# Privacy preserving on personalized medical data in cloud IoT using Extended Fully Homomorphic Encryption

**Pradeep Bedi**
GEHU: Graphic Era Hill University
**S B Goyal** ( drsbgoyal@gmail.com )
City University of Malaysia https://orcid.org/0000-0002-8411-7630

**Research Article**

**Keywords:** Medical data, Cloud Computing, Internet of Things (IoT), Homomorphic encryption

**Posted Date:** May 17th, 2022

**DOI:** https://doi.org/10.21203/rs.3.rs-1630013/v1

# Privacy preserving on personalized medical data in cloud IoT using Extended Fully Homomorphic encryption

Pradeep Bedi[a] , S B Goyal[b]

[a] Graphic Era Hill University, Dehradun, INDIA, bedipradeep@gmail.com

[b] City University, MALAYSIA, drsbgoyal@gmail.com

Abstract: -Transition of healthcare to digital platforms is necessary for the present era to provide a better diagnosis with reduced operational cost. Digital platform makes the patient data available in an appropriate time. Cloud computing in health care applications senses the data through IoT modules and stored in the cloud. Manipulating medical data needs an essential protection mechanism to ensure data privacy. To reduce the privacy issues, encryption algorithms are preferred generally but their efficiency needs to be improved without breaking the data confidentiality. This research work proposed an Extended Fully Homomorphic Encryption (EFHE) scheme to preserve medical data privacy. Parameters such as Signal to Noise Ratio, Peak Signal to Noise Ratio, Mean Square Error, encoding, and decoding time are considered for analysis and conventional homomorphic and fully homomorphic algorithms are used to compare with the proposed research model to validate the superior performance of the proposed encryption scheme.

Keywords: - Medical data, Cloud Computing, Internet of Things (IoT), Homomorphic encryption

## 1. INTRODUCTION

Internet of things (IoT) is an emerging paradigm that brought more attention almost in all domains. Since the world is moving towards the next level technology in all applications which efficiently utilizes various sensors and devices to achieve reliable and smart service. Dependability of sensor-based smart architectures is developed everywhere and IoT supports the system through its innovative methodologies. Smart cities [1], smart transport, smart management systems [2] [3] are some of the familiar examples of the Internet of things. Recently healthcare applications adopted IoT technology to provide smart medical applications. As the number of things or objects need to be interconnected through the internet, then the presence of IoT is unavoidable in the present situation. Remote health monitoring [4], Smart medical diagnosis [5], e-health care [6], are some of the IoT adopted medical applications which are efficiently implemented in recent days.

Encryption is an effective approach to preserve data privacy and recently IoT devices used encryption schemes to avoid data breaches [7]. Encryption algorithms are used to secure the data which is collected by sensor nodes in an IoT environment. Applying encryption increases data protection, data confidentiality, and data integrity [8] and that could be an effective countermeasure against attacks and threats. Various cryptographic schemes are evolved to achieve data security and among them, Advanced Encryption Algorithm (AES) [9], Data Encryption Algorithm (DES) [10], Rivest Shamir Aldeman (RSA) [11], Homomorphic Encryption [12], Fully Homomorphic Encryption [13], are some of the familiar models. Homomorphic encryption is one of the familiar models that enables computation over encrypted data without retrieving the plain text. The moderate performance of Homomorphic Encryption (HE) is overcome in Fully Homomorphic Encryption (FHE) that provides full support to homomorphic operations. Homomorphic encryption based solutions undecrypt ciphertext even when operations are performed over encrypted data in order to protect the data privacy. To improve the data privacy in medical IoT applications, this research work proposed an Extended Fully Homomorphic Encryption (EFHE) which improves the data privacy. The article is structured as follows: Section 2 provides a brief literature survey, Section 3 presents the proposed Extended Homomorphic Fully Encryption, Section 4 presents the discussion of experimental results and finally, the conclusion is presented in section 5.

## 2. RELATED WORKS

This section provides a detailed analysis of existing research works for privacy preservation and data management in cloud computing and IoT environment. The methodology used in the research work, merits, and demerits are observed to frame the proposed research work objective. Various encryption schemes are introduced to improve data security and privacy in cloud IoT environments. Attribute Based Encryption (ABE) is reported in various research works [14] [15] to preserve the data privacy. Based on the user preference sensitive data is preserved in attribute based encryption. Reduced computation cost and better encryption efficiency are the major advantages of attribute based encryption models. The issues in IoT layers such as application layer, transport layer, and perception layer are reduced through fault tolerant encryption scheme. [16] Ciphertext integrity protection and secure key sharing used in fault tolerant model improve the

data security. However, the system complexity of fault tolerant model is high compared to other encryption processes which is the major limitation of the research work.

Secure searchable encryption for cloud-IoT is reported in the literature [17] which reduces the computation cost. The issues in existing searchable symmetric encryption and public-key encryption are used to frame the objective of the Secure searchable encryption model. The encryption protocol used the trapdoor permutation function to design the searchable encryption model. Though the computation cost is minimized, the requirement of storage is high which increases the storage cost. To improve the performance of searchable encryption, fuzzy based approach [18] and dynamic searchable symmetric encryption [19] are introduced which improves the functionality, efficiency, and extensibility of the data along with better tradeoff.

Priority Re-Encryption (PRE) based data encryption model is introduced in the literature [20]. Proposed identity-based PRE model similar to conventional model except for the keys. Encrypter is used to generate the keys instead of the delegator. Compared to the conventional PRE model, the proposed model attains better security performance on securing cloud data. Similar Symmetric Proxy Re-Encryption (PRE) is reported in the literature [21] to establish secure communication between IoT devices and clients. The proposed model used a Field-Programmable Gate Array to secure IoT data in public clouds. The symmetric session key is introduced to establish a secure communication path between cloud Field Programmable Gate Array and devices. Proposed hardware implementation results demonstrate the performance is much better than software-based models.

Ciphertext Policy Attribute-Based Encryption (CP-ABE) is reported in the literature [22] which provides fine-grained access control and better data privacy for the IoT environment. It allows the uses based on the attributes which match the access policies. Matched users are allowed to decrypt the ciphertexts others are neglected to access the data which increases the security feature. But, conventional models leak the attributes in the key generation phase which leads to threats to user privacy. To overcome this security lag, 1-out-of-n oblivious transfer technique is introduced in the research work to protect the user attributes. The performance of the proposed model is much better than conventional CP-ABE.

A review of homomorphic encryption techniques is presented in the literature [23]. From the analysis, it is observed that homomorphic encryption is efficient and eliminates data privacy issues.

Homomorphic encryption allows the user to search and manipulate the data in the cloud environment without decryption which is considered an advantage in the encryption process. Homomorphic encryptions are considered as the best choices for cloud IoT data security and recently fully homomorphic encryptions schemes are widely adopted in various cloud applications. The challenges in adopting cloud-IoT are addressed in literature [24] through fully homomorphic encryption which used proxy re-ciphering as a service. Long-term privacy-preserving for encrypted data is achieved through the proposed encryption model and provides efficient secure and reliable cloud-IoT applications.

### 2.1 Research gap

From the above literature analysis, the following research gaps are identified and summarized as follows

1. Most of the encryption models provide better performance in data security and privacy without concern about other parameters like computation cost, memory, and efficiency.
2. Few research models addressed the issues in medical data privacy preserving policies, but still, it needs to be improved.
3. Multi objective encryption models should be introduced to attain a complete security model for the cloud IoT domain.
4. System complexity is found as a major limitation of few encryption schemes.

### 2.2 Objective

Based on the identified research gaps, the objective of the proposed work is framed as follows

1. To introduce an enhanced privacy preserving model for medical data in cloud IoT.
2. To develop a multi objective model to minimize the system complexity and to improve the data privacy along with encryption and decryption

Considering the above objectives, the proposed privacy preserving model is developed using Extended Fully Homomorphic encryption (EFHE). Compared to conventional homomorphic encryption, the performance of fully homomorphic encryption scheme is better and it is further improved through the proposed Extended Fully Homomorphic encryption (EFHE) model.

## 3. PROPOSED WORK

An Extended Fully Homomorphic Encryption (EFHE) is proposed in this research work to secure user data in cloud-IoT medical applications. Theoretical analysis of improved encryption schemes is discussed in this section. From the conventional homomorphic encryption, the proposed improved encryption model is derived. Fully homomorphic encryption supports homomorphic addition and multiplication on the ciphertext. A Semi-homomorphic system supports either homomorphic multiplication or addition and these encryption models provide opportunities to develop programs for any functionality. Programs that run over encrypted inputs produce encrypted results. However, it does not require decryption for its inputs and it can be executed in any untrusted third-party applications. Those third party service providers are unaware of inputs and internal states; this provides better practical advantages in fully homomorphic encryption schemes. Figure 1 depicts the process flow of the proposed IoT cloud module with an Extended Fully homomorphic encryption scheme.

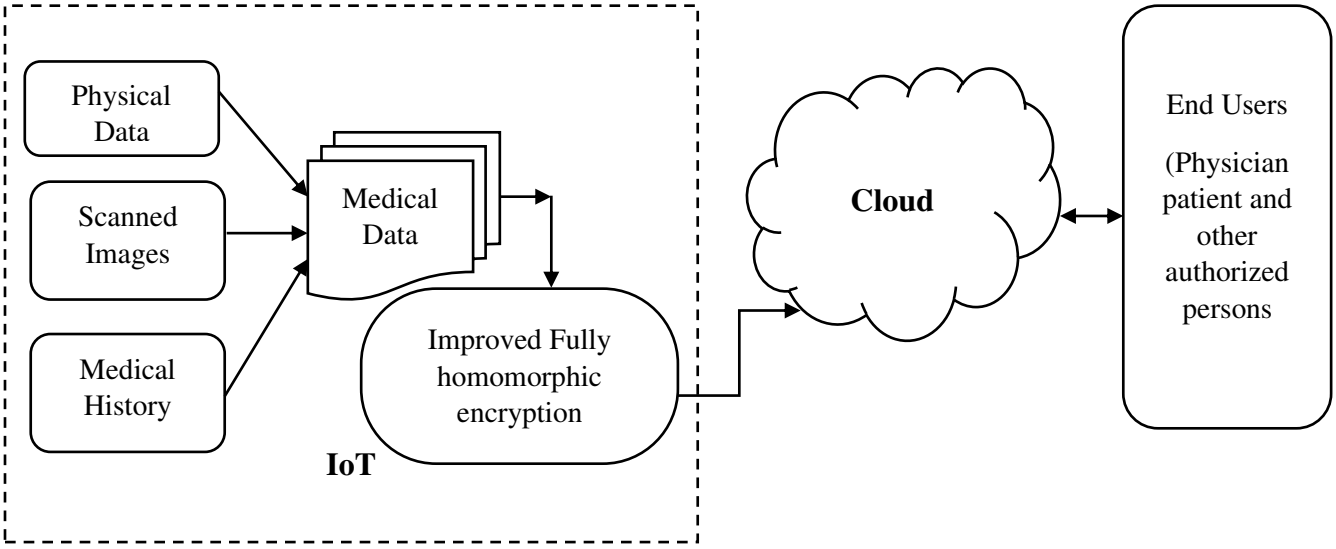



**Figure 1 Proposed model process flow**

Consider a conventional FHE system in which the private key is represented as $(k)$, and the public key is represented as $(n)$. The public key is generated using the private key $(k)$ and random sample $(r_s)$ and it is given as

$$k \times n = 2r_s \tag{1}$$

The encryption process is used to convert plaintext into ciphertext. Consider the plain text $x \in \{0,1\}$ and the message is set as $m = (x, 0,1, \ldots..0)$ with a random sequence $n_r$. The ciphertext for the given plaintext will be obtained as

$$C_t = m + n^T . n_r \tag{2}$$

where $n^T$ is the transpose of public key and $m$ is message set which has values of 0 and 1. The decryption is performed to convert the ciphertext into plain text using a private key $(k)$ and it summarized as follows

$$\begin{aligned} &\left(([C_t, k])_q\right)_2 = \left(([m + n^T . n_r, k])_q\right)_2 \\ &= \left(([m^T \mathrm{s} + (n^T . n_r)^T k])_q\right)_2 \\ &= ([x + {n_r}^T n. k])_q \\ &= ([x + {n_r}^T 2r_s])_q = x \end{aligned} \tag{3}$$

where q is used to perform modulo and the correctness of the decryption depends on the total noise introduced to the system and it should be in the level of ${n_r}^T r_s < \frac{q}{4}$. The proposed work introduces Extended Fully homomorphic encryption to improve the efficiency of the conventional FHE model. Two major modifications are performed in the conventional model to attain improved performance. (1) The Re-linearization technique is introduced for the multiplicative ciphertext to reduce the size which reduces the elements in the rings. The noise and ciphertext modulus is reduced further using the modulus switching technique. (2) Instead of using both re-linearization and modulus switching on each multiplication process, it is utilized only when it is required for multiplicative homomorphic. These two conditions improve the efficiency of a fully homomorphic encryption scheme compared to the conventional FHE model.

The mathematical model for Extended Fully homomorphic encryption is described based on the setup phase, key generation phase, encryption phase, addition, and multiplication phase, decryption phase. In the setup phase, the input security parameter is taken as $\varphi$ and its level is considered as $\alpha$. Generate prime modulus based on the security parameter and its level and it is given as

$$q_i = q_i(\varphi, \alpha) \text{ where } i = 0,1,2, \ldots.. \alpha - 1 \tag{4}$$

The above equation must satisfy the condition of $q_0 < q_1 < \cdots < q_{\alpha-1}$ and the error distribution is represented as $x \in n_r$. Based on the error distribution the range of the parameter are redefined as $q_i = 0,1,2 \ldots . \alpha - 1, x$. In the key generation phase, these parameters are considered and select secret key $(l)$ as $l \in s_r$. The random coefficients are represented as $s_r$ in the range $\{0,1\}$. Based on the above terms, the generated key is derived as

$$g_k = (-[n.l + x.n_r])_{q_i} \tag{5}$$

where is $n$ obtained from uniformly random $s_{q_i}$ in a sampled manner, $n_r$ is the error coefficient which is selected from the plain text modulus $x$. The switching matrix for an integer is represented as $m_i = (g_{k_i}, n_i)$, where $g_{k_i} = \left(-[n_i.l + x.n_{r_i} - n_i.l^2]\right)_{q_i}$ , $n_i \in s_{r_i}$, $n_{r_i} \in x$, and $i = 0,1,2, \ldots . \alpha - 1$. In the encryption phase, the plain text is sampled based on $n_{r_i}$ and $x$. The ciphertext is obtained as follows

$$C_t == \left[\left(x + g_k.s + t.n_{r_1}\right)_{q_i}, \left(x + g_k.s + t.n_{r_2}\right)_{q_i}, \left(x + g_k.s + t.n_{r_3}\right)_{q_i}, \ldots .\right] \tag{6}$$

where $i = 0,1,2, \ldots . \alpha - 1$. The additive process in the Extended Fully homomorphic encryption is processed as follows. Consider two ciphertext $C_t'$ and $C_t''$ and it is represented as $C_t' = \left[C_{t0}', C_{t1}', C_{t2}' \ldots C_{tp}'\right]$, $C_t'' = [C_{t0}'', C_{t1}'', C_{t2}'' \ldots C_{tz}'']$. For both ciphertexts, the same secret key is used and the necessary condition for additive ciphertext is $p \leq z$, where the range of $p, z$ is given as $\{1,2\}$. The additive ciphertext for the two ciphertexts is obtained as

$$C_f = \left[(C_{t0}' + C_{t0}'')_{qi}, (C_{t1}' + C_{t1}'')_{qi}, \ldots \left(C_{tp}' + C_{tz}''\right)_{qi}\right] \tag{7}$$

where $i \in 0, \alpha - 1$. In the case of multiplicative ciphertext, two ciphertext $C_t'$ and $C_t''$ are considered which uses the same secret key, the multiplicative ciphertext is obtained as follows

$$\left.\begin{aligned} C_{f0} &= [C_{t0}'.C_{t0}'']_{qi} \\ C_{f1} &= [C_{t0}'.C_{t1}'' + C_{t1}'.C_{t0}'']_{qi} \\ C_{f1} &= [C_{t1}'.C_{t1}'']_{qi} \end{aligned}\right\} \tag{8}$$

In multiplicative homomorphic operation, the size of the ciphertext is reduced using the weight function $w_i = [w_{i,0}, w_{i,1}]$ and this reduces the ring elements. This technique is termed as re-linearization and the ciphertext $C_t^* = [C_{t0}^*, C_{t1}^*]$ obtained after re-linearization is defined as follows

$$\left.\begin{aligned} C_{t0}^* &= \left(x.C_{t0} + C_{t2}.w_{i,0}\right)_{x.qi} \\ C_{t1}^* &= \left(x.C_{t1} + C_{t2}.w_{i,1}\right)_{x.qi} \end{aligned}\right\} \quad (9)$$

Modulus switching technique is used to convert $C_t^*$ into $C_f$ and reduced $x.qi$ into $qi$ which reduces the noise for the decryption process. The decryption process of Extended Fully homomorphic encryption is formulated as

$$m = \left([C_{t0} + C_{t1}.l]_{qi}\right)_t \quad (10)$$

The final ciphertext after homomorphic operation is generalized as $C_f = \left(C_{f,0}, C_{f,1}, C_{f,2}, \ldots C_{f,z}\right)$ and the encrypted text is generally represented as

$$m = \left(\left[C_{f0} + C_{f1}.l + \cdots + C_{f,z}.l^z\right]_{qi}\right)_t \text{ where } z \in \{1,2\} \quad (11)$$

The above formulations describe the encryption, key generation, and decryption process of an Extended Fully homomorphic encryption process. Summarized pseudocode for the proposed encryption scheme is given as follows

---

*Input: Medical Data (Sensor data, scan images)*

*Output: encrypted medical data*

*Initialization: Initialize sensors, cloud virtual machines*

*begin*

*collect data from sensors, scan images and consolidate as medical data*

*begin encryption*

*{*

*Initialize private key and public key*

*Generate prime modulus using equation (4)*

*Initialize secret key*

*Generate a final key using equation (5)*

*Encrypt the plain test using equation (6)*

*Compute additive ciphertext for* $C_t'$ *and* $C_t''$

*If* $p \leq z$

*Compute* $C_f$ *using equation (7)*

*Compute multiplicative ciphertext using equation (8)*

*If no additive process*

*Compute weight function* $w_i$

*Generate new ciphertext using equation (9)*

*Decrypt the message using equation (11)*

*end*

*end*

---

## 4. RESULT AND DISCUSSION

The performance of proposed Extended Fully homomorphic encryption in the cloud-IoT medical application has experimented in NetBeans version 8.1 installed on Windows 8 operating system in i3-2328M processor of 2.20 GHz frequency with 16Gb memory model. Simulation parameters used for the experimentation are listed in table 1.

**Table 1. Simulation parameters**

| S.No | Parameter | Value |
|---|---|---|
| 1 | Number of VMs | 10 |
| 2 | Number of cloudlets | 10 |
| 3 | Number of datacenters | 05 |
| 4 | Encrypted file size | 300KB-10MB |
| 5 | Decrypted file size | 300KB-10MB |
| 6 | Computation time | 160ms |
| 7 | RAM size | 2024MB |

Medical images are used in the experimentation process and figure 4 depicts the sample of the input images. Seven different images are used in experimentation.

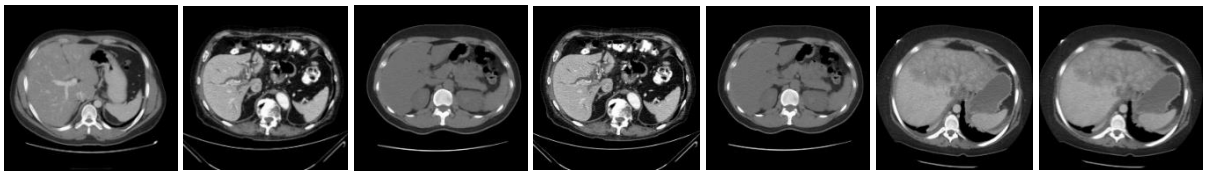


**Figure 2 Sample input images**

The ratio of the mean square difference of two images to the maximum mean square difference is obtained as peak signal to noise ratio (PSNR). The quality of the image is defined based on the PSNR values. The performance of the proposed Extended Fully homomorphic encryption is compared with conventional homomorphic and fully homomorphic models for PSNR values and depicted in figure 3. It is observed that the improved model attains high PSNR values compared to other models. High PSNR indicates better image quality which is achieved in the proposed model.

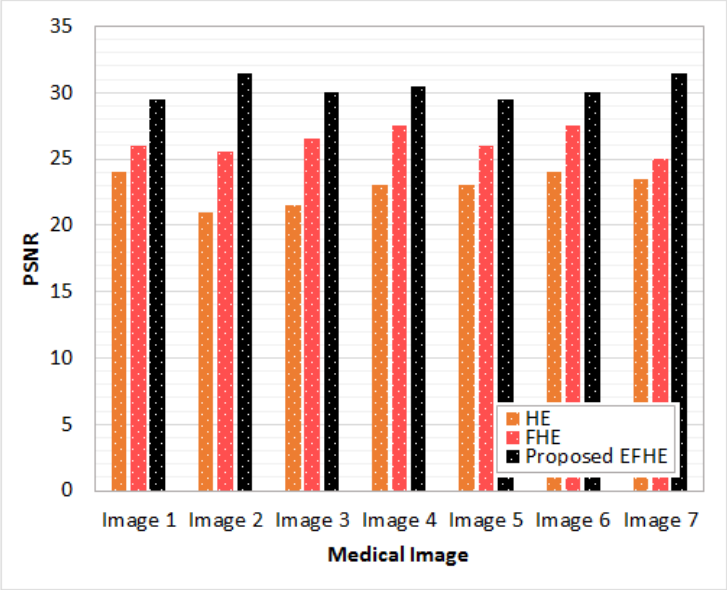



**Figure 3 PSNR Comparison**

The SNR performance of the proposed extended fully homomorphic encryption (EFHE) is compared with conventional Homomorphic Encryption (HE) and Fully Homomorphic Encryption

(FHE) Model and depicted in figure 4. It is observed that proposed Extended Fully homomorphic encryption attains better SNR ratio due to its re-linearization and modulus switching process.

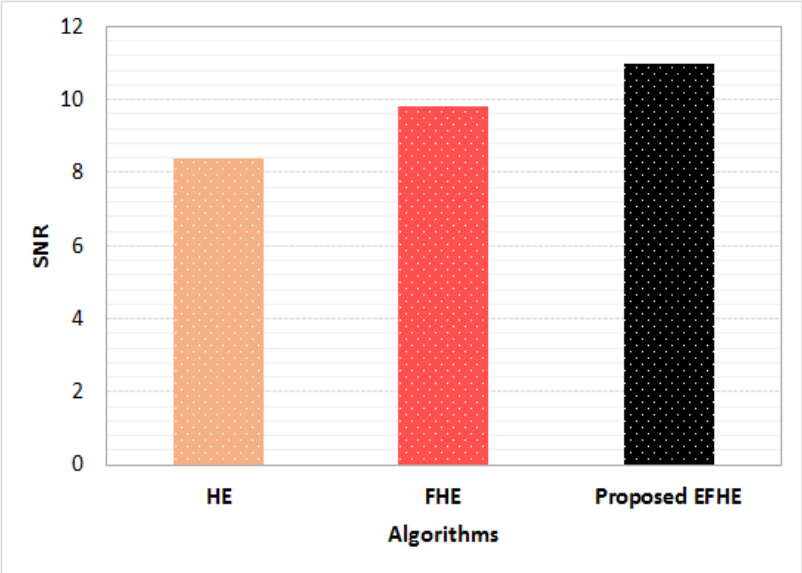



**Figure 4 SNR Comparison**

Figure 5 depicts the comparison of mean square error for the proposed approach and conventional models. The minimum error of the proposed encryption model indicates better performance compared to conventional models.

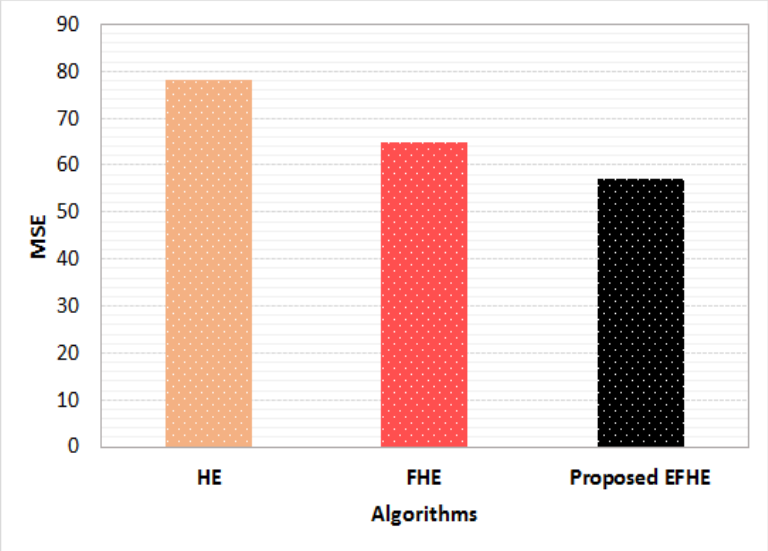
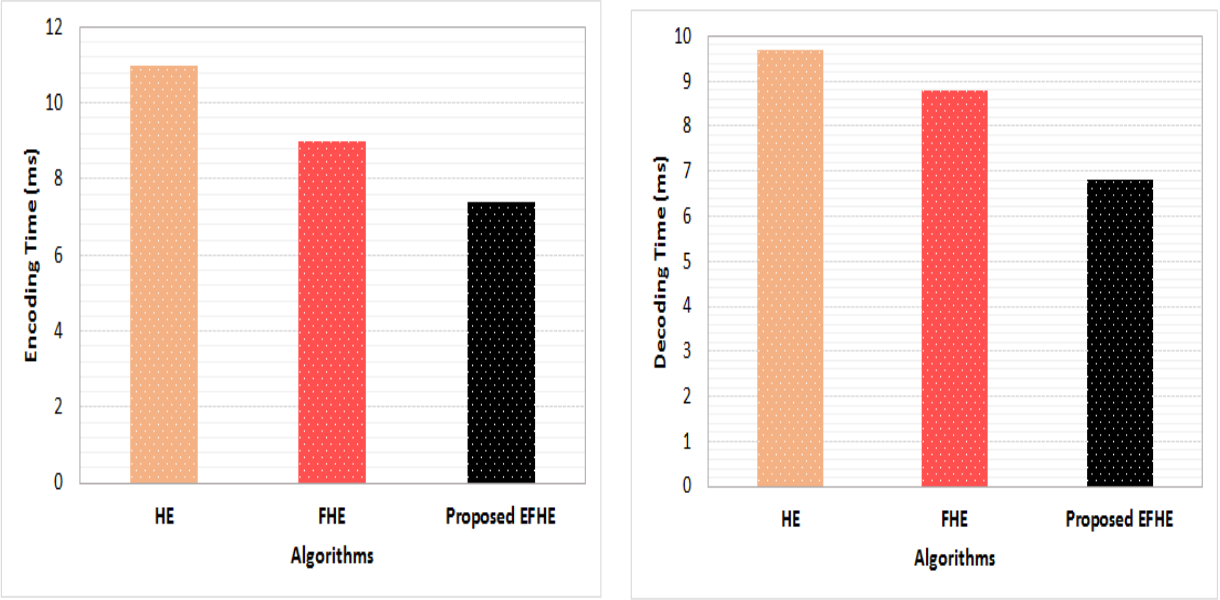



**Figure 5 MSE Comparison**




**(a)** **(b)**

**Figure 6 Computation time – (a) Encryption (b) Decryption**

Computation time for proposed Extended Fully homomorphic encryption is depicted in figure 6. The time taken to encrypt the input image is calculated as encoding or encryption time. The average encryption time of all three models is depicted in figure 6(a). Similarly, the time taken to decrypt the encrypted message is calculated as decryption time and an average decryption time is reported in figure 6(b). It is observed in both the encryption and decryption process the proposed model secures data takes minimum time compared to conventional models. Moreover from the experimental analysis, it is observed that due to improved encryption and decryption, user privacy is increased. The system complexity is also less compared to other encryption standards.

## 5. CONCLUSION

Privacy preserving on personalized medical data in cloud IoT using Improved Homomorphic encryption is proposed in this research work. conventional IoT based healthcare applications are suffered from storage and security issues. The overcome the issue and to improve the performance cloud computing is integrated. But the cloud environment is vulnerable to attacks and data privacy is important in healthcare applications. Encryption is a suitable option to improve data privacy, considering these advantages, the proposed model introduces Extended Fully homomorphic encryption to secure medical data in an IoT-cloud based healthcare application. Conventional

encryption models such as homomorphic encryption and fully homomorphic encryption are compared with proposed Extended Fully homomorphic encryption to validate the better performance of the proposed model. with minimum encoding and decoding time proposed model attains better performance for signal to noise ratio, peak signal to noise ratio, and mean square error parameters. Further this research work could be improved using hybrid encryption models to enhance the data privacy and security.

## *Conflict of Interest Disclosure*

*Article Title: "*Privacy preserving on personalized medical data in cloud IoT using Extended Fully Homomorphic Encryption"

Author: Pradeep Bedi, S B Goyal

We certify that there is no actual or potential conflict of interest in relation to this article.

29.12.2020

**Pradeep Bedi**

Graphic Era Hill University, Dehradun, INDIA

bedipradeep1983@gmail.com

**S B Goyal**

City University, MALAYSIA

drsbgoyal@gmail.com

**Authorship Contributions**

**We have indicated individual authors conrtribution as follows:**

**Pradeep Bedi**

Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Resources, Software, Validation, Visualization, Writing-original draft

**S B Goyal**

Finalization of cenecptaulization, Formal Analysis, Paper Admisnitration, Supervision, Validation, Visualization, Writing-Final Draft, Writing-review and editing

29.12.2020

**Pradeep Bedi**

Graphic Era Hill University, Dehradun, INDIA

bedipradeep1983@gmail.com

**S B Goyal**

City University, MALAYSIA

drsbgoyal@gmail.com

## REFERENCES


1. Daming Li, Lianbing Deng, Qinglang Su (2020), "Improving communication precision of IoT through behavior-based learning in smart city environment" Future Generation Computer Systems, vol.108, pp.512-520.
2. Abdellah Daissaoui, Azedine Boulmakoul, Ahmed Lbath (2020), "IoT and Big Data Analytics for Smart Buildings: A Survey" Procedia Computer Science, vol.170, pp.161-168.
3. Junaid Latief Shah, Heena Farooq Bhat, Asif Iqbal Khan (2020), "Integration of Cloud and IoT for smart e-healthcare" Healthcare Paradigms in the Internet of Things Ecosystem, pp. 101-136.
4. Yuanyuan Pan, Minghuan Fu, Biao Cheng, Xuefei Tao, Jing Guo (2020), "Enhanced Deep Learning Assisted Convolutional Neural Network for Heart Disease Prediction on the Internet of Medical Things Platform", IEEE Access, vol. 8, pp. 189503-189512.
5. Rahul Krishnan Pathinarupothi, P Durga, Ekanath Srihari Rangan (2019), "IoT-Based Smart Edge for Global Health: Remote Monitoring With Severity Detection and Alerts Transmission", IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2449-2462.
6. Atena Roshan Fekr, Katarzyna Radecka, Zeljko Zilic (2015), "Design and Evaluation of an Intelligent Remote Tidal Volume Variability Monitoring System in E-Health Applications" IEEE Journal of Biomedical and Health Informatics, vol. 19, no. 5, pp. 1532-1548.
7. Karen R. Sollins (2019), "IoT Big Data Security and Privacy Versus Innovation", IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1628-1635.
8. Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, Biplab Sikdar (2019), "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", IEEE Access, vol. 7, pp. 82721-82743.
9. Luca Crocetti, Luca Baldanzi, Luca Fanucci (2019), "A simulated approach to evaluate side-channel attack countermeasures for the Advanced Encryption Standard" Integration, vol.68, pp. 80-86.
10. Rui Zhang; Rui Xue; Ling Liu (2018), "Searchable Encryption for Healthcare Clouds: A Survey", IEEE Transactions on Services Computing, vol. 11, no. 6, pp. 978-996.

11. Khalid El Makkaoui, Abderrahim Beni-Hssane, Anas El-Ansari (2017), “Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing” Procedia Computer Science, vol.113, pp. 33-40.
12. Yang Lu, Minghui Zhu (2018), “Privacy preserving distributed optimization using homomorphic encryption” Automatica, vol. 96, pp. 314-325.
13. Jian Xu, Laiwen Wei, Chong-zhi Gao (2018), “Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures” Journal of Network and Computer Applications, vol.107, pp. 113-124.
14. Libing Wu, Biwen Chen, Debiao He (2018), “Efficient and secure searchable encryption protocol for cloud-based Internet of Things” Journal of Parallel and Distributed Computing, vol.111, pp.152-161.
15. José L. Hernández-Ramos, Salvador Pérez, Antonio F. Skarmeta (2018), “Protecting personal data in IoT platform scenarios through encryption-based selective disclosure” Computer Communications, vol.130, pp.20-37.
16. Sana Belguith, Nesrine Kaaniche, Rabah Attia (2018), “Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT” Computer Networks, vol.133, pp. 141-156.
17. Peng Zhang, Juntao Gao, Xuelian Li (2019), “Design of compressed sensing fault-tolerant encryption scheme for key sharing in IoT Multi-cloudy environment(s)” Journal of Information Security and Applications, vol.47, pp. 65-77.
18. Shahzaib Tahir, Sushmita Ruj, Muttukrishnan Rajarajan (2019), “Fuzzy keywords enabled ranked searchable encryption scheme for a public Cloud environment” Computer Communications, vol.133, pp.102-114.
19. Yen-Wu Ti, Chia-Feng Wu, Chia-Mu Yu, Sy-Yen Kuo (2020), “Benchmarking Dynamic Searchable Symmetric Encryption Scheme for Cloud-Internet of Things Applications”, IEEE Access, vol. 8, pp. 1715-1732.
20. Xu An Wang, Fatos Xhafa, Zhiheng Zheng (2019), “Controlled secure social cloud data sharing based on a novel identity based proxy re-encryption plus scheme” Journal of Parallel and Distributed Computing, vol.130, pp.153-165.

21. Mohd.Al-Asli, M. E. S. Elrabaa and M. Abu-Amara (2019), “FPGA-Based Symmetric Re-Encryption Scheme to Secure Data Processing for Cloud-Integrated Internet of Things”, IEEE Internet of Things Journal, vol. 6, no. 1, pp. 446-457.
22. Qi Han, Yinghui Zhang, Hui Li (2018), “Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things” Future Generation Computer Systems, vol.83, pp.269-277.
23. Mohamed Alloghani, Mohammed M. Alani, Ahmed J. Aljaaf (2019), “A systematic review on the status and progress of homomorphic encryption technologies” Journal of Information Security and Applications, vol.48, pp.1-10.
24. Shruthi Ramesh, Manimaran Govindarasu (2020), “An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data” IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8700-8708.