryption comprises the key for recovering the original data. The decryption process is completely handled by data transmission. If the key is not matched, the data does not decrypt.

- **Key Generation**

Key generation is a primary aim of the decryption. Key generation is utilized the cryptographic tool to create a key which is encompassed with the alpha-numeric sequences.

The software privacy is mainly concentrated on key generation here. If the encryption generates the key, the decryption also produces the same key in the decryption process otherwise data is not decrypted.

Initially, the extraction of data and user attributes are performed, then any two attributes are randomly selected. The AND operation is performed for choosing the attributes. The local key is the resultant value of the AND operation. The local key is executed with exclusive OR (XOR) and the private key is generated. The private key is converted into the secret key by using hashing operation. The user required to retrieve data, their request is transferred to the data owner by the third party provider. The user directly received the secret key form data owner and it applied to decrypt the cipher text which is attained from cloud to get their unique plain text.

- **Key Authentication**

Access of cryptographic key material should be given to the identified communication authority and it is the communication entry between two parties. The two parties can be unilateral or mutual.

- **Key Conformation**

Communication agents should prove the control of authenticated keying material after providing of key conformation by the protocol.

- **Key Freshness**

Creating the unique and new independent generated keys among the different communication agents which grow the security and the process. This is done by key freshness. Generally decryption algorithm robustness is considered according to the subsequent concerns-

- Compression friendliness
- Security
- Format compliance
- Time efficiency

III. LITERATURE REVIEW

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:

In [2] authors have 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 allows anyone to check the validity of cipher texts before they decrypt. The scheme secures proven 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.

In [3] proposed profile matching techniques and secure data sharing in the MHSN cloud computing. However, the social networks and cloud computing were changed via of healthcare to provides the real phase data sharing in cost 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 ciphertext to be authorized in the cloud environment to convert them into new ciphertext of identity based encryption structures without leaked any delicate information by the specialist. Also they provided the matching mechanism of MHSN were based on the identity encryption with the test of equality. It helped the patients to find the networks in the privacy conserving mode and it flexible approval to encrypt the health records with the keywords of guessing attacks. Then the results were protected the data in privacy and security with MHSN.

In [4] authors developed the cloud security with ontology to control, compliances and threat. They have offered 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.

In [5] they 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.

In [6], they gave a survey of existing techniques to the symmetric of the cloud security issues in cloud environment. For the purpose of the cloud experts to shown address client and to measure that where they placed the software security of client service running in the cloud. So 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.

In[7], authors elaborated the security and privacy in cloud computing approaches. They improved security in cloud computing have used the methods of cryptography concepts. But some of the limitations consist in cloud environment for that they offered the homomorphic encryption techniques are used to perform the high level of security, scalable and efficient security in this solutions. Then it required the lengthy computations.

In [8], they 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 minimize of users. Another thing was proposed the traffic shaping algorithm. It converted the user health data collision to non health data collision have such capability to analyzed the traffic attacks to reduced.

IV. PROPOSED METHODOLOGY

The method which is utilized in electronic health record 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 main concern to handle it. Therefore it is explained through a novel proposed algorithm.

The work flow of our proposed algorithm for role based proxy decryption is depicted in fig.1 below.

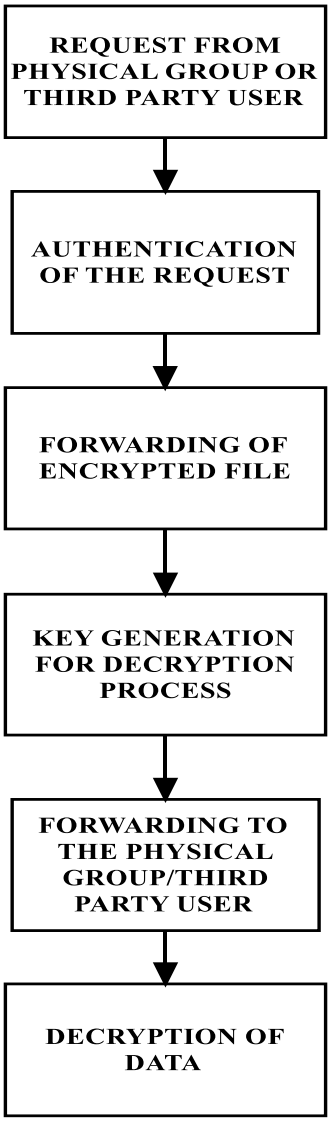

Fig.1. Flow of Role Based Proxy Decryption

Request from the physical group or third party to access the user is given as the input for the decryption algorithm. After the authentication process, encrypted file is forwarded to the user dependent on the role specific model. Public key is generated as per the user request and forward to the physician group. Third parties or physician group can access the data by utilizing the decryption key.

A. Role based Proxy Decryption Proposed Algorithm

In our proposed methodology an identity based encryption technique is utilized for uploading data into the clouds. Identity of the user is extracted initially to generate the public key. Public key is generated by utilizing phone number and email ID. Finally the encrypted data is uploaded to the clouds. Encryption of data is explained through following novel proposed algorithm.

***Input**: Request to access a user*
***Output**: Key and encrypted file*
***Procedure**:*
Step 1: let X be the request from the physician group users or the third party group users and s is set as the patient id.
Step 2: if (requestor ← authenticated)
Step 3: then encrypted file is forwarded to the group user based on the role specific model
Step 4: based on the group user model, the public key for decryption is generated and forwarded to the Physician group user as GP_{Pk}
Step 5:

$$Dec_S = \begin{cases} if\ (P_G == G_{Py})\ ,Then\ decrypt\ (\alpha,\beta,\gamma,Pr_X) \\ if(P_G == G_N),\quad Then\ decrypt\ (\beta,Pr_X) \\ if(P_G == G_{Lb}),Then\ decrypt\ (\beta,\gamma,Pr_X) \end{cases}$$

Step 6: also for the Third party user, generate the public key for decryption and forward to the third party user as GP_{Pk}
Step 7: finally decrypt the data using, $Dec_S = if\ (P_G == TP_G)\ ,Then\ decrypt\ (\delta,Pr_X)$
Where Pr_X *is the private key of the user either the physician group user or the third party user.*

V. IMPLEMENTATION DETAILS

The implementation of our proposed EHR storage model is carried out in the cloud storage for health care systems where each transaction stored on clouds and computed the energy consumption for each transaction. The experimental setup consists of Java and Wamp server. The setup is performed on Intel(R) i3 processor 2.50 GHz running Window x64-based processor with 4 GB of RAM and 1 TB of local storage.

In this work simulation results of existing and proposed algorithms is evaluated and compared. 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 that is relevant to them with the help of some encryption key provided by them. This section provides the performance evaluation of our proposed approach in terms of level-1 decryption, and level-2 decryption. The cost of decryption could also be reduced in this proposed approach which makes the system a much more efficient one.

This section shows the simulation results for proposed work. Here, each and every process of proposed work is explained in this section.

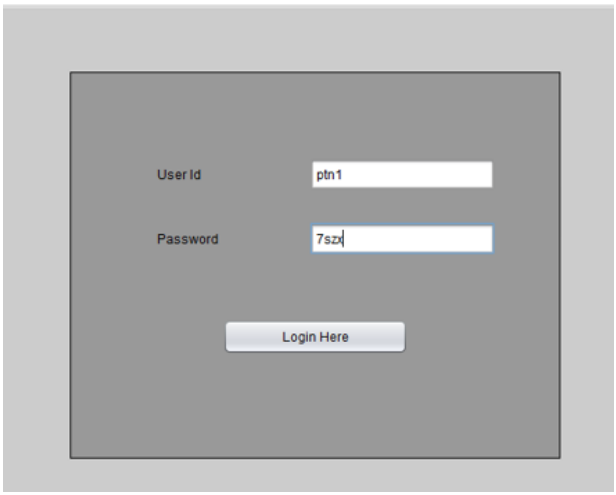

Fig.2 Login GUI Window

Figure 2 shows the login page for users. This windows include user id, password. The user enters unique id and password to login their page. If the user id and passwords are mismatched, then the user can't open their page.

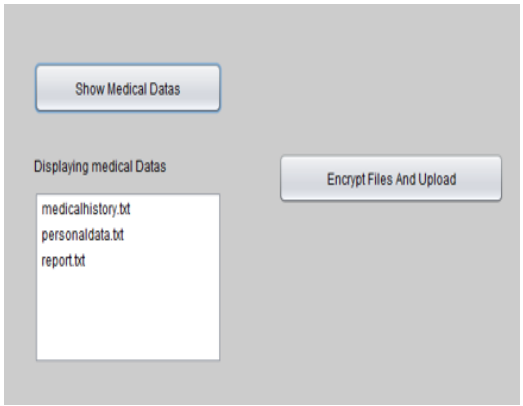

Fig.3. Medical Datasets

Figure 3 shows the medical data for specific user. Here this window includes show medical data, displaying medical data and encrypt files and upload details. If the user clicks the show medical data and it will show the all details in displaying medical data window. If the user encrypted and upload button, then the entire data are encrypted and uploaded in server. Here the encryption process is done for security purposes.

Fig.4. Doctors User Interface

Figure 4 shows the login window for doctors. This window will opened by only doctors. It includes user Id, password and profession. Here the doctor enter all details then login button to open the pages.

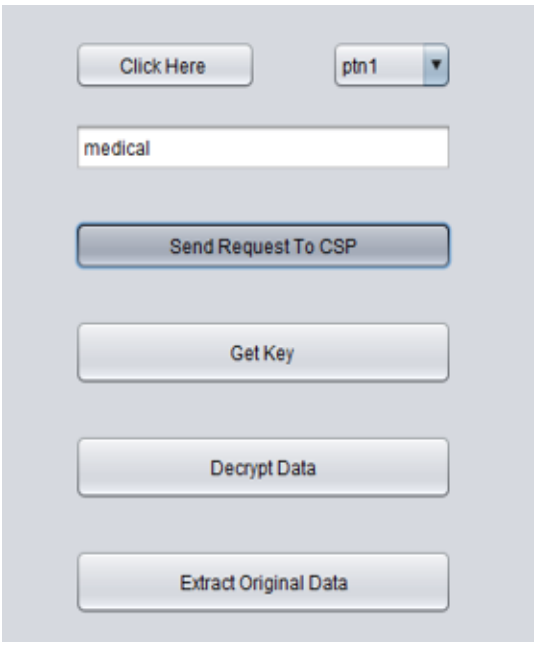

Fig.5. Cloud Service Provider Window

Figure 5 shows the available user data details and it includes click here, send request to Cloud Service Provider (CSP), get key, decrypt data and extracted original data. Initially, the doctor sends the request to Cloud Service Provider (CSP). So the doctors select the user and click send request to Cloud Service Provider (CSP).

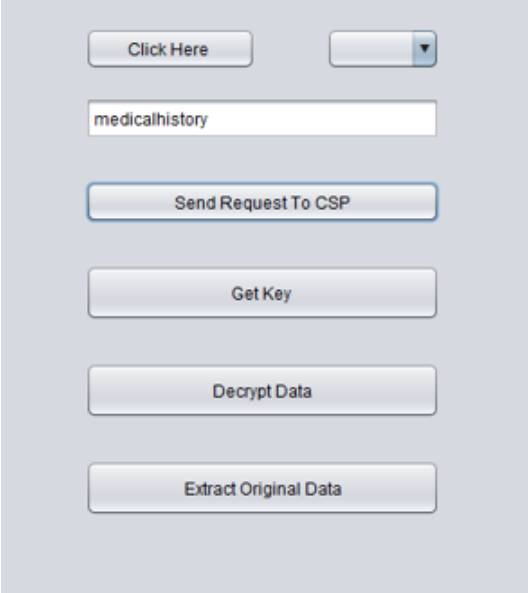

Fig.6. Request Window to Cloud Service Provider

Figure 6 shows the user details which are retrieved from cloud server. Initially, the doctor sends the request to Cloud Service Provider (CSP) and get key form sever. Then, the doctor enter the user Id and key details, if both are same then, the data will decrypt and extract the original data. Otherwise, the doctor can't decrypt the data from Cloud Service Provider (CSP).

A. Performance Analysis of Decryption Level-II Cost

The performance analysis of decryption level-II checking cost for different data size is discussed and presented. Table 1 shows the performance analysis of checking decryption cost for different data size of the proposed scheme with existing schemes.

Table 1. Performance Analysis of Decryption Level-II Cost* 10^5

Decryption Cost* 10^5					
Data (in GB)	**GA07B**	**LZD**	**WCW**	**IBPRE**	**Proposed**
1	0.01	0.01	0.01	0.01	0.009
100	0.05	0.1	0.01	0.1	0.009
500	0.1	0.4	0.3	0.3	0.09
1000	0.2	0.6	0.5	0.5	0.1

The above table 1 shows the performance analysis of decryption checking cost level-II for different data size such as 1 GB, 100 GB, 500 GB, 1000 GB. Here four existing methods such as GA07B, LZD, WCW and IBPRE are utilized for validating and comparing of simulation results to our proposed method. Besides it the size of data range from 1 GB to 1000 GB is used for analyzing the performance of our proposed approach.

For 1 GB data size, the existing GA07B along with LZD, WCW, IBPRE has taken time 0.01 ms to process the 1 GB data whereas our proposed approach takes time 0.009 ms only. For 100 GB data size, the existing GA07B takes much time than the LZD, WCW, IBPRE whereas our proposed approach takes time 0.009 ms only. For 500 GB data size, the existing LZD takes much time than the three ones whereas our proposed approach takes less time 0.09 ms. Similarly, for 1000 GB data size, the existing LZD takes much time than the GA07B WCW, IBPRE whereas our proposed approach takes very less time 0.01 ms only. From the obtained results, it is observed that the proposed method achieves better performance than the existing methods. The graphical representation of this performance evaluation of decryption level-II checking cost for different data size is depicted in figure 7.

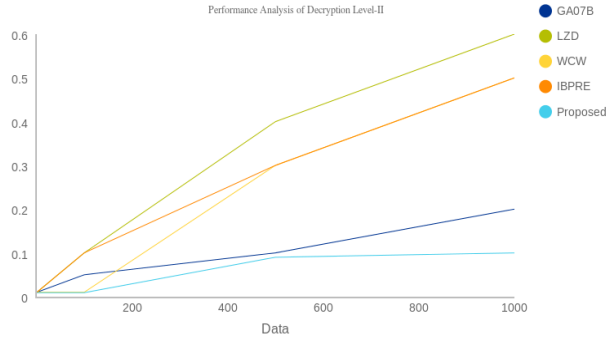

Fig.7 Performance Analysis of Decryption Level-II

Therefore the accuracy of execution time for each method is shown in figure 8.

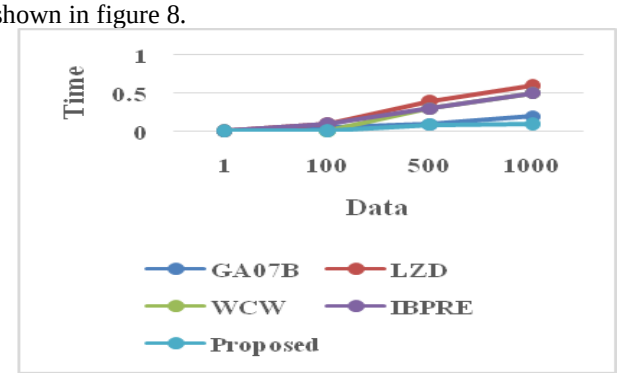

Fig.8. Accuracy of Time selected Methods

VI. CONCLUSION

In this paper, cryptography methods are utilized for privacy, security and reliability with e-health cloud system through cloud storage systems. Several methods of e-health, decryption framework and personal health records are analysed in a detailed way. Here we proposed a scheme as role based proxy decryption approach supported the delegate of decryption rights to user's revocation. This paper provides the performance evaluation of our proposed approach in level-2 decryption by using role based proxy decryption. The energy consumption in decryption for each transaction could be reduced in our proposed system that makes the system more efficient one. The ultimate aim of this paper is to secure the intimate patient information by deploying electronic health record data and providing better security in electronic health records using two levels decryption. In this method proxy decryption method is presented to extract the data and again the decryption process is controlled to extract the original data with the help of public key. So, the medical data about the patient could be safely and securely retrieved using the electronic health records.

REFERENCES

1. Vikas Bajpai, “The Challenges Confronting Public Hospitals in India, Their Origins, and Possible Solutions,” Advances in Public Health, Vol. 2014, Article ID 898502, 27 pages, 2014.
2. Li J, et. al, ‘Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing’, Computers & Security, Vol. 72, 2018.
3. Huang Q, et. al, ‘Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing’, IEEE, Vol. 6, 2018.
4. Kalaiprasath R, et. al., ‘Cloud. Security and Compliance- A Semantic Approach in End to End Security’, International Journal of Mechanical Engineering and Technology (IJMET), Vol. 8, No.5, 2017.
5. Luna J, et. al., ‘Quantitative Reasoning about Cloud Security Using Service Level Agreements’, IEEE Transactions on Cloud Computing, Vol. 5, No. 3, 2017.
6. S. A. Aljawarneh et. al., "A conceptual security framework for cloud computing issues," International Journal of Intelligent Information Technologies (IJIIT), Vol. 12, 2016.
7. Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, "Security and privacy in cloud computing: Vision, trends, and challenges," IEEE Cloud Computing, vol. 2, pp. 30-38, 2015.
8. Q. Shen, X. Liang, X. S. Shen, X. Lin, and H. Y. Luo, "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, pp. 430-439, 2014.
9. Shadab Ahmed, Manoj Singh, Arvind K Sharma, Mobile Cloud Computing: Issues and Applications, IJCST Vol. 8, Issue 4, 2017