Secure Multiparty computation enabled E- Healthcare system with Homomorphic encryption

A Vijaya Kumar¹, Mogalapalli Sai Sujith², Kosuri Tarun Sai³, Galla Rajesh⁴, Devulapalli Jagannadhra Sriram Yashwanth⁵

¹Assistant Professor, ², ³, ⁴, ⁵Student
¹, ², ³, ⁴, ⁵Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswarum, AP, India,

E-mail: vijay.adury@gmail.com

Abstract.: With the spread of Covid – 19 pandemic it is difficult for many patients to physically visit the Hospitals and get treatment. The Improved technology enable such patients to contact the concern doctors and get diagnosis information online. The security of the sensitive data of the Patients is vulnerable when the information is shared across the network. To address this, we are proposing a novel approach with the Privacy ensured self-care health management schema using Secure Multiparty computation (MPC). Through this approach the patient can share the sensitive data to the Hospital server through the online mode, the data will be shared in the encrypted format which will be matched with the existing data at the Hospital records and the best relevant match based on the smart Index of disease. The privacy preserving is key aspect in this model as the data is shared in the sensitive mode so the Homomorphic Encryption (HE) approach is used to perform computations on the Patient’s sensitive data in the encrypted mode and ensure the confidentiality from Intruders to access the information. This model also proposes a novel approach which can overcome many security threats. The patient’s data will be shared and used in a more secured manner so the patients specifically the elder who are not advised to visit the public places in this pandemic can also receive better treatment through online.

1. Introduction
The rapid growth in the IT technology enabled the e-medical advice approach which is predominantly gained popularity in recent days. The Novel Covid-19 pandemic[2] drastically affected the day to day life, specifically the old people and children and people suffer with chronic diseases who require medical advice and/or diagnosis are not advised to visit the hospitals unless an emergency situation. Technology enabled e-Medical Advice model helps the patients to take medical advice in the digital mode. The data shared by the patient’s is private and sensitive but the security of the data shared in the group [4] is vulnerable. To maintain the huge number of patients information for diagnosis or advice purpose require the cloud enablement for better accessibility and high availability. The security of the data stored in the third party clouds is always untrusted by many people. The sensitive information should not be compromised [5], as it may be used for unethical practices by the intruders. The secure multiparty computation [1] useful to produce the diagnosis for a patient based on the symptoms provided compared with previous patient’s information without revealing the details to others. The need for medical diagnosis is becoming an essential thing because of the high chance of affecting seasonal or diseases for everyone. Group data shared model [3] focuses on the data shared by group but the data may be compromised. In this paper we propose the e Medical advice model enabled with Secure Multiparty computation. In spite of
SMC as the data is stored over the cloud a holomorphic encryption [6] approach is chosen so that the data will be in ciphered mode. This makes the data could be shared across patient and hospital and diagnostic centers and pharmacies too. In the related work the challenges in the existing models are discussed the proposed SMC based Holomorphic Encryption enabled e-Advice System. The medical diagnosis that is self-serviced and secured over the internet. Many medical services have developed so far to reduce medical costs. IoT enabled Healthcare devices[7] are available to provide accurate medical data such as thermometers, blood pressure monitors, infusion pumps, oximeters etc. The temperature, blood pressure, sugar levels and oxygen levels data will be taken from the smart devices and other symptoms will be provided by the patients or caretakers. Patients’ medical data in the encrypted digital format over the cloud will be providing diagnosis using multiparty computation with doctors’ advice and/or further diagnosis.

2. Literature Review

The cyber-attacks on medical data have been increasing day-to-day. It’s unsure that the medical data in the cloud is not leaking to anyone. The data leakage of medical information may cause emotional harm to the patients, which may lead to threatening dementia and other psychic problems which is the challenging aspect of self-serviced medical diagnosis system. [3] Proposed the data shared model in the public cloud by group of users. Many patients have security concerns over uploading their data to the third-party cloud vendors. The large and variety of the data uploaded by the patients need cloud based storage for fault tolerant [8] and high available data access. Hybrid encryption model over the IoT network and Water marking techniques [10] deal with specific aspects of the data security. This model focuses on the test reports of the patients which cannot be tampered with the watermarking technique provided, the shortfall of this model is the user symptoms other than medical reports are not focused. The augmented review [11] of the health care data explains how the IoT enabled devices access the patient’s information as stated can be securely quality health report by applying various decision making algorithms over it. [12] Proposed a model which is an e-consultancy to provide healthcare for rural communities. This model detailed how the rural communities can get benefit out of the e healthcare system. A new privacy-preserving medical diagnosis was performed, which uses the latest encryption algorithm like Holomorphic encryption, which encrypts data while forwarding to the cloud. If there is any data leakage, then there is no chance of misuse of medical information. For images and medical reports related data and adaptive LSB and PVD [13] model is proposed. The encrypted mode of data occupy more space, a crypto based cloud compressed storage model [14] can be considered.

2.1 Secure Multi Party Computation Model

The key purpose of using the secure multiparty computation [16] (SMC) model is to compute the common function across the participants which hold the private information. This model works on the principle that only the result of the computation will be shared with the participants and the others inputs will be only available with the Manager or authority who maintains the whole transaction. The e-healthcare model matches to this approach as the patient’s sensitive data should not be revealed to others and it only need to be used for the diagnosis with the comparison with existing patient’s data. The data size is enormous as it consists of previous medical reports too which leads to the public cloud storage model for efficient, cost effective and fault tolerant model.
Figure 1. Secure Multiparty computation illustration

The $f(x, y)$ indicates a function which is computed over two arbitrary inputs from two people who only knows/shares their input with the computing authority. Once computation function is evaluated then the result is shared across parties, there could be more than two parties to participate in many transactions. In health care model also many patient’s data is used to identify the diagnosis of the remote user. The patient’s information will be shared to the public cloud environment for persistent storage. Whenever new Patient symptoms are given to the system then the match will be performed and the most probable diagnosis will be shared with the patient.

2.2 Homomorphic Encryption

The secure multiparty computation (SMC) ensures that the data stored in the cloud is not shared with other parties of the activity. The data stored in the public cloud may be compromised which leads to the issue of Integrity [17].

Couple of algorithms, attribute based [18] and hash based [19] and public key encryption model approaches have proposed models to address the cloud storage security aspect. These models securely However as part of secure multiparty computation these models also should decrypt the data before it being supplied to the function of SMC, then the data may be tampered or eavesdropping would happen. Homomorphic Encryption [6] basic principle is to perform the operations on the encrypted data. The inputs will be in the encrypted format and the function $f(x, y)$ will also be performed on the encrypted inputs $g(E(x), E(y))$ where

$E(x)$ is the encrypted input stored in the cloud for data $x$

$E(y)$ is the encrypted input stored in the cloud for data $y$

$G(E(x), E(y))$ is the function which perform the operation gives the same result of $f(x, y)$ but it works on the encrypted data.
Many of the above proposed models are practically limited, rich in goals. The major difficulty of the e-Medical advice model is who is the owner of the data? The patients worry is always about their sensitive information shared with the Healthcare institute. In the previous developed models the patient’s will receive the diagnosis but it is not guaranteed that the data breaches not exist in the current model.

![Figure 2. Homomorphic Encryption Evaluation](image)

![Figure 3. e-Medical advice model without SMC and homomorphic encryption](image)
3. Proposed Model

3.1 SMC based Homomorphic encrypted e-Medical advice model

i) The existing e-healthcare models are doctor centric models where the patient will submit the data to the hospital. The proposed model is designed with patient centric approach, where the data without being revealed to doctor can be shared across various entities of the systems like diagnostic centres, pharmacies etc.

ii) This proposed model stores the data in the encrypted format which prevents the eavesdropping and ensure the trust among the patient community. As the computation also performed on the encrypted data and only the result will be shared across the patient, the data cannot be eavesdropped.

![Diagram](image)

**Figure 4. SMC enabled e-Medical Advice model with Homomorphic Encryption**

The above model the patient data will be first encrypted and stored in the cloud system. The Hospital systems access the encrypted patient symptom data from the cloud and matches with the existing patients’ symptoms which are also in the ciphered form. The fully homomorphic enabled SMC model performs the operation on the encrypted data and Encryption system and select the diagnosis. The best diagnosis can be found by applying different machine learning algorithms like Decision Tree, Artificial Neural networks and Decision Tree based random forest approaches.
The diagnosis offered by the automated system will be verified with the doctor with whom the patient took the appointment and suggest the remedy or medicines, even the prescription of the medicines can also be shared to the pharmacies and the medicines also can be ordered. No personal information about the patient will be revealed to the Diagnostics Centre or pharmacy, only the necessary information will be provided. The diagnosis or treatment details provided by the doctor in the encrypted format will be decrypted by the private key of the patient.

3.2 E-Medical Advice model based on SMC with Homomorphic Encryption

The Patient Data is taken as vector/set of symptoms

\[ D = (d_1, d_2, \ldots, d_n) \]

The Hospital Cloud or database will be already having Background Knowledge i.e. Previous Data to which the user input should be matched with.

The patient data will be encrypted and send to the hospital

\[ E(d_1, d_2, d_3, \ldots, d_n) \]

The Cloud or hospital storage system has the previous knowledge database with various symptoms

\[ (f_1, f_2, \ldots, f_k) \]

where \( k >> n \)

The symptoms of the patients 1 to n will be mapped with corresponding columns of 1..k of the Hospital database and will be compared based on the similarity index prepared by the Random Forest Algorithm as it focuses on all the aspects of the Decision tree to give more optimal prediction of the

![Flow Diagram of e-Medical Advice Model](image_url)
Disease. The disease prediction information will be shared to the doctor and he suggest the prescription and tests if any required.

The similarity index of the Data $E(d_1,\ldots,d_n)$ with $(f_1,\ldots,f_k)$ data store gives the more relevant information about the disease.

### 3.3 E-Medical Advice system process steps

1. The patient first register with the Hospital system
2. The Patient submit the symptom details through online
3. The symptom details and previous reports will be encrypted and will be sent to the hospital database
4. After authenticating the patient details, the hospital server compares the patient’s symptoms information with the Pre Existing background knowledge of disease database.
5. Homomorphic encryption helps to perform the operation on the encrypted mode of data
6. The Random Forest Machine Learning algorithm will be applied to find the best match based on the data provided by the patients and predict the best match in the encrypted match
7. The encrypted diagnosis information will be given to the patient which will be encrypted on the patient side and get the diagnosis information

### 3.4 Encryption and decryption with paillier homomorphic encryption approach

```python
# import syft package used for secure deep learning
import syft as syft
# import torch package
import torch as torch

# generate the public and private keys
pukey, prkey = syft.keygen()

# Applying the pailler algorithm of Homomorphic encryption
x = torch.tensor([1, 2, 3]).encrypt(protocol="paillier", public_key=pukey)
y = torch.tensor([2, 2, 2]).encrypt(protocol="paillier", public_key=pukey)

# encrypted sum
sum = x + y

# decryption with private key
print(sum.decrypt(protocol="paillier", private_key=prkey))
# tensor([3, 4, 5])
```
4 Conclusion

Our work preliminarily focused on the secure storage of the sensitive medical data of patients in the public cloud or third party. In the IT enabled world the patients can get the electronic based medical advice from the doctors. But the security of the private information they are sharing with the Hospital system bothers the patients. We proposed a Secure Multiparty Computation enabled E-Medical advice system which takes the symptoms from the patient and the symptoms are compared with pre knowledge data store available at the Healthcare system. To ensure the security of the data stored at the data store homomorphic encryption approach model is applied. Paillier encryption algorithm is used to realize the partial homomorphic encryption approach. This model can also be extended to the Diagnostic centers and pharmacy too. Though it provides security and reliability of the user data the model runs relatively very slow as the operations are performed on the encrypted data rather than plain data. This model can also be extended to the E auction and E Voting models too.

References

[1] Zhao, Chuan& Zhao, Shengnan& Zhao, Minghao& Chen, Zhenxiang&Gao, Chong-Zhi& Li, Hongwei&yu-an, Tan. (2018). Secure Multi-Party Computation: Theory, Practice and Applications. Information Sciences. 476. 10.1016/j.ins.2018.10.024.
[2] https://www.who.int/emergencies/diseases/novel-coronavirus-2019/global-research-on-novel-coronavirus-2019-ncov
[3] Burramukku, Tirapathi&Chava, Ch & Kumar, T & Kalyan, V. (2019). Security key provided for group data sharing in cloud computing.
[4] Sun, Yunchuan& Zhang, Junsheng&Xiong, Yongping& Zhu, Guangyu. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. 2014. 1-9. 10.1155/2014/190903.
[5] Lindell, Y. (2005). Secure multiparty computation for privacy preserving data mining. In Encyclopedia of Data Warehousing and Mining (pp. 1005-1009). IGI Global.
[6] Gentry, C., &Boneh, D. (2009). A fully homomorphic encryption scheme (Vol. 20, No. 9, pp. 1-209). Stanford: Stanford university.
[7] Tang, W., Ren, J., Deng, K., & Zhang, Y. (2019). Secure data aggregation of lightweight e-healthcare iot devices with fair incentives. IEEE Internet of Things Journal, 6(5), 8714-8726.
[8] Bala, A., & Chana, I. (2012). Fault tolerance-challenges, techniques and implementation in cloud computing. International Journal of Computer Science Issues (IJCSI), 9(1), 288.
[9] Kolla, Bhanu. (2019). Hybrid Encryption for Medical Applications Using Advanced Algorithms in Internet of Things . M Krishna Sai, P Lakshma Reddy, N Siva Rama Krishna, P Venkata Naga Sai Ravi Teja, KollaBhanu Prakash. Indian Journal of Public Health Research and Development. 10. 191.
[10] Aparna, Puuvadi& Kishore, P.V.V.. (2017). An Efficient Medical Image Watermarking Technique in E-healthcare Application Using Hybridization of Compression and Cryptography Algorithm. Journal of Intelligent Systems. 27. 10.1515/jisys-2017-0266.
[11] PremaLatha, V. &Karimunnisa, S. &Harita, U.. (2017). Augmented review on internet of things for health care. Journal of Advanced Research in Dynamical and Control Systems. 9. 529-541.
[12] Miah, S. J., Hasan, J., &Gammack, J. G. (2017). On-cloud healthcare clinic: an e-health consultancy approach for remote communities in a developing country. Telematics and Informatics, 34(1), 311-322.
[13] Sahu, Aditya Kumar & Swain, Gandharba. (2019). Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis. International Journal of Electronic Security and Digital Forensics. 11. 10.1504/IJESDF.2019.10021739.
[14] Saidhbi, S., & Rao, K. T. (2017). A Modern Approach in Cloud Computing Storage by Using Compression and Crypto Mechanism. International Journal of Applied Engineering Research, 12(9), 1815-1818.
[15] Niraja, K. S. & Murugan, C. S. & Prabhu. (2017). Security Risks in Internet of Things: A Survey. 1-7. 10.1109/ICCIC.2017.8524355.
[16] Goldreich, O. (1998). Secure multi-party computation. Manuscript. Preliminary version, 78.
[17] Luo, W., & Bai, G. (2011, September). Ensuring the data integrity in cloud data storage. In 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (pp. 240-243). IEEE.
[18] Vurukonda, Naresh & Rao, Dr. B. Thirumala. (2017). Hash counter hash method for privacy and security in cloud computing with attribute-based encryption. Journal of Advanced Research in Dynamical and Control Systems. 9. 281-289.
[19] Naga Divya, Lakshmi & Ahamed, Shakeel. (2018). A novel chaotic hash-based attribute-based encryption and decryption on cloud computing. International Journal of Electronic Security and Digital Forensics. 10. 1. 10.1504/IJESDF.2018.089203.
[20] Tarasvi Lakum and B. Thirumala Rao, “A Key-Ordered Decisional Learning Parity with Noise (DLPN) Scheme for Public Key Encryption Scheme in Cloud Computing” International Journal of Advanced Computer Science and Applications(IJACSA), 10(11), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0101121

Acknowledgements
Authors extends the heartfelt wishes to Koneru Lakshmaiah Education Foundation for the constant encouragement and motivation.