iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30580

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Enabling Authorized Encrypted Search for Multi-Authority Medical Databases using 3DES

Ajinkya Dongare[1], Suchitra Theurkar[2], Manjushri Sonkamble[3], Varsha Rodge[4], Mr. Ramkrushna Maheshwar[5]
[1, 2, 3, 4, 5]*International Institute of Information Technology, Pune*

Abstract: ***E-medical systems play a quite essential role in the digital transformation of health care record, which allows a patient or the user to create, manage, and control its private Personal Health Record (PHR) through the internet [1][2]. Most of the E-Medical record services are outsourced to a third-party that is public cloud. However, such outsourcing of data may lead to a variety of privacy and security related issues because of the risk of information leakage. To avoid such problems, we are developing systems in which data will be encrypted using 3DES algorithm before uploading to the cloud. Subsequently, only the authorized client who has the key or permissions can decrypt the data. E-Medical records are basically sensitive and should be stored in database in encrypted form. Once medical records are encrypted and outsourced, the cloud server can no longer perform keyword search, because the server is not expected to obtain any information about the records. Hence, the goal of the project is to provide security to personal health records where data needs to be kept private.***

Keywords: Multi-Authority; Encrypted Data using 3DES Algorithm; Personal Health Records; E-medical System; Third Party Auditor; Cloud Storage; Forward Security;

I. INTRODUCTION

In medical field, the database reports are sensitive, so there is a need to secure it and provide a strong privacy so as to avoid illegal access to the information [2]. When we upload the PHR record on the cloud there is a chance of data leakage, so to avoid this malicious attacks on the personal data we need to provide a strong security, proper authentication and also provide an end-to-end encryption to the information so as to secure our Personal Health Records containing private information to only those who has authority to access data [4]. The aim is to build a system which will be capable of securing and storing private Personal Health Record(PHR) in E-Medical System [1][10]. We are developing systems in which data will be encrypted using 3DES (Data Encryption Standard) algorithm before uploading to the cloud. Subsequently, only the authorized client who has the key or permissions can decrypt the data. E-Medical records are sensitive and should be stored in database in encrypted form. So, basically the purpose of the project is to provide security to personal health records where data needs to be kept secure with the help of Triple DES algorithm.

II. LITERATURE REVIEW

We have referred "Enabling Authorized Encrypted Search for Multi-Authority Medical Databases" [1], where they have performed the encryption and decryption using RSA algorithm. In which the multi-authority dynamic searchable encryption system is created, which provides fine-grained access control on encrypted PHRs stored through outsourced storage services [3]. The features of the proposed system can be summarized as follows: Multi-Authority- Their system supported encrypted data search under scenarios in which all data records are encrypted by multiple authorities. Multi-Client- Due to the use of attribute-based encryption, this work satisfies multi-client requirement as well. Because all search capabilities are encrypted under an access policy before being sent to the clients, only the allowed clients with corresponding attributes can obtain a valid search token [5]. In fact, the client side is controlled by providing different search capabilities for authorized keywords. Non-interactive-Their system also provided an efficient approach to enable non interactive authorized search. Forward Privacy- Because of the dynamic setting, their design also supported forward privacy such that a supporter or server will not know the relationship between the updated keywords and documents present [1]. Currently, researchers are more focused on exploring practical and secure properties for encrypted data search on a large scale [6]–[8].

In this paper we have included Triple DES algorithm. It is proved to be much more secured than RSA and DES (Data Encryption Standard) algorithms. Triple Data Encryption Standard Algorithm is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. The Data Encryption Standard's (DES) 56-bit key. Nevertheless, a more secure encryption is produced by an adapted version of DES, Triple DES (3DES) using the same algorithm. Hence 3DES provides more security providing no room for unauthorized users due to function of encrypting and decrypting thrice, with three different keys.

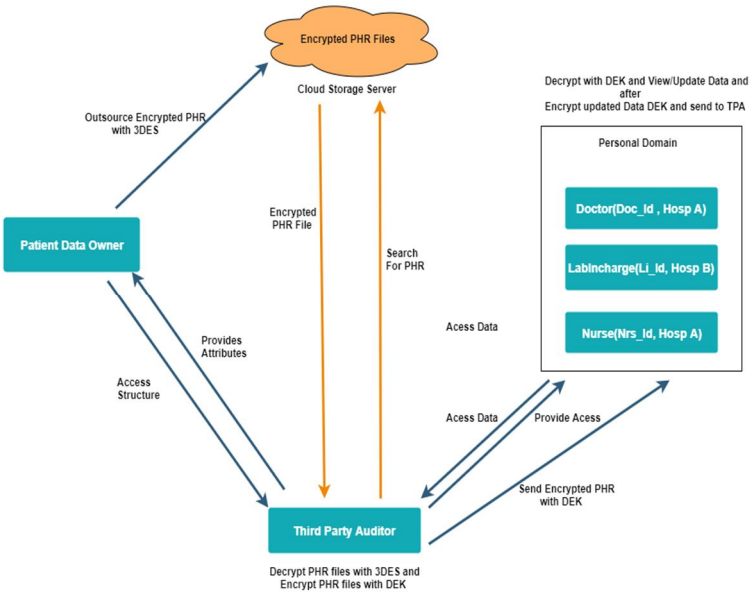


Fig.1. Architecture Diagram

A dynamic searchable encryption scheme consists of the following three polynomial algorithms among a data owner, a client and a server [9]. Input: Patients share their PHA (Personal Health Records) containing data which is encrypted by 3DES. Output: Doctors/Nurse gets the encrypted PHA (Personal Health Records) containing data and can decrypt it by download option and view it easily. Functions: Identify data structures, classes, divide and conquer strategies to exploit distributed/parallel/concurrent processing constraints. Our system works in a distributed manner. It means one module is dependent on another module. The output of previous module is required as an input to the next module.

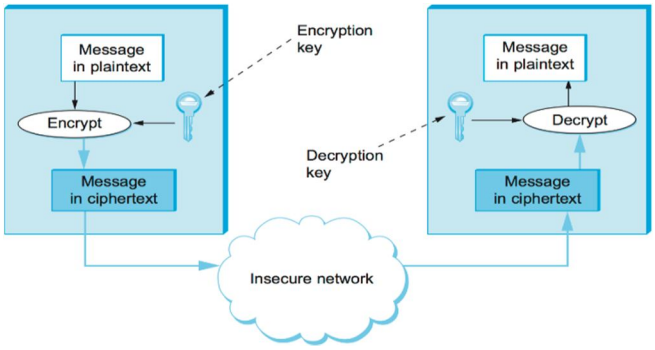


Fig. 2. Encryption and Decryption Process using keys

A. Algorithm of 3DES

In cryptography, **Triple DES** (**3DES** or **TDES**), officially the **Triple Data Encryption Standard Algorithm** is a symmetric-key block cipher which is published by the National Institute of Standards and Technology (NIST), which applies the DES cipher algorithm three times to each data block. Triple DES uses a "key bundle" that specifically comprises of three DES keys which are K1, K2 and K3, each of 56 bits. It is proved to be more secured than RSA and DES (Data Encryption Standard) algorithms. The Data Encryption Standard's (DES) 56-bit key is not considered as enough in the face of modern cryptanalytic techniques and supercomputing power any longer. Nevertheless, a more secure encryption is produced by an adapted version of DES, Triple DES (3DES) using the same algorithm. Hence 3DES provides more security providing no room for unauthorized users due to function of encrypting and decrypting thrice, with three different keys.

The encryption algorithm is:

Cipher text = Encrypt K3 (Decrypt K2 (Encrypt K1 (Plain text))).

That is, DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

The decryption algorithm is:
Plain text = Decrypt K1 (Encrypt K2 (Decrypt K3))
Plaintext = DK1(EK2 (DK3 {Cipher text}))

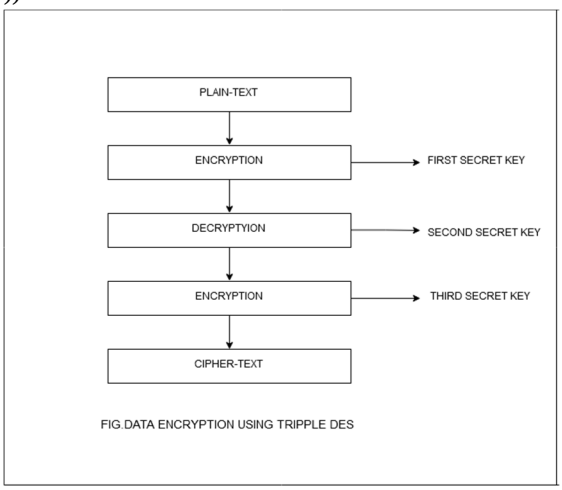


Fig. 3. Encryption Process in 3DES

B. Steps for Output

1) Creating a database of the information, the backend regarding the user and the admin (patient and doctor/nurse) who has the access.
2) Creating a GUI which consists of dashboard displaying the login and registration of the doctor and the patient.
3) Encryption and decryption process using the TPA (third party auditor), Cipher text algorithm and triple DES.
4) Final view of the project as an application for enabling access to multi-authority in the medical database.

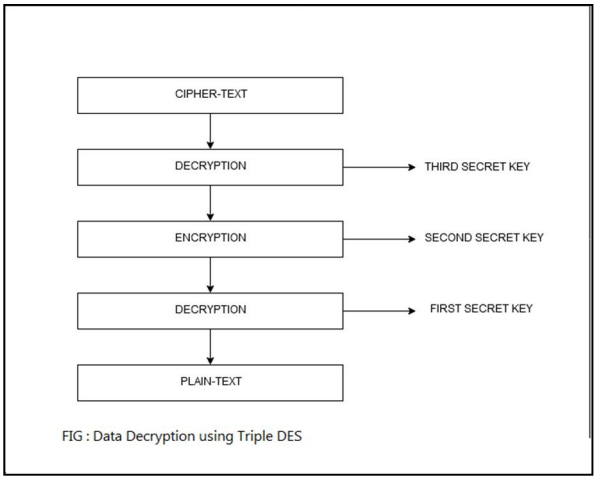


Fig. 4. Decryption Process in 3DES

C. Advantages of 3DES

Triple DES runs three times slower than DES, but is much more secure than RSA and DES algorithms. The procedure for decryption is the same as the procedure for encryption hence it is easier, except that the decryption is executed in reverse. It is symmetric key block cipher. Also, same key is used for encryption and decryption process. Due to its Feistel structure and not simple logic, DES is easier to comparatively implement. It is hugely secure due to three different keys used for encryption and decryption process.

D. Limitations of 3DES

Triple DES runs three times slower than DES. The main disadvantage of DES is that, it is broken using brute-force search. However, using 3DES reduces this issue at the cost of increasing execution time. DES is also weak and helpless when attacked using linear cryptanalysis. However, in this manner it completely takes 247 known plaintexts to break DES algorithm.

III. PROPOSED SYSTEM

In medical field, the medical database reports are extremely sensitive hence, there is a need to secure it and provide a strong privacy so as to avoid illegal access to the information. When we upload the PHR record on the cloud there is a chance of data leakage, so to avoid this malicious attacks on the personal data and health records we need to provide a strong security, proper authentication and provide an end-to-end encryption to the information to only those who has authority to access data. As a result, only the authorized person is able to access the information available and the data is kept secured.

To avoid all these conditions its necessary that our system is perfectly working as expected. To implement a system that can solve the security related problem. Our system will be able to solve problems due to which there would not be any hacking scenes. Due to the security provided by Triple DES algorithm, the information is end-to-end encrypted and cannot be accessed by any unauthorized users or steal any data by unfair means. By implementing the encryption and decryption process using the TPA (third party auditor) and triple DES.

A. Model Building

Firstly, the complete model of the system is made containing the GUI of the system which includes the dashboard of home page containing doctor login and patient login primarily.

B. Input

Input is the concerned with the doctors and patient information which is necessary to access to their login and to work on the system. So firstly, the doctor login of various doctors for different specifications related to the type of diseases or illness. Later the patient login who are interested to get appointment and consult the doctors for their personal illness or related purpose.

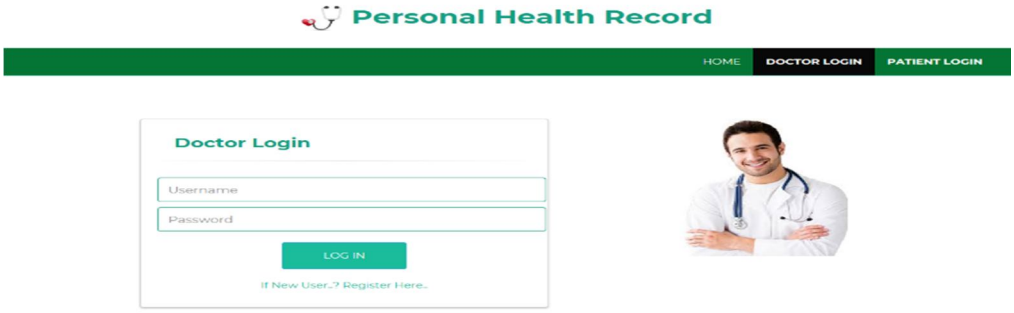


Fig.5. Doctor login

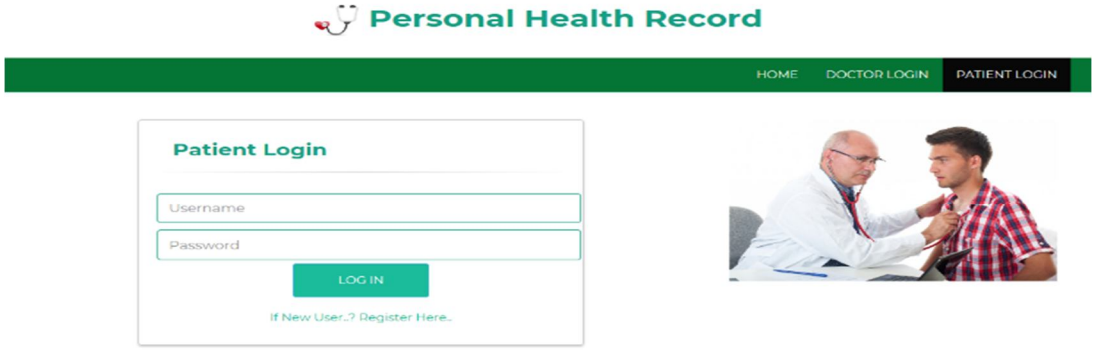


Fig.6. Patient login

C. Selection Phase

In this process, after having the database of all the doctors the patient can login and select the doctor he/she wants to consult to.The patients can share their past health reports and apply for an appointment to meet the doctor. Also only the doctors who gets the patients report can download and access it and suggest the change in medications or any kind of useful information on through reports which will be end to end encrypted to those two itself. No other users oreven the doctors can access those personal health reports without authority.

Fig.7. Patient upload report

Fig.8. Patient can view and share report with the doctor

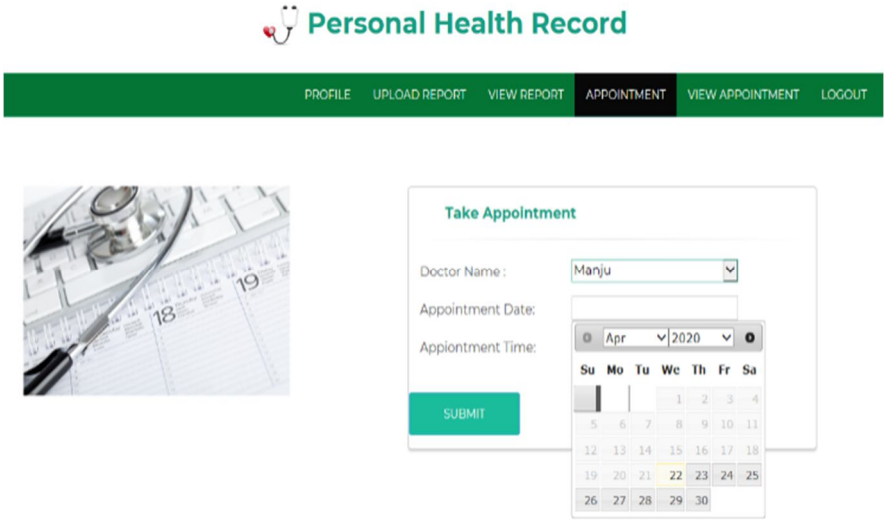


Fig.9. Patient can take appointment and visit accordingly

D. Working phase

When the doctors receive the appointment request, either he can confirm or reject depending on his work and timings. Also, the doctor can access the patients PHR which are shared by the patients and are authorized to give suggestions or prescription after the meeting to the concerned patient. This report of information send will also be end to end encrypted by 3DES algorithm. The compete file is encrypted and can be decrypted on by the authorized person.

Fig.10.Doctor can download and access the report and add and view prescription.

IV. RESULT AND DISCUSSION

Our main outcome is providing overall security and storing private Personal Health Record(PHR) in E-Medical System, we have successfully implemented authorized encrypted search for the various personal health records which provides data security using Triple DES algorithm. We demonstrated how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the E-medical system. By implementing the different functionalities stated above such as the 3DES using the TPA (Third Party Auditor) and other services, we try to increase efficiency of our resources.

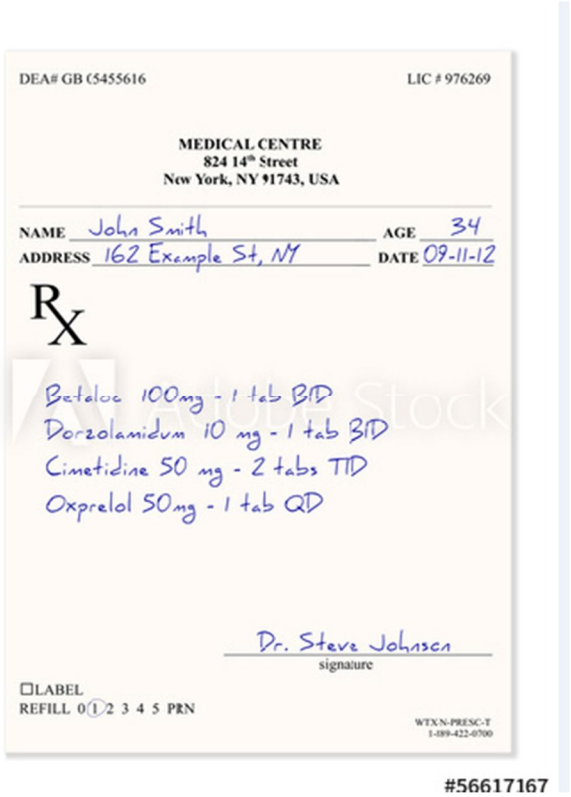


Fig.11.Before Encryption of PHR using 3DES

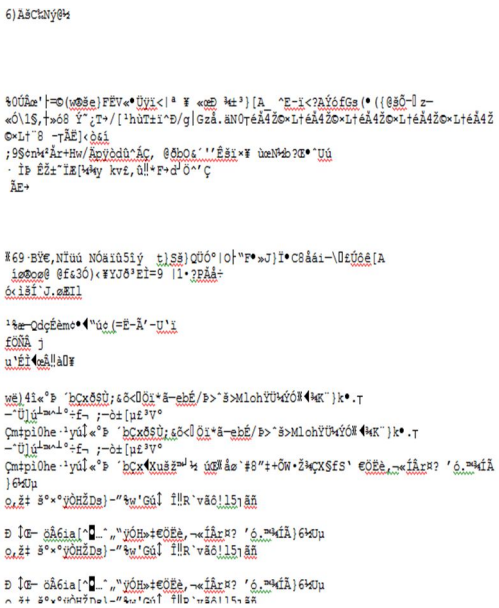


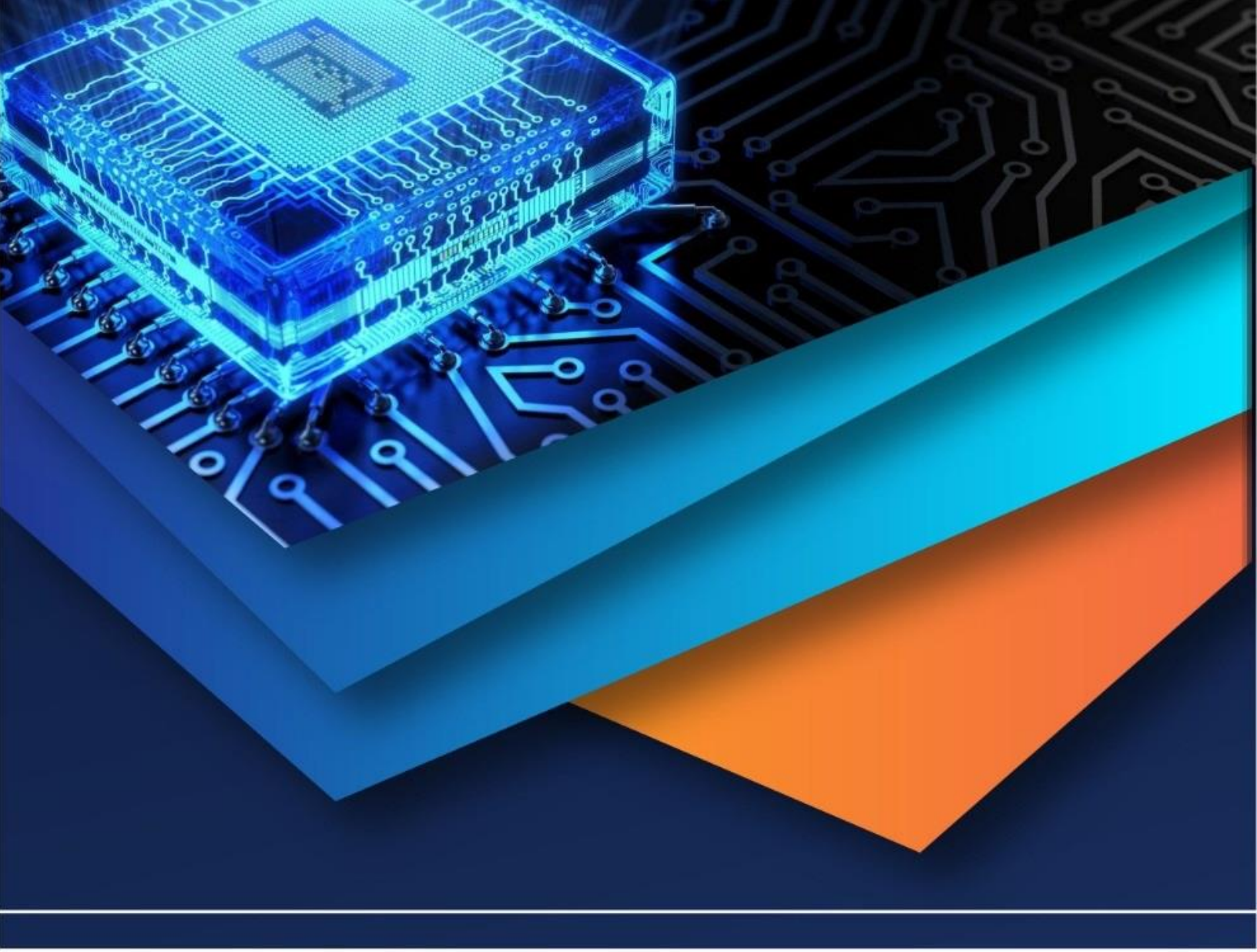
Fig.12. After Encryption of PHR using 3DES

V. CONCLUSION AND FUTURE WORK

The aim is to build a system which will be capable of securing and storing private Personal Health Record (PHR) in E-Medical System. In this system, we have tried to implement authorized encrypted search for the various personal health records which provides data security using Triple DES algorithm. We proposed an efficient and secure data retrieval method for securing our medical record and privacy. The data is secured due to the 3DES algorithm encryption and decrypting it using 3 different keys and hence the problem of confidentition and privacy is resolved. We demonstrated how to apply the proposed mechanism to securely and effiefficiently manage the confidential data distributed in the E-medical system. In Future we are trying to provide more security to our system which can encrypt huge. In future we will try to develop mobile application and run it on different systems. Also, there is a scope and need of such security in the fields of business, banks and even in stock market related works.

REFERENCES

[1] Lei Xu, Shifeng Sun, Xingliang Yuan, Joseph K. Liu, Cong Zuo, Chungen Xu*, “Enabling Authorized Encrypted Search for Multi-Authority Medical Databases”, Citation information: DOI 10.1109/TETC.2019.2905572, IEEE Transactions on Emerging Topics in Computing.IEEE ,2019.
[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.
[3] J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute based signcryption,” Future Generation Computer Syst., vol. 52, pp. 67–76, 2015.
[4] S. Lai, S. Patranabis, A. Sakzad, J. K. Liu, D. Mukhopadhyay, R. Steinfeld, S.-F. Sun, D. Liu, and C. Zuo, “Result pattern hiding searchable encryption for conjunctive queries,” in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 745–762.
[5] S. K. Kermanshahi, J. K. Liu, and R. Steinfeld, “Multi-user cloud based secure keyword search,” in Proc. of 22nd Aus. Conf. on Inf. Security and Privacy, 2017, pp. 227–247.
[6] X. Yuan, H. Cui, X. Wang, and C. Wang, “Enabling privacy-assured similarity retrieval over millions of encrypted records,” in Proc. of 20th Eur. Symp. on Research in Comput. Secur., 2015, pp. 40–60.
[7] X. Yuan, X. Wang, C. Wang, C. Yu, and S. Nutanong, “Privacypreserving similarity joins over encrypted data,” IEEE Trans. Inf. Forensics Secur., vol. 12, no. 11, pp. 2763–2775, 2017.
[8] C. Zuo, J. Macindoe, S. Yang, R. Steinfeld, and J. K. Liu, “Trusted boolean search on cloud using searchable symmetric encryption,” in Proc. of 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 113–120.
[9] R. Bost, “Poφoς: Forward secure searchable encryption,” in Proc. of the 2016 ACM SIGSAC Conf. on Comput. and Commun. Secur., 2016, pp. 1143–1154.
[10] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private information retrieval,” in Proc. of 36th Annu. Symp. on Foundations of Comput. Sci., 1995, pp. 41–50.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY