Proceedings of the International Conference on Sustainable Computing and Smart Systems (ICSCSS 2023)
IEEE Xplore Part Number: CFP23DJ3-ART; ISBN: 979-8-3503-3360-2

2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS) | 979-8-3503-3360-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSCSS57650.2023.10169776

Privacy-Aware Artificial Intelligence with Homomorphic Encryption using Machine Learning

1. Dr.B. Srinivasa Rao,
Professor, Department of Computer Science and Engineering, Bachupally, Hyderabad, Telangana, India.
bsrgriet2015@gmail.com

2. Saumitra Chattopadhyay,
Assistant Professor, Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India.
Schattopadhyay@gehu.ac.in

3. Prashant Singh,
UG Scholar, Department of Computer Science and Engineering, Amity School of Engineering and Technology Lucknow, Amity University, Uttar Pradesh, India.
er.prashant0001@gmail.com

4. Bramah Hazela, Assistant Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology Lucknow, Amity University, Uttar Pradesh, India.
bramahhazela77@gmail.com

5. G. Sabarinathan,
Associate Professor, Department of Mathematics, PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India.
sabarinathan.g@gmail.com

6. Kalva Yamini,
Assistant Professor, Cyber Security in Computer Science and Engineering, Sri Ramachandra Institute of Higher Education and Research, Chennai, Tamilnadu, India.
yam190697@gmail.com

***Abstract*—Along with the expansion of machine learning (ML) applications, the amount of data required to create predictions increases. Big-data ML has always been limited by off-chip memory capacity and computational speed. Considerably, privacy is one of the limitations of big data, which can be solved by homomorphic encryption (HE). Due to the combination of HE and ML, the multi-party privacy-protected ML suggested in this research may assist numerous users in doing artificial intelligence (AI) without disclosing private data. The technique may train common models in situations of data abuse, particularly in private data protection. The model trained using the ML technique named Artificial Neural Network (ANN) has a similar impact to the model developed using all data on a single computer, according to experiments using the algorithm. The gradient data is simply transmitted by all parties, and homomorphic procedures in the main computing system combine the gradient data. Besides, the optimal key is selected using the significance of the Lion Algorithm (LA). After homomorphic procedures, the learning model is modified depending on the new gradient data.**

Keywords*— *Artificial Intelligence, Homomorphic Encryption, Machine Learning, Privacy, Artificial Neural Network

I. INTRODUCTION

Data privacy has emerged as one of the most important challenges in the big data age. Many security measures and encryption methods have been developed to date in an effort to protect sensitive data [1]. Also, the majority of their security plans make the assumption that only those who own secret keys may access the private data. Nevertheless, with the widespread usage of ML, particularly centralised ML, data needs to be gathered and sent to a central location in order to train an effective model. Thus, the danger of data leakage will always exist for such private and sensitive data. A crucial problem for sharing information is how to do ML on confidential datasets without causing data leakage [2].

In order to ensure the security of their own data, ML with multi-party privacy protection might assist users of all parties in learning together using each other's data. AI is a typical example of one of them that might assist in resolving the privacy issues associated with multi-party computation [3]. The crucial enabling technologies are what make AI more pervasive and improve the efficiency of human operations. For instance, gesture recognition is a data-driven application in human-computer interaction that uses ML algorithms to do temporal tracking and 3D hand modelling. It has been used to manage multimedia applications and portable devices. Moreover, trained screen touch data and a classifier based on the AI algorithm that provides ongoing authentication are key security elements in touch-enabled devices [4]. Fig. 1 explains the application of HE in the healthcare industry.

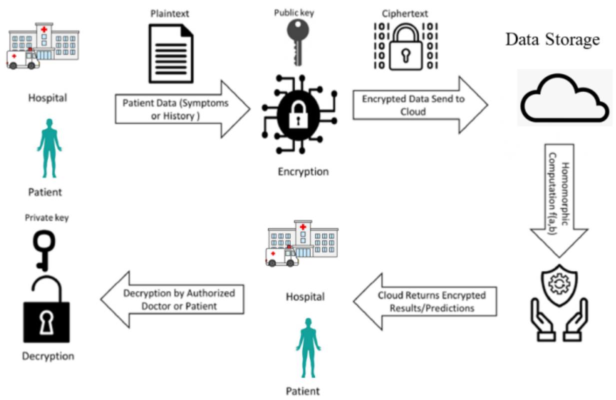

Fig. 1 Application of HE in Healthcare Industry

With HE, ciphertexts may be processed mathematically without having to be decrypted. With the help of the HE technique, the central server may update the homomorphic operation-based global model parameters and use the encrypted local gradients. Since it sends the encrypted local gradients to the server, the distributed ML participants, also known as clients, are free from worrying about data leaking through local gradients [5] [6]. Homomorphic procedures, meanwhile, may only be carried out between values encrypted with the same public key in the mL-based approach; therefore, the clients should share a single private key [7]. In this study, the LA-ANN ML technique is created, which uses HE to provide privacy protection. There are several possibilities in real-world applications for the multi-party privacy-protected ML based on HE that are suggested in the study.

The key contributions of the study are stated below.

- In essence, multi-party privacy is used to secure the gradient learning process used to jointly train the model.
- Each iteration of the model is specifically improved using gradient descent, and by sending the gradient, one can benefit from the data of other users.
- Together with HE, the proposed LA-ANN model is used to enable data security with enhanced accuracy.
- Also, the developed system is compared with traditional systems in terms of computation time, key length, and accuracy.

The rest of the paper is organized as given as follows. Section II deals with the literature regarding previous and recent research in HE and ML models. Section III presents the proposed architecture of HE with the ML model and the traditional and proposed methodologies. Besides, the experimental analysis and the attained results are demonstrated in Section IV. Finally, Section V concludes the paper.

II. Literature Review

A. Related Works

In 2020, F. Turan et al. [8] developed a HE approach using HEAWS, a domain-centric coprocessor system, to speed up homomorphic function estimation on encrypted information. An efficient and simultaneous coprocessor system for the FV HE technique, which has grown in popularity for doing precise arithmetic on the encrypted data, was created by utilising the enormous size of the Amazon FPGAs. Lastly, an ANN for five times faster energy consumption forecasting in a smart grid application was introduced.

In 2020, J. Park et al. [9] addressed a reinforcement learning (RL) model to enhance privacy in cloud systems. Moreover, facilitation for arithmetic operations on cloud systems without needing to decode ciphertexts was implemented. Users were only permitted to provide ciphertexts to the cloud computing (CC) system through the HE scheme in order to access RL-based applications. Several CC-based intelligent service scenarios were used to conduct performance analysis and assessment for the proposed PPRL architecture.

In 2020, Y. Su et al. [10] suggested a Fully HE (FHE) model using the Ring Learning with Errors (RLWE) problem. In this research, a fast implementation of the levelled FHE scheme and the development of a high parallelism architecture based on an FPGA to accelerate the FHE schemes were provided. Both circuit- and block-level pipeline solutions increase clock frequency, which in turn accelerates the processing speed of polynomial multipliers and homomorphic evaluation functions in order to decrease computation latency and boost performance.

In 2020, A. C. Mert et al. [11] presented an FHE approach with Brakerski/Fan-Vercauteren (BFV) HE techniques. The BFV HE system was accelerated using high-performance polynomial multipliers using two hardware designs. In comparison to former implementations, the suggested system speeded up the offloaded encryption and decryption procedures by nearly 12- and 7-times the delay, respectively.

In 2021, Ha Eun David Kang et al. [12] pointed out a HE model to preserve the privacy of small and medium manufacturing enterprises (SMEs). A 2-party cooperative architecture for safe in-house PHM analytics contracting for SMEs was provided. After this, while maintaining the privacy of the sensor information, the frequency-based peak recognition system (H-FFT-C), which created a system health diagnostic and medication report, was provided.

In 2020, Qizhong Li et al. [13] introduced a robust Cramer Shoup Delay Optimised Fully Homomorphic (RCS-DOFH) to preserve privacy. There were three phases to this process. The Robust Cramer Shoup Decryption (RCSD) technique reduces communication overhead and time. Next, a Delay Optimised Fully Homomorphic Encryption (DOFHE) technique was developed to reduce data latency and network delay. This method calculates the delivery delay between the base station and the signal from an IoT device.

TABLE I. Features And Challenges Of Recent Researches in Privacy-Aware Helathcare Systems

Authors	Methods	Merits	Demerits
F. Turan *et al.* [8]	The HEAWS Model	Established five times faster energy consumption	Hard to implement in real-time systems
J. Park *et al.* [9]	RL	Outperformed existing models	Exhibited high computation time
Y. Su *et al.* [10]	RLWE	Computation latency was decreased Boost performance was used	Revealed complex architecture
A. C. Mert *et al.* [11]	BFV	Attained minimized delay	Exposed computational cost
Ha Eun David Kang *et al.* [12]	H-FFT-C	Achieved privacy aware system	Yet, accuracy of implementation is low
Li, *et al.* [13]	RCS-DOFH	Delivery delay was minimized	Computational complexity limited the performance

B. Review

Table I summarizes the merits of demerits of recent privacy aware models in healthcare systems. In the former implementations, most of the HE approaches used standard and ML HE approaches to enable a privacy-aware data transmission system. These advancements in the secure transmission system provided intrusion free as far as privacy-enabled services. However, complications in the form of time delay, accuracy, and computational cost play a vital role in real-time implementation which drastically limits efficiency. Thus, there is still room for advancements and developments are present in the privacy-aware secure transmission of data.

III. A Novel Privacy-Aware Model using LA-ANN-HE Approach

A. *Proposed Architecture*

Fig. 2 delivers the basic architecture of the implemented model. Initially, the gradient learning method used to jointly train the model is secured via multi-party privacy. Generally, gradient descent is used to precisely enhance each model iteration, and by sharing the gradient, one may take use of other users' data. The suggested LA-ANN model is utilised in conjunction with HE to offer data security with improved accuracy. Unscrupulous individuals in the training might build a shadow model using the plaintext gradient in order to jeopardize the privacy of other users' data, according to the member inference attack. In order to counter this threat, we develop HE, which enables one to conduct computations on encrypted data without having to decode it. Hence, the homomorphic operation's outcome upon decryption is identical to the operation on the plaintext data. The security of private data may be ensured because, during the whole homomorphic operation procedure, the operation is unable to identify the data being operated. The accuracy, calculation time, and key length of the created system are also evaluated in comparison to those of conventional systems

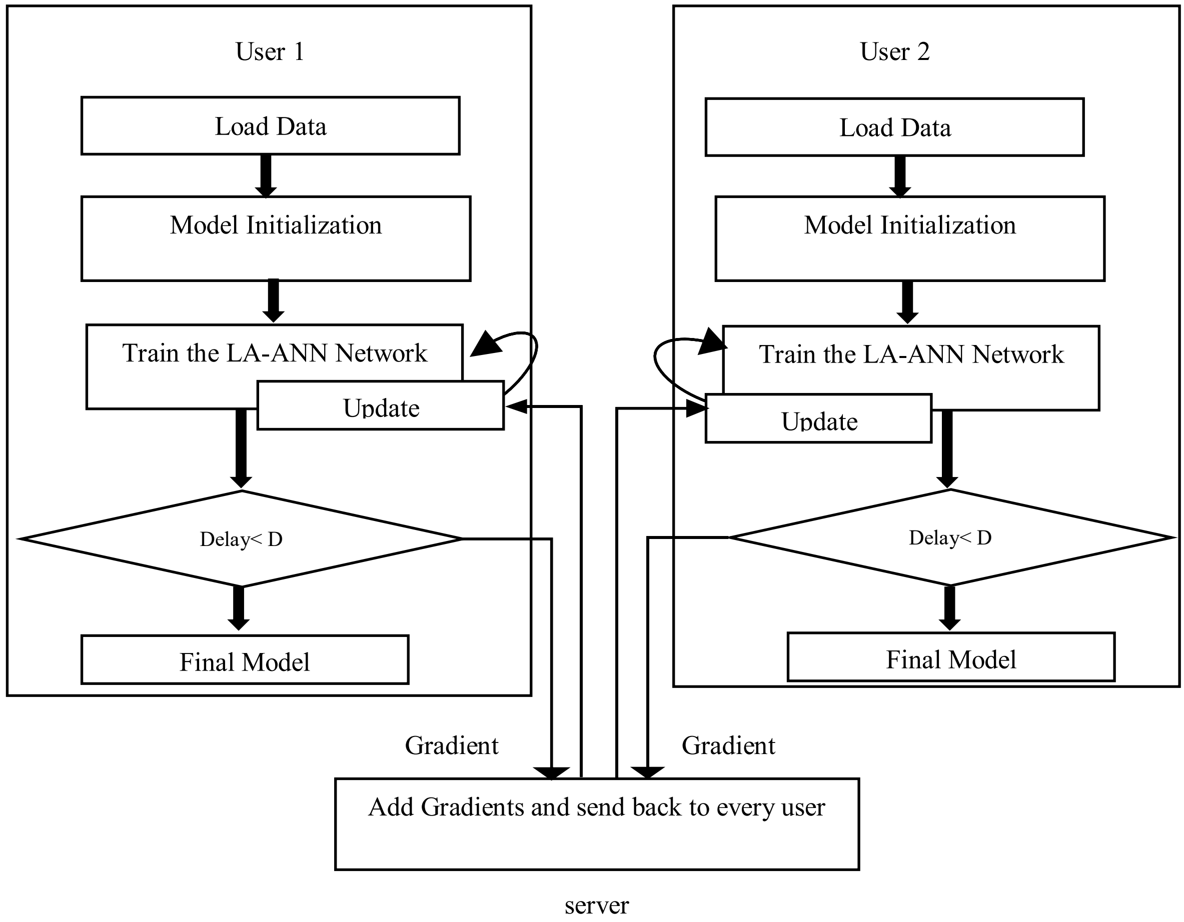

Fig. 2 Systematic Representation of Proposed Model

B. *The ANN Architecture*

Since networks can draw conclusions from a complex and apparently an unconnected set of facts, self-learning that results from experience may occur in networks. Fig. 3 depicts the basic architecture of NN.

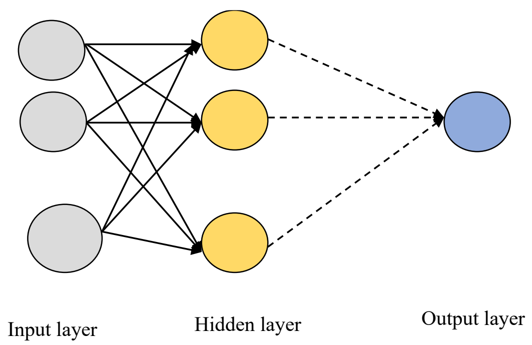

Fig. 3 Basic Architecture of NN

Eq. (1) presents the mathematical model of ANN [14], in which d_i represents weight, B_i indicates bias, and a_i signifies input data. Based on Eq. (1), an estimate of ANN's output is made in Eq. (2),

$$\sum_{i=1}^{N} d_i a_i + B_i = d_1 a_1 + d_2 a_2 + \cdots + d_N a_N + B_i \quad (1)$$

$$o(a) = \begin{cases} 1 & if \quad \sum d_1 a_1 + B \geq 0 \\ 0 & if \quad \sum d_1 a_1 + B < 0 \end{cases} \quad (2)$$

Once the input layer has been determined, weights are applied. With larger weights having a higher effect on the outcome than smaller ones, these weights help determine the proportional importance of each variable. Each input is given the appropriate weight before being amplified as a whole. As a result, once the result has been passed through it, the outcome is calculated using an activation function. By using a softmax activation function, an extension of the logistic function, the outputs of the Neural Network (NN) (or a softmax component in a component-based network) for categorical target variables may be interpreted as posterior probabilities. As it offers a level of categorization certainty, this is advantageous for classification. The softmax activation function of an ANN is given by Eq. (3).

$$b_i = \frac{e^{a_i}}{\sum_{j=1}^{N} e^{a_j}} \quad (3)$$

Now, the parameters of ANN such as weight, batch size, Neurons (in every layer), and learning rate are optimized to enhance the performance so as to ensure the privacy-enabled system using LA. ANN model is employed to detect the authenticated and vulnerable data sharing over the network. Also, optimization concept is used to enhance the performance of ANN model. The model is initiated at every iteration of the optimization algorithm while executing the fitness function.

C. The LA

The LA [15] model used to optimise the DBN's hidden neurons is presented in this section.Fig. 4 delivers the flowchart of LA model.

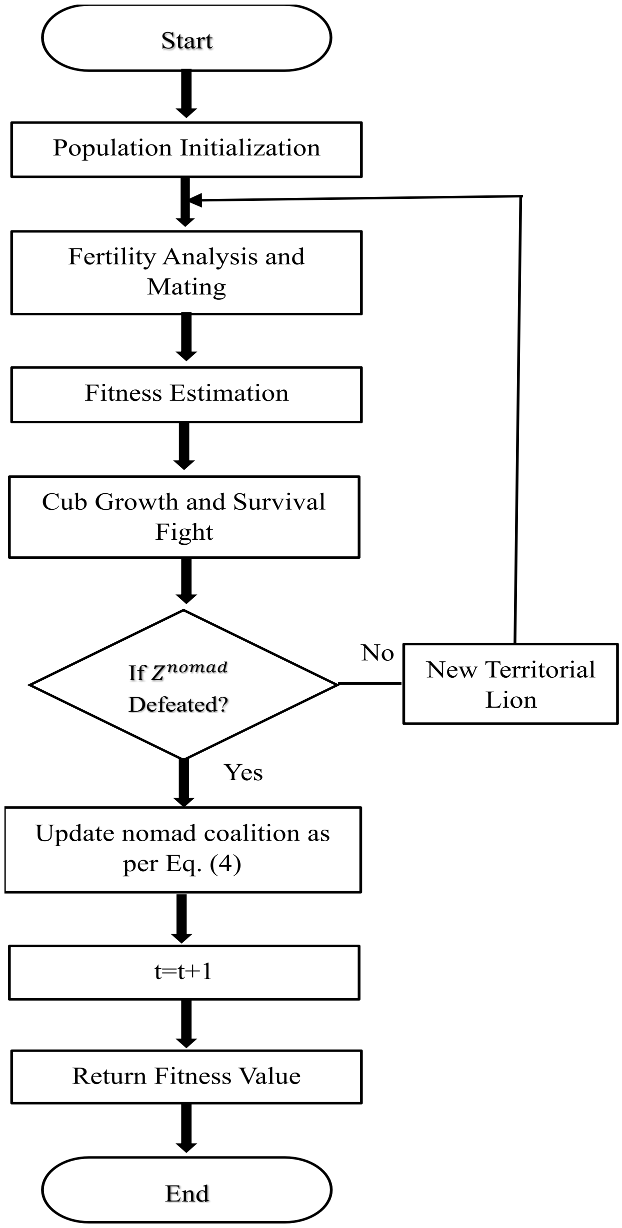

Fig. 4 Flowchart of LA

The mathematical formulation is provided below, and LA is generally based on the biological behaviour of lions. It has five main stages, including the formation of a pride, evaluation of fertility, the lions' mating behaviour, territorial defence, territorial takeover, and algorithm termination. At this point, the notations Z^{male}, Z^{female}, and Z^{nomad} indicates the territorial male, female and nomadic lions respectively. The lower and upper limits of the lions for $N > 1$ are specified as Z_k^{male}, Z_k^{female}, and Z_k^{nomad} with random integers, in which $k = 1,2, \dots, K$. Now, K refers to the lions' group length.

If $S_v > S_V^{max}$, then female update takes place as portrayed in Eq. (4). Here, S_V^{max} is the tolerance rate, $Z_k^{female+}$indicates the updated lioness. When the Z_k^{female} is replaced by $Z_k^{female+}$, the lioness update takes place. This process continues till the generation value $g_v > g_v^{max}$.

$$Z_k^{female+} = \begin{cases} Z_r^{female+} & for\ k = r \\ Z_k^{female+} & o.w \end{cases} \quad (4).$$

In fact, if no $Z_k^{female+}$ found over the entire process, then Z_k^{female} is considered a fertile one as stated in Eq. (5) and (6), in which $Z_r^{female+}$, and $Z_k^{female+}$ refers to the r^{th} and k^{th} vector elemennts of $Z^{female+}$ correspondingly. Besides, ω_1 and ω_2 are the arbitrary numbers in the range $[0,1]$, and r points out an arbitrary number in the range $[1, K]$.

$$Z_r^{female+} = \min[Z_r^{max}, \max(Z_r^{min}, \nabla_r)] \quad (5)$$

$$\nabla_r = \left[Z_r^{female} + (0.1\omega_2 - 0.05)\left(Z_r^{male} - \omega_1 Z_r^{female}\right)\right] \quad (6)$$

Using LA, the hyperparameters of ANN are optimized. Algorithm 1 shows the pseudocode of the propsoed privacy-aware HE model.

Algorithm 1: Pseudocode of Proposed Privacy-Aware HE Model

Input: Message to be transmitted

Output: Final Model M_{fin} from LA-ANN

1. Request key pairs (K) for encryption
   Generate keypairs (K)
2. Model parameter initialization M
3. For $i < T$ (where i stands for the current iteration and T denotes total iteration)
4. $O_i = ANN(a_i, M_i)$
5. Determine loss: $l_i = loss(f(a_i), O_i)$
6. If $l_i < D$ then
7. Break
8. Else
9. $G_i = ANN(a_i, O_i, l_i)$
10. $Encrypt(G_i) = Encrypt_p(public_{key}, G_i)$ (utilize the public key of user 1 for encryption of gradient G)
11. Transmit $Encrypt(G_i)$ to server and receive $Encrypt(G_{inew})$
12. $G_i = Decrypt_p\left(private_{key}, Encrypt(G_i)\right)$ (utilize the private key of user 1 for decryption of gradient G)
13. Update $M_{i+1} = M_i - LR * G_{new}$ (where LR stands for the learning rate of ANN)
14. End if
15. End for
16. Return M_{fin}

IV. Simulation Results

A. Simulation Setup

The proposed privacy-aware HE model using the ML approach was implemented in MATLAB on an Intel core® core i3 processor, 8 GB RAM, and 64-bit OS. The significance and efficiency of the developed method were implemented using simulated analysis. Besides, the analysis was implemented through various performance parameters such as accuracy, key length, delay, and cost. The efficacy of the proposed model is compared over various conventional models such as ANN [14], K-Nearest Neighbor (KNN) [16], Recurrent NN (RNN) [17], and Multi-Layer Perceptron (MLP) [18].

B. Algorithmic Analysis

Here, the proposed privacy-aware HE model using the suggested LA-ANN approach and the accomplished results are addressed. Fig. 5 demonstrates the accuracy of the transmitted message over user 1 and 2. The proposed model attained better accuracy which is 2.58%, 4.79, 4.24%, and 2.14% better than ANN, KNN, RNN, and MLP respectively. Fig. 6 reveals the time delay (D) of the proposed model which accomplished minimized delay of 3.05 minutes at the end of the iteration than other models. Besides, Fig. 7 depicts the key length of the proposed model. Here, the data used for implementation ranges from 5 MB to 25 MB. The proposed model used 3 unit key for 5 MB of data and 5 unit key for 25 MB of data. The unit represents the key length based on the keypairs (K) which got minimized key length than all other methods. Fig. 8 shows the cost of the proposed model which is 5.12%, 15.01%, 9.12%, and 7.51% improved than ANN, KNN, RNN, and MLP respectively. Finally, Fig. 9 exposed the time (Bps) of the proposed model which achieved minimized time to send every byte when compared with other models. Thus, the proposed model attained better performance than existing systems and proved its efficiency.

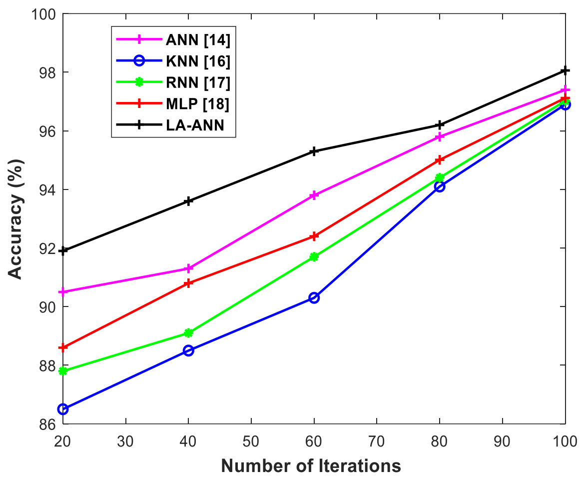

Fig. 5 Representation of Accuracy of Proposed Model over Other Models

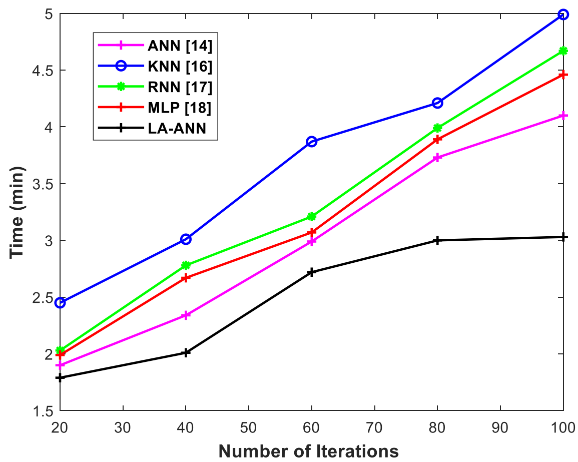

Fig. 6 Representation of Time Delay (D) of Proposed Model over Other Models

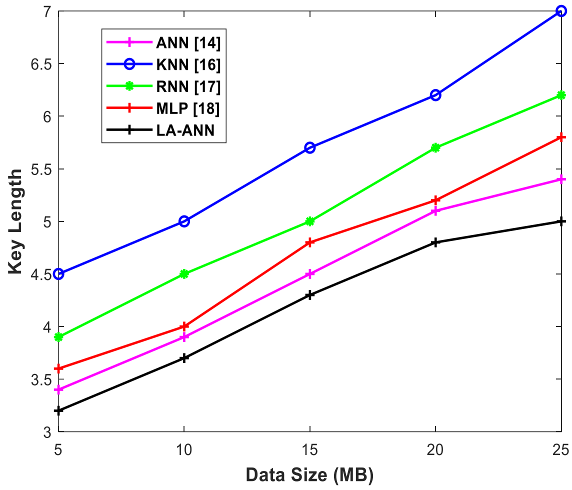

Fig. 7 Representation of Key Length of Proposed Model over Other Models

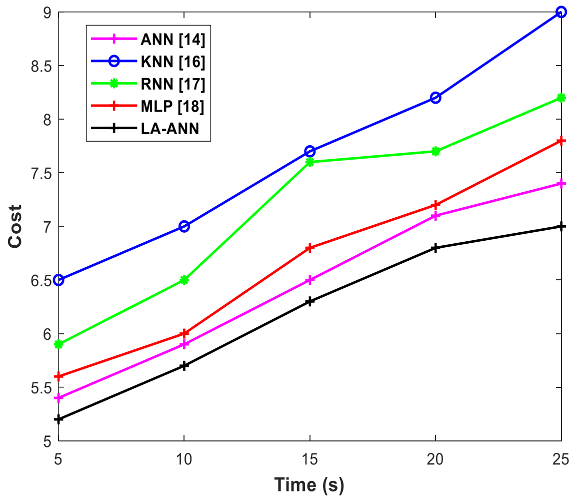

Fig. 8 Representation of Cost of Proposed Model over Other Models

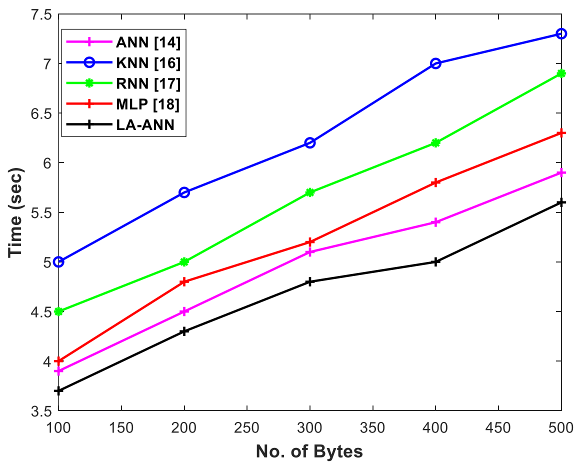

Fig. 9 Representation of Time in bytes per second (Bps) of Proposed Model over Other Models

V. Conclusion

This study established multi-party privacy to protect the gradient learning technique used to jointly train the model. Using the recommended LA-ANN model with HE allows for enhanced accuracy and data security. According to the member inference attack, dishonest participants in the training might create a shadow model utilizing the plaintext gradient to compromise the privacy of other users' data. HE makes it possible to do calculations on encrypted data without having to decode it, in order to combat this threat. Hence, the output of the homomorphic operation after decryption is the same as the operation on the plaintext data. A Comparison of the developed system to traditional systems was carried out concerning the accuracy, computation time, and key length. In the future, pre-processing steps will be taken place to enhance the algorithmic performance.

References

[1] I. Chillotti N. Gama M. Georgieva and M. Izabachène "TFHE: Fast fully homomorphic encryption over the torus" J. Cryptol. vol. 33 no. 1 pp. 34-91 Jan. 2020. doi.org/10.1007/s00145-019-09319-x

[2] A. Qaisar Ahmad Al Badawi Y. Polyakov K. M. M. Aung B. Veeravalli and K. Rohloff "Implementation and performance evaluation of RNS variants of the BFV homomorphic encryption scheme" IEEE Trans. Emerg. Topics Comput. Mar. 2019. DOI: 10.1109/TETC.2019.2902799

[3] Martin Albrecht, Melissa Chase, Hao Chen, Jintai Ding, Shafi Goldwasser, Sergey Gorbunov, Shai Halevi, Jeffrey Hoffstein, Kim Laine, Kristin Lauter, Satya Lokam, Daniele Micciancio, Dustin Moody, Travis Morrison, Amit Sahai, and Vinod Vaikuntanathan, "Homomorphic encryption standard" IACR Cryptol. ePrint Arch. vol. 2019 pp. 939 May 2019. doi.org/10.1007/978-3-030-77287-1_2

[4] S. S. Roy F. Turan K. Jarvinen F. Vercauteren and I. Verbauwhede "FPGA-based high-performance parallel architecture for homomorphic computing on encrypted data" 2019. DOI: 10.1109/HPCA.2019.00052

[5] K. Emura G. Hanaoka K. Nuida G. Ohtake T. Matsuda and S. Yamada "Chosen ciphertext secure keyed-homomorphic public-key cryptosystems" Des. Codes Cryptogr. vol. 86 no. 8 pp. 1623-1683 2018. doi.org/10.1007/978-3-642-36362-7_3

[6] M. Ibtihal and N. Hassan "Homomorphic encryption as a service for outsourced images in mobile cloud computing environment" in Cryptography: Breakthroughs in Research and Practice Hershey PA USA:IGI Global pp. 316-330 2020. doi.org/10.4018/IJCAC.2017040103

[7] X. Sun P. Zhang J. K. Liu J. Yu and W. Xie "Private machine learning classification based on fully homomorphic encryption" IEEE Trans. Emerg. Topics Comput. vol. 8 no. 2 pp. 352-364 Jun. 2020. DOI: 10.1109/TETC.2018.2794611

[8] F. Turan, S. S. Roy and I. Verbauwhede, "HEAWS: An Accelerator for Homomorphic Encryption on the Amazon AWS FPGA," IEEE Transactions on Computers, vol. 69, no. 8, pp. 1185-1196, 1 Aug. 2020. DOI: 10.1109/TC.2020.2988765

[9] J. Park, D. S. Kim and H. Lim, "Privacy-Preserving Reinforcement Learning Using Homomorphic Encryption in Cloud Computing Infrastructures," IEEE Access, vol. 8, pp. 203564-203579, 2020. DOI: 10.1109/ACCESS.2020.3036899

[10] Y. Su, B. Yang, C. Yang and L. Tian, "FPGA-Based Hardware Accelerator for Leveled Ring-LWE Fully Homomorphic Encryption," IEEE Access, vol. 8, pp. 168008-168025, 2020. DOI: 10.1109/ACCESS.2020.3023255

[11] A. C. Mert, E. Öztürk and E. Savaş, "Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 353-362, Feb. 2020. DOI: 10.1109/TVLSI.2019.2943127

[12] Ha Eun David Kang, Duhyeong Kim, Sangwoon Kim, David Donghyun Kim, Jung Hee Cheon, and Brian W.Anthony, "Homomorphic Encryption as a secure PHM outsourcing solution for small and medium manufacturing enterprise", Journal of Manufacturing Systems, Available online 19 June 2021. doi.org/10.1016/j.jmsy.2021.06.001

[13] Qizhong Li, Yizheng Yue, and Zhongqi Wang, "Deep Robust Cramer Shoup Delay Optimized Fully Homomorphic For IIOT secured transmission in cloud computing", Computer Communications, Vol. 161, pp. 10-18, 1 September 2020. doi.org/10.1016/j.comcom.2020.06.017

[14] Díaz, E, Brotons, V, Tomás, R, "Use of artificial neural networks to predict 3-D elastic settlement of foundations on soils with inclined bedrock", Soils and Foundations, Vol. 58, No. 6, pp. 1414–1422, September 2018. doi.org/10.1016/j.sandf.2018.08.001

[15] Rajakumar Boothalingam, "Optimization using lion algorithm: a biological inspiration from lion's social behaviour", Evolutionary Intelligence, Vol. 11, pp. 31–52, 2018. doi.org/10.1007/s12065-018-0168-y

[16] Jiasen Liu, Chao Wang, Zheng Tu, Xu An Wang, Chuan Lin, and Zhihu Li, "Secure KNN Classification Scheme Based on Homomorphic Encryption for Cyberspace", Security and Communication Networks, Vol. 2021, 2021. doi.org/10.1155/2021/8759922

[17] R. Podschwadt and D. Takabi, "Non-interactive Privacy Preserving Recurrent Neural Network Prediction with Homomorphic Encryption," 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Chicago, IL, USA, 2021, pp. 65-70, doi: 10.1109/CLOUD53861.2021.00019.

[18] Ali, Hassan; Javed, Rana Tallal; Qayyum, Adnan; AlGhadhban, Amer; Alazmi, Meshari; Alzamil, Ahmad; et al. (2022): SPAM-DaS: Secure and Privacy-Aware Misinformation Detection as a Service. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.19351679.v1