CLOUD DATA SECURITY MODEL USING MODIFIED 
DECOY TECHNIQUE IN FOG COMPUTING FOR E-
HEALTHCARE

Dr. P. Maragathavalli¹, S. Atchaya², N. Kaliyaperumal² and S. Saranya²
¹Assistant Professor, Department of Information Technology, Pondicherry Engineering College, 
East Coast Road, Pillaichavadi, Puducherry, ¹marapriya@pec.edu
²Student Member, Department of Information Technology, Pondicherry Engineering College, 
East Coast Road, Pillaichavadi, Puducherry.
²atchaya5899@pec.edu

Abstract In recent years, the cloud provides the facility of storing the possible files to 
a remote database which can be retrieved on demand. Healthcare cloud infrastructure is 
used to store the medical records which in turn help in managing and tracking the 
records of the user. The primary care providers use Electronic Medical Record (EMR) 
for diagnosing and evaluating medical data. Big data analytics is an important 
technology in enormous business areas which includes banking, social media, machine 
sensor data and medical welfare. Healthcare cloud provides various storage facilities 
such as Google drive, dropbox business and one drive in which security issues like data 
theft attacks to be considered as the serious security breaches of the cloud. In this paper, 
a modified decoy technique is proposed in order to ensure more security for the user’s 
Medical Big Data (MBD). The tri-party authentication key uses key agreement protocol 
which is modelled by bilinear pairing cryptography. The proposed system detects the 
attacker and sends the information such as IP address, access time and date to the user. 
It also provides the facility to block the account from further access. Using the triple-
des algorithm in bilinear pairing the parameters like throughput is increased and 
computational complexity is decreased.

Keywords: Remote Database; Security and Privacy; Medical Big Data Analytics; 
Electronic Medical Record; Key Agreement Protocol.

1. INTRODUCTION
Hybrid cloud for healthcare data sharing and accessing facilities is provided to store the medical records 
of the patients. It also helps in managing the users record and tracking the records of them, even if the 
patient moves across any part of the world [3]. It has several security issues such as privacy and security,
policy issues, transparency, data protection, and licensing. To achieve a secure healthcare cloud fog computing and cloud is used in our proposed methodology in the users Medical Big Data (MBD)[2].

This paper sections are ordered as follows: The literature survey is described in section II. The proposed methodology with design, coding and implementation in section III. Section IV describes the input and output specification. Implementation environments are described in section V, performance parameters in section VI and the conclusion of this paper is concluded section VII.

2. LITERATURE SURVEY

Medical big data analysis: preserving security and privacy with hybrid cloud technology [1] has provided various mechanisms and algorithms for the security of the cloud. Analysing the several techniques it provided the alternative security model using bilinear pairing protocol. In this proposed model the parameters like computational complexity is considered in which in the result it decreases by 20%. The limitation in the proposed work is time consumption which is high.

Lightweight and privacy and medical service access for healthcare cloud [4] which uses Attribute Based Signature (ABS) technology to overcome the above limitations. By providing the stronger security model it focuses on the time consumption which in the result reduces the response time by 0.25s. The proposed system has some limitations which it is suitable for small scale medical access.

Improving security and privacy attribute-based data sharing in cloud computing technology [5] has provided various mechanisms and algorithms for the security of the cloud. Analysing the several techniques it provided the alternative security model using Ciphertext policy- Attribute based encryption (CP-ABE). In this proposed model the parameters like computational overhead is considered in which in the result it decreases by 40%. The proposed work provides the weak security model.

A novel smart healthcare design, simulation and implementation using healthcare using 4.0 processes [6] has provided various mechanisms and algorithms for the security of the cloud. Analysing the several techniques it provided the alternative security model using Blockchain which uses the existing dataset. In this proposed model the parameters like time consumption is considered in which in the result it reduces by 1s. The proposed work has the limitation in adding the additional features to the system.

Secure verifiable database supporting efficient dynamic operations in cloud computing [7] has provided various mechanisms and algorithms for the security of the cloud. Analysing the several techniques it provided the alternative security model using BLS signature which uses the existing dataset. In this proposed model the parameters like time throughput is considered in which in the result the throughput is increased by 20%. The proposed work has the limitation in which the pairing is not efficient.

In the above paragraphs, the literature survey is done from an existing system which has some limitations in time consumption, pairing, weaker security model and those limitations are considered in our project.

3. PROPOSED METHODOLOGY

Decoy technique helps in generating the decoy files or the duplicate medical records and detects unauthorized users with the help of user profiling. It also helps in securing users’ medical records by confusing the attacker with a decoy gallery.

3.1 Design

The proposed system focuses to keep Original Medical Big Data (OMBD) secret by user profiling the attacker is detected and Decoy Medical Big Data (DMBD) is used as a honeypot. DMBD data is secured by pre-existing values and an efficient tri-party authentication key is proposed.

In this method initially both the user and attacker will be accessing the DMBD and they are considered as the unauthorized users. This DMBD is placed in the fog computing layer near user profiling and it contains the fake Medical Big Data (MBD) which makes the attacker believe that they are accessing the OMBD. When the user gets to know that it is not his profile he will be going to the next process of verification and after passing some security challenges he will be accessing the OMBD. By user profiling the attacker is detected and SMS is sent to the user that his account is being accessed and it contains information like access time, date and IP address.
Now if the user wants to upload his medical records for this the tri-party needs to be communicated. The secret key is generated from the Private Key Generator (PKG) and it is received by the tri-party. Now each party authenticates with another party to communicate with others secretly. Then the medical records are encrypted using the triple-des algorithm. These encrypted data are stored in the cloud and again decrypted for viewing purposes using this algorithm.

Thus the two level security is proposed firstly DMBD as the honeypot and the other by keeping the encrypted medical record in the cloud secretly Fig.1 shows the proposed system.

![Fig. 1 Proposed System Design](image)

3.2 Coding and Implementation

User profiling and decoy technique detects abnormal patterns such as login count, download data, security failure questions.

The pseudo-code for user profiling and decoy technique is given below:

**Step 1:** Calculate the user login count, cntLoginFail increase.

**Step 2:** Check the downloaded datas, cntDataDownload increase.

**Step 3:** Count the security failure question, cntSecQueFail increase.

**Step 4:** IF cntLoginFail > 3 && cntDataDownload > 3 && cntSecQueFail > 3 && Key matches. If the above condition is passed then the user is an attacker or a normal user.

**Step 5:** Send the information to the user.

**Step 6:** Block the attacker.

3.3 Encryption

When the user uploads the medical record, the encryption process is done. The medical record is encrypted by asymmetric encryption technique Triple DES with the secret key that is generated by the private key generator (PKG). Now the original record is converted into the cipher image. This encrypted cipher image is kept securely in the cloud storage with the help of a cloud service provider which is shown in Fig. 2.
3.3.1 Changed pseudo-code for encryption

cipherimage64bits = Encrypt(64bitimagelst,i)
cipherimage64bits = Decrypt(64bitimagelst,j)
cipherimage64bits = Encrypt(64bitimagelst,k)
cipherimage64bits = Inverse(Finalpermutation(cipherimage64bits))
for cimage in cipherimage
64bits:cipherimage = cipherimage + cimage
Output: cipherimage

3.4 Decryption

Decryption is the process of converting encrypted data into the plain text. The cipher image stored in
the cloud service provider is decrypted into the original data with the secret key which is generated by
the private key generator and the original data is available to the user is shown in Fig. 3.

3.4.1 Modified pseudo-code for decryption

cipherimage64bits = Decrypt(64bitimagelst,i)
cipherimage64bits = Encrypt(64bitimagelst,j)
cipherimage64bits = Decrypt(64bitimagelst,k)
image64bits = Inverse(FinalPermutation(image64bits))
for image in image
64bits: imager=image + image
Output: imager

4. INPUT – OUTPUT SPECIFICATION

4.1 Input specification

- Input data – plain medical image
4.2 Output specification

- Output data – plain medical image (after decryption)
- Format for each output data – cipher text

The input-output specification is shown in Fig. 4.

![Orginal Image](image1)
![Encrypted](image2)
![Decrypted](image3)

Fig. 4 Input and Output Data Processing

5. IMPLEMENTATION

5.1 Data set description

The Multimedia Dataset of 128MB with 150 entries is used as an input to this project. The multimedia dataset is converted into cipher text which is used as input data for this project. The output of our project is also a cipher text.

URL: [https://www.kaggle.com/kmader/siim-medical-images](https://www.kaggle.com/kmader/siim-medical-images)

5.2 Hardware Requirements

- Processor: 64 bit, 1.5 GHZ minimum per Core
- RAM: 2GB minimum
- Hard disk: 10GB

5.3 Software requirements

- Real time SMS provider: MYSMSMANTRA
- Front end: Python 3.8
- Back end: SQL Server

5.4 Implemented code for encryption using Triple DES
Based on the following comparisons, the triple des algorithm gives a better throughput, computational complexity and time consumption as a result triple-des is the best algorithm which is used in our proposed system.

### 6.1 Throughput

The throughput is done for the encryption and decryption and proposed system is compared with the existing system. Throughput is estimated by the average number of data blocks that transfer successfully to the time taken which is measured by bits per second (bps).

\[
\text{Throughput} = \frac{\text{Number of data blocks successfully transferred}}{\text{Time taken}}
\]

Throughput is increased by 20% since the data transfer in encryption by using the triple des algorithm provides efficiency in throughput whereas encryption by blowfish increases by 10% only.
6.2 Computational complexity
Computational complexity is the amount of time taken by the process. It is estimated by the number of bilinear pairing cryptography which is shown in below equation,

\[ B(n) = O(n^2) \]

Where B(n) is a bilinear pairing function and O(n^2) is a complexity analysis function. Complexity time taken for bilinear pairing is reduced by using secret key and tri party authenticate key when compared to the existing system it is reduced by 10%.

6.3 Time consumption
The time consumption is the process of time required to complete the key generation.

\[ \text{time consumption} = \frac{\text{Amount of time taken for individual key size}}{\text{Total rate of the time consumption}} \]

Time consumption is calculated with respect to the key size generated in bilinear pairing cryptography and time consumption is reduced by 25% by using triple des algorithm than blowfish algorithm.

7. CONCLUSION
A cloud data security model is developed for protecting the patient’s information in the EHR system by fog computing in which two levels of security have been provided. By user profiling the attacker can be detected in that decoy gallery as the honey pot. The Original Medical Big Data (OMBD) is maintained secretly in cloud storage and Decoy Medical Big Data (DMBD) in fog computing layer. When a user wants to access the OMBD needs verification. Thus, by storing the OMBD as the hidden gallery, OMBD becomes secure. For communication between OMBD and DMBD, a Private Key Generator (PKG) is used. By using the proposed methodology, the throughput can be increased by 20% as well as the computational complexity and time can also be reduced significantly than the existing techniques.

8. REFERENCES
[1] Shanmugapriya. E and Kavitha.R. “Medical big data analysis: preserving security and privacy with hybrid cloud technology”, Soft Computing, Springer 23, 2585–2596 (2019). https://doi.org/10.1007/s00500-019-03857-z.
[2] M. Joshi, K. Joshi and T. Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 932-935, doi: 10.1109/CLOUD.2018.00139.
[3] M. Du, K. Wang, X. Liu, S. Guo and Y. Zhang, "A Differential Privacy-Based Query Model for Sustainable Fog Data Centers," in IEEE Transactions on Sustainable Computing, vol. 4, no. 2, pp. 145-155, 1 April-June 2019, doi: 10.1109/TSUSC.2017.2715038.
[4] J. Liu, H. Tang, R. Sun, X. Du and M. Guizani, "Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud," in IEEE Transaction on Dependable and secure computing, vol. 7, pp. 106951-106961, 2019, doi: 10.1109/ACCESS.2019.2931917.
[5] L. Zhang, Y. Cui and Y. Mu, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," in IEEE Systems Journal, vol. 14, no. 1, pp. 387-397, March 2020, doi: 10.1109/JSYST.2019.2911391.
[6] Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover and E. Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes," in IEEE Transaction on Dependable and secure computing, vol. 8, pp. 118433-118471, 2020, doi: 10.1109/ACCESS.2020.3004790.
[7] J. Shen, D. Liu, M. Z. A. Bhuivyan, J. Shen, X. Sun and A. Castiglione, "Secure Verifiable Database Supporting Efficient Dynamic Operations in Cloud Computing," in IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 2, pp. 280-290, 1 April-June 2020, doi: 10.1109/TETC.2017.2776402.
[8] Abouelmehdi. K, Beni-Hessane. A and Khaloufi. H, “Big healthcare data: preserving security and privacy.” Big Data 5, 1 (2019). https://doi.org/10.1186/s40537-017-0110-7
[9] Mithun Mukherjee; Mohamed Amine Ferrag; Leandros Maglaras; Abdelouahid Derhab; Mohammad Aazam, "Security and Privacy Issues and Solutions for Fog,” in Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics, Wiley, 2020, pp. 353-374, doi: 10.1002/9781119501121.ch14.

[10] Claudio A. Ardagna, Rasool Asal, Ernesto Damiani, “From Security to Assurance in the Cloud: A Survey”, Publication: ACM Computing Surveys, July 2019, Article No.: 2, https://doi.org/10.1145/2767005.

[11] Lahar Singh Nishad, Akriti, Sarvesh Kumar and Sumitra Beniwal, “Security, Privacy Issues and challenges In Cloud Computing: A Survey” ICTCS ’16: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, March 2019, Article No.: 47, Pages 1–7, https://doi.org/10.1145/2905055.2905253.