ISSN: 2182-2069 / E-ISSN: 2182-2077

Strengthening Financial Cloud Security with ML-Driven Data Hiding Strategy

Shikha Singh[1*], Akash Kumar Bhagat[2], Wamika Goyal[3], Dr. Shashikant Patil[4], M.S. Nidhya[5], and Dr. Mohit Sharma[6]

[1*]Assistant Professor, Department of Computer Application, Anand Engineering College, Agra, India. shikhasinghjyoti@gmail.com, https://orcid.org/0000-0002-2750-8328

[2]Assistant Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India. akash.b@arkajainuniversity.ac.in, https://orcid.org/0000-0001-8717-764X

[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. wamika.goyal.orp@chitkara.edu.in, https://orcid.org/0009-0004-8729-7464

[4]Professor, Department of uGDX, ATLAS SkillTech University, Mumbai, Maharashtra, India. shashikant.patil@atlasuniversity.edu.in, https://orcid.org/0000-0002-8835-908X

[5]Associate Professor, Department of Computer Science and Information Technology, Jain (Deemed to be University), Bangalore, Karnataka, India. ms.nidhya@jainuniversity.ac.in, https://orcid.org/0000-0002-1290-4520

[6]Associate Professor, Symbiosis Law School, Noida, Symbiosis International (Deemed University) Pune, India. mohit9826@gmail.com, https://orcid.org/0000-0001-7576-2200

Received: April 08, 2025; Revised: May 21, 2025; Accepted: July 10, 2025; Published: August 30, 2025

Abstract

Data hiding is a modern paradigm that efficaciously hides a class or module's implementation details, revealing just the essential information to the outdoors world. It improves security and encapsulation by proscribing access to sensitive records and procedures, lowering unintended intrusion, and supporting modular design principles. In this research, we aim to develop an innovative machine learning (ML)-driven data hiding strategy for financial cloud security. We propose a new Secured Dynamic Paillier Federated Neural Network (SDPFNN) encryption algorithm to overcome the data hiding problem in distributed ML (DML) included economic cloud packages with embedded structures. Initially, research gathered a dataset that includes financial transaction data from various organizations to train our suggested model. The data cleaning procedure is conducted to pre-process the gathered raw data. Our recommended encryption approach prevents individuals from recognizing encrypted data. We present a technique for mapping the original data into high-dimensional space. We conducted results analysis using different metrics to assess the effectiveness of the suggested model. To determine the efficiency of the suggested strategy, research performed a comparative study with other comparable methodologies. The experimental findings demonstrate that the proposed model outperforms conventional approaches.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 18-31.
DOI: *10.58346/JISIS.2025.I3.002*

*Corresponding author: Assistant Professor, Department of Computer Application, Anand Engineering College, Agra, India.

Keywords: Data Hiding, Machine Learning (ML), Secured Dynamic Paillier Federated Neural Network (SDPFNN), Security, Financial, Cloud Computing.

1 Introduction

Cloud computing technologies, including financial cloud computing, have emerged as the de facto method for training neural networks. Some ML service providers, such as Google, to speed up neural network operations on cloud servers (Netto et al., 2018; Shrestha et al., 2023; Sehgal et al., 2022). They promote the uploading of datasets to cloud storage. However, this business model has two issues (Karimov & Bobur, 2024). Cloud ML applications are useful to customers, however each upload can only employ algorithms that are developed by the service provider (Narayanan & Muthukumar, 2022). Hardware on cloud servers restricts the resources, and this cannot be changed under extreme load. Despite the initial resolution, certain individuals lack the required proficiency to create superior models for self-improvement. The fixed efficiency of the commercial models does not satisfy customers. To make consumers' services superior, they want to go further with more advanced and different algorithms (Aldhyani & Alkahtani, 2022) The second method is not sufficient in terms of computing resources. Consequently, a distributed machine learning (DML) system that utilizes embedded devices (EDs) is suggested. On EDs, the cloud service provider functions merely as an intermediate between the algorithm owner and the data publisher (Sehgal et al., 2022; Shrivastava & Ahmed, 2024).

There are major security problems with DML systems, especially in financial cloud computing. Sensitive personal information, such as an identity number or bank card password, could be exposed (Kaur & Chandra, 2024). Meanwhile, there's a chance that patented algorithms could leak (Elankavi et al., 2017). The system's unauthorized nodes can steal data and models through the exchange of information (Ma et al., 2018).

Financial cloud safety facts covering techniques are vulnerable to sophisticated cyberattacks. Even when personal information is concealed, skilled hackers can nonetheless proceed to gain weaknesses by using insider threats or sophisticated decryption (Ren et al., 2021). System scalability and performance can be impacted by means of implementation complexity and control problems (Sharma & Iyer, 2023). Robust encryption, admission to limits, and ongoing tracking need to all be included in a comprehensive protection strategy to overcome these drawbacks. Therefore, even though statistics hiding improves protection, it nonetheless calls for complementing strategies to correctly mitigate risks (Thabit et al., 2023).

The objective of this study is to provide a novel data-hiding approach for financial cloud security that is powered by ML. Research propose a new encryption algorithm called Secured Dynamic Paillier Federated Neural Network (SDPFNN) (Pillai & Panigrahi, 2024).

There are five sections in the structure. In Section 2, the related work is discussed. Section 3 provides a detailed explanation of the methods. A detailed outline of the study's results is given in Section 4. Section 5 provides a conclusion.

2 Related Works

Luo et al., 2021 provided a singular approach that targeted "separable records-hiding techniques for encrypted pix the use of block compressive sensing (SDH-EI-BCS)". The suggested technique minimizes the machine's complexities and enhances its performance in compression, reduction of facts loss, and hiding functionality.

Xu et al., 2022 provided a progressive "Reversible statistics hiding in encrypted pics (RDHEI)" approach that makes use of the "median facet detector (MED)" and a newly advised "hierarchical block variable period coding (HBVLC)" approach.

Moyou Metcheka & Ndoundam, 2020 delivered a novel steganography strategy that proves each obvious to capability attackers and was resistant to identification and secret restoration. The research provided thrilling comparative findings that spotlight huge protection benefits.

Mawgoud et al., 2022 examined data security in ad hoc cloud platforms utilizing deep learning (DL) and an enhanced steganography method. The effectiveness of the established ad-hoc system was greater than that of Amazon AC2, and the deep steganography method demonstrated an excellent assessment rate for data and image suppression when verified beside multiple attacks in an ad-hoc cloud system atmosphere (Kapoor & Malhotra, 2025).

Chen & Chi, 2019 presented a sophisticated information-hiding strategy that applied the “block truncation coding (BTC)” photograph compression method. Based on research results, the counseled technique achieves higher than traditional methods in terms of embedding capacity and image great assessments.

Luo et al., 2021; Liu et al., 2019; Ma et al., 2018 presented a "deep neural network-based invisible textual content steganalysis (DNNITS)" approach for hiding business records. The outcomes validated that, in assessment to other traditional techniques, the counseled DNNITS model more advantageous in the extraction charge, significance charge, performance ratio, and performance ratio, consider ratio, and reduced error charge.

Jose & Subramanian, 2021 presented a fuzzy-based encryption method with high-capacity reversible data stored in encrypted images. Convolutional neural networks (CNN) process texture classification to classify clear solid areas. Implementation studies showed that the new model outperformed the traditional methods in terms of power areas and maximum signal-to-noise ratio.

Hameed et al., 2023 provided an image steganography technique that provides high privacy by successfully hiding the secret records inside a cowl photo employing the “Least Significant Bit Substitution (LSB)” and “Nature-Inspired Harris Hawks Optimisation (HHO)” algorithm. Comparing the suggested approach with traditional LSB or multi-directional Pixel value differencing (PVD) embedding techniques showed that it was more optimized and had a greater embedding capacity while preserving the visual appearance.

3 Methods

3.1 Dataset

The dataset we use consists of 81 manually analyzed 10-K reports, comprising 1355 sentences with 4522 items and 3841 relations. A 10-K report is an annual report issued by publicly traded companies detailing their financial achievements (Deußer et al., 2022).

3.2 Preliminaries for DML

The design of the DML method is initially explained in this section. Subsequently, we explain why the structure's model hiding and data hiding problems need to be resolved.

3.2.1 DML Framework with Integrated Devices

Hardware and the default algorithms of the service provider restrict the cloud servers' computational capacity. Research suggest a DML system to address this issue; this system differs from DML on diverse computing systems. In cloud ML, the business pattern has changed. Our system is based on computer networks. $H = \langle U_d, F_d \rangle$ represents the structure of a computer network. Here U_d signifies the union of three distinct sets as displayed in Figure 1 ML server node u_0, dataset publishing node sets $\{u_{11}, u_{12}, \ldots, u_{1m}\}$, and computer node sets with computational resources $\{u_{21}, u_{22}, \ldots, u_{2m}\}$. Through the internet, ML server node u_0 obtains datasets from $u_{1j}, 1 \leq j \leq m$, and posts the task data. The ML server u_0 receives an automatic request from the computer that satisfies task criteria $u_{2i}, 1 \leq i \leq n$, and then sends the dataset to computer u_{2i} over the internet. u_{2i} offers a DL technique to train the dataset. Following the completion of training, the ED transmits the DL model back to the ML servers, which use the validation dataset to give the computer a certain amount of money. Finally, the server delivers the DL model back to the dataset publisher node.

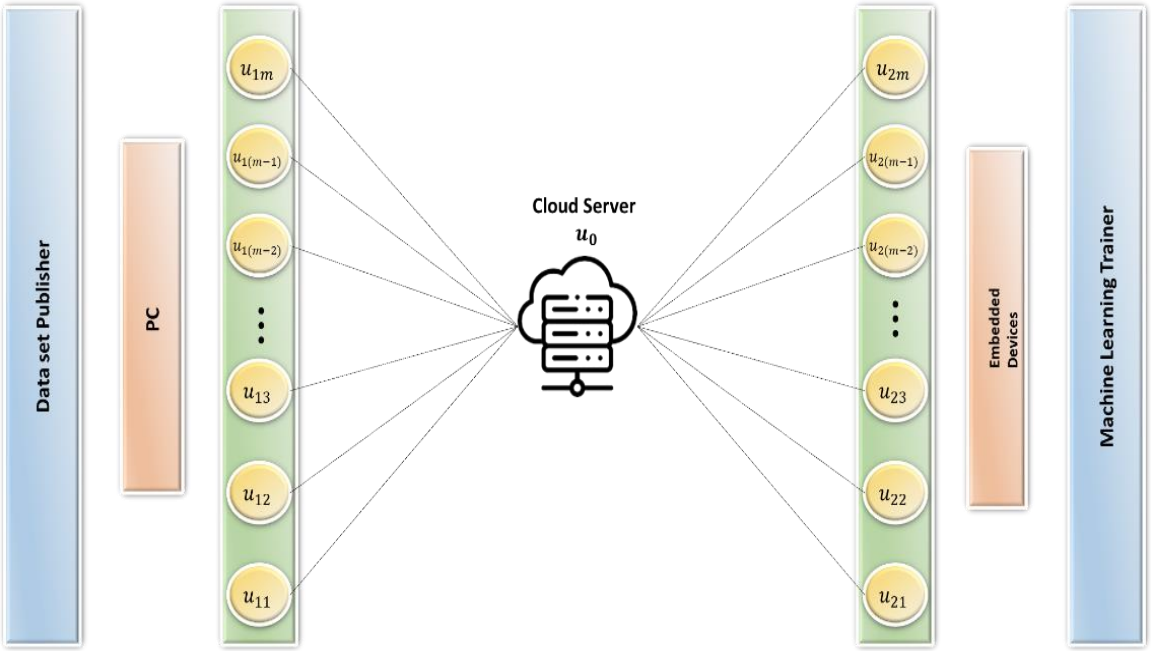

Figure 1: Architecture of the DML System

In this design, the ML server does not require computational assets. It serves as an intermediate between algorithm implementation and data (Figure 1).

- u_{2i} - Publisher of the DL model and a user of the dataset,
- u_{1j} - Publisher of the dataset and the user of the trained DL model.

Our approach has no server resource limitations in contrast to the cloud ML systems. It may assist in the dataset publishers' search for particular algorithms. The system encourages algorithm developers to take an active role in algorithm validation.

3.2.2 Model Covering

Users of computer $u_{2i}, 1 \leq i \leq n$ want their confidential training algorithms to remain private. To communicate with the dataset publisher and the DL model publisher, u_{2i} serializes the model into an international format (such as ONNX). The DL model's algorithm may be hidden since the universal

formatted model lacks the optimization technique and data augmentation procedure. The u_{1j} node is unaware of the precise training algorithm, whereas the u_{2i} node is capable of training the model. (The image categorization system of a research group is tested on computer u_{21}. Then, without revealing the training procedure, the algorithm is trained using data obtained from ML service provider u_0, creates an ONNX file, and sends it back to u_0 for validation). Our technology provides good protection for the secret training algorithm. The secret training technique is only known by u_{2i}.

3.2.3 Data Hiding

To preserve private and sensitive data, publishers with datasets of the format $u_{1j}, 1 \leq j \leq m,$ have users who do not want others to have access to the information of their datasets. Research create an encryption algorithm for hiding data. However, using such an encryption method for hiding data will lead to issues with neural network training. Because this approach modifies the dataset's initial distribution, the neural network's accuracy decreases significantly. Thus, FHE is suggested by certain researchers. Nevertheless, there is no applicability of the existing FHE in DL algorithms. As a basic model, only certain models can be utilized. In the remaining portion of the study, research emphasize the training accuracy of encrypting data and provide our encrypt approach (SDPFNN) to enhance neural network reliability on encrypted datasets.

3.3 Formulation of the Problem and its Solution

The mathematical basis of the SDPFNN is provided in this section. In the final phase, research suggest parameters for assessing an encryption scheme's effectiveness.

3.3.1 Data Hiding Problem

An objective function $E(w)$, a set of constraint functions $D_j(w)$, and a vector of parameters w comprise the three main parts of an optimization problem. Finding a specific value for the parameter vector w that maximizes $E(w)$ while fulfilling each of the constraint functions $D_j(w)$, as represented below in Equations (1-3).

$$\min E(w) \tag{1}$$

$$D_j(w) \leq 0, j \in M \tag{2}$$

$$D_j(w) = 0, j \in R \tag{3}$$

Where $w \in Q^m, Q, M, R$ represents the sets of real numbers, indices for in-equality constraints (ECs), and indices for ECs.

Typically, research utilize an iterative technique with a low learning rate to increase $E(w)$. Research need to make sure the outcome meets the limitations after every iteration. In real-world situations, most restriction functions cannot be represented analytically. While backpropagation in neural networks is used to address optimization problems with clear gradient data (GD), evolutionary algorithms are typically employed to solve optimization problems with no GD. It is only unconstrained optimization issues that both of them can address. Constrained optimization problems are challenging to reduce to unconstrained optimization issues depending on particular issues. Constrained optimization problems like data hiding exist. The problem's objective is to increase the gap between the encrypted data distribution function (DF) $h(w)$ and the initial data DF $e(w)$. The problem's restriction is that DL algorithms can still identify the encrypted data $h(w)$ with great accuracy. The limitation is the concept of ensuring algorithm adaptability in DML systems. The remainder of the study concentrates on simplifying the data-hiding issue so that a neural network can resolve it.

3.3.2 Federated Neural Network Algorithm

This research proposes a federated learning network whose primary goal is to facilitate the cooperative training of a single model by transmitting intermediate parameters across parties during training. Research select gradients as its intermediate variables in this instance since gradient descent is the training method used for the majority of neural networks. Model training is facilitated by the gradient's ability to show the connection among the model and the data, even when it is not able to specifically represent all of the data.

3.3.2.1 Computing Server (CS)

The CS operates as an intermediary network during the process of learning. Acquiring the GD from several LCs, calculating the gradients, connecting the data acquired by various models, and sending the outcome to each LC independently are the major activities.

3.3.2.2 Learning Client (LC)

LCs use their confidential data to initialize a model, train locally, extract gradients, compute gradients, acquire responses, transfer outcomes, update the model, and repeat until the model merges.

3.3.3 Federated Neural Network

The "Federated Multi-layer Perceptron (FMLP)" is a method that uses gradient sharing to train a basic model for every LC in multi-party information emptiness situations. A standard DL model is the MLP, which is often referred to as a "deep feed-forward network".
Where, lr - Training's learning rate,

$$\theta = \{x_1 \dots \dots x_m, a_1 \dots \dots a_m\} \text{ - Model's parameter,}$$

$$w = \{w_1 \dots \dots . w_m\} \text{ - Data set.}$$

The model's goal is to approximate a given distribution e^*. The network's forward operation is used to determine the training output, which can be characterized as shown in Equation (4),

$$out = fp(w, \theta) \tag{4}$$

The following is a description of the loss function that determines the difference among the ideal value and the output shown in Equation (5),

$$d = loss(e^*(w), out) \tag{5}$$

Calculating and propagating gradients from the loss function backward is the purpose of back-propagation, assisting the network in modifying parameters by the gradient to lower the fault among the perfect one and output value. "Back-propagation" could be described as shown in Equation (6),

$$grad = bp(w, \theta, d) \tag{6}$$

The procedure for updating models includes changing the system's factors by the gradient that results from backpropagation, which is represented in Equation (7).

$$\theta' = \theta - lr.grad \tag{7}$$

A federated MLP (FMLP) can be obtained through the federated network that MLP achieved. Subsequently, every LC has a reproduction of the MLP classical deposited locally. The input data's feature dimensions determine the size of the output layer, which has m hidden levels with z units each, and an input layer with w units. Furthermore, the size of y is determined by the network's needed output, which is strongly correlated with the goal outcome of the actual requests.

The CS's primary purpose is to combine the GD, allowing the system to speed up the Descending gradient with each customer serving as a teaching tool. Every LC transfers the gradients to the CS for classical preparation before the classical is modified. Furthermore, the CS then combines all of the client-provided GD and sends each client a newly computed gradient for updating the model. The model converges when the client loss is less than ϵ, and the same federated model is available to all clients.

3.3.4 Paillier Federated Neural Network

This research proposes a federated network that enables several participants to work together on isolated data to accomplish cooperative ML. In reality, however, it requires both the final model that has been trained by numerous parties and the data that the participants have provided.
Through server data, they gain access to the server and derive many shadow models. Finally, using these shadow models, they may establish its ensemble learning theory on a forecast that resembles the model shown through real-world collaboration. To clarify, the federated model in this instance is limited to resolving data security issues and does not address model safety.

As a result, homomorphic encryption could potentially used in federated learning to ensure model safety. Furthermore, the fundamental principle of homomorphic encryption is that the outcome of certain procedures on d in the "ciphertext (CT)" space, following the encryption of plaintext (PT) b to CT d, is equal to the outcome of encryption functions on an in the PT space is described in Equation (8),

$$F(b)\oplus F(a) = F(b \otimes a) \tag{8}$$

b and a are two distinct plain messages, while F is an encryption technique. Operators are represented by $\oplus$ and $\otimes$. Multiplicative homomorphisms, such as the algorithm, are satisfied by homomorphic encryption when an operation is a multiplication process. The additive homomorphism is achieved by the homomorphic encryption technique if the operation is an addition process. The most popular method is the Paillier algorithm. Moreover, the encryption technique accomplishes full homomorphism if it simultaneously satisfies additive and multiplicative homomorphism. Homomorphic encryption can be achieved using the Paillier technique because the MLP requires us to sum the GD.

3.3.4.1 Improved Paillier Algorithm

However, the effectiveness of network training will be impacted by the Paillier algorithm's high level of difficulty when it comes to decryption and encryption. Consequently, research employ a refined iteration of Paillier and the accuracy and effectiveness of the optimization.

Key generation - The "private key" can be replaced with λ by using $\propto$ as the divisor. We can change h in the public key to make sure that h is in the correct sequence, $\propto m$.

Encryption - Considering that q is a random positive integer, d is the CT, n is the PT, and q is less than α. The enhanced encryption method is demonstrated in Equation (9),

$$d = h^n . q^m mod\ m^2 \tag{9}$$

Decryption - The decryption procedure can be represented in Equation (10),

$$n = \frac{K(d^\alpha mod m^2)}{K(h^\alpha mod m^2)}\ mod\ m \tag{10}$$

These approaches demonstrate that the primary benefit of utilizing α over λ is the ability to decrypt data. The quantity of control activities has shifted from $2.\lambda$ times to $2.\alpha$ times. The time overhead has been greatly decreased because α is a divisor of λ. Native Paillier has a computational complexity (CC) of $\mathcal{O}(|\mathrm{m}|^3)$, while enhanced Paillier has a CC of $\mathcal{O}(|\mathrm{m}|^2||\alpha|)$.

3.3.4.2 Architecture of the Paillier Federated Neural Network

To safeguard the GD, research employ Paillier encryption (PE). As a result, even if crackers gain access to the CS, they will be unable to obtain particular information regarding the GD from every LC. Furthermore, crackers cannot utilize encrypted GD for training shadow models.
Since PE necessitates key sets, research incorporate a "key management center (KMC)" into the algorithm to produce and maintain key pairs.

3.3.5 Paillier Federated Neural Network

The fundamental architecture of PFMLP and FMLP are very comparable. Before training begins, the LC should request the KMC meanwhile PFMLP necessities to communicate with the KMC. After confirming that every participant is online, the KMC creates key pairs and sends them back to the LCs. Every LC uses encrypted data to execute multi-party ML after obtaining the key pairs. Figure 2 displays the PFMLP flow chart.

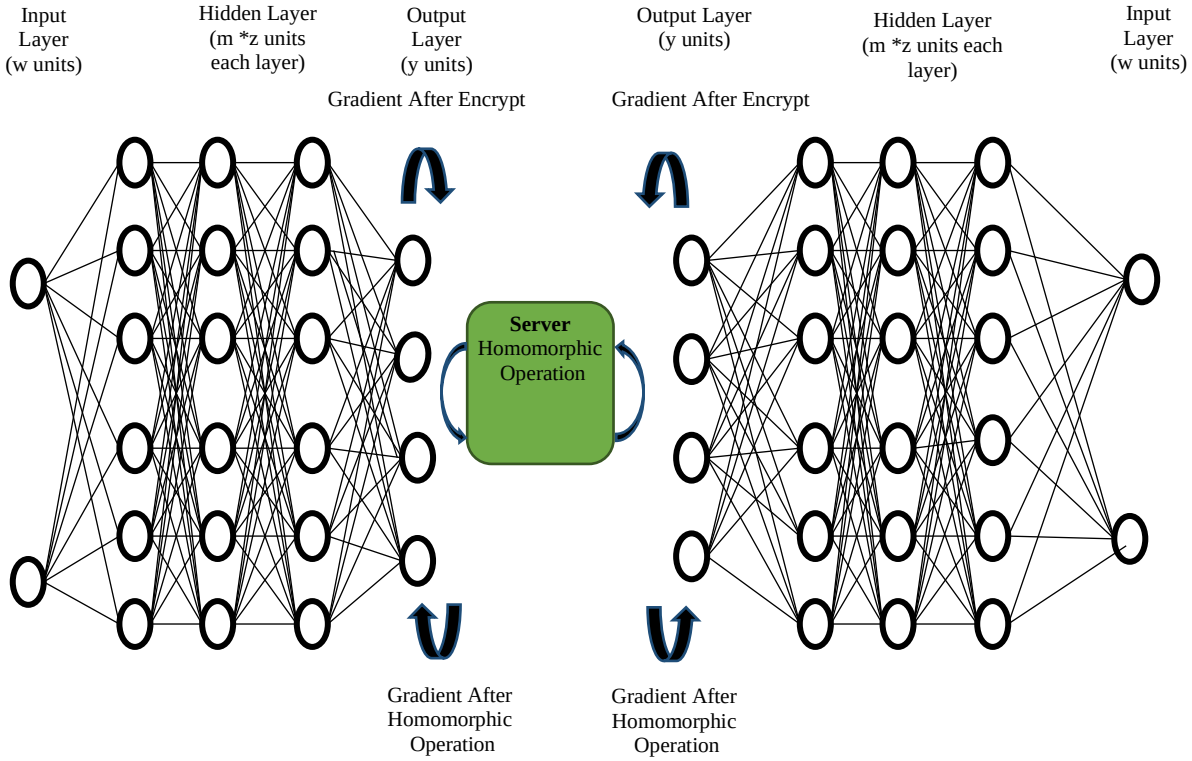

Figure 2: Flow Chart of Paillier Federated Neural Network

PFMLP includes an additional three sections in comparison to FMLP. (1) LCs' encryption and decryption processes, (2) Homomorphic functions within the CS, and (3) In the KMC, key pairs are generated and distributed. PFMLP involves KMC, CSs, and LCs.

The LC computes the gradient for every learning iteration but fails to modify the local model instantly. The GD is homomorphically encrypted before being transmitted to the CS. After the server completes the homomorphic functioning, it waits for the newly encrypted GD to be returned. In the decryption stage, the client may modify every LC's local model with the latest gradient after decrypting

the newly encrypted GD. Therefore, the new gradient indirectly comprises the private data of other clients to indirectly safeguard the data privacy.

The GD is encrypted using PE by PFMLP, thus even in the event that a hacker compromises the CS, the leaked data only displays the encrypted version of the GD, $Enc(grad)$. As a result, inference attack risk can be reduced.

Every LC provides encrypted GD, which is processed homomorphically by the CS. Furthermore, the CS processes the encrypted data through homomorphic operations and transfers the outcomes back to the client upon receiving a request from the client. All of these provide data privacy throughout model training because the CS does not receive the key during the entire procedure.

4 Result

The SDPFNN encryption technique is used in the experimental setup for financial cloud security. Python was chosen for implementation due to its flexibility and large package. For the system to accommodate the computational needs of neural network operations and encryption, a minimum RAM capacity of 16 GB is needed. The proposed method is compared with the existing methods such as ResNet 50, and VGG 16 (Singh et al., 2023).

The F1-score measures the balance of precision and recall when measuring efficacy. It offers a single number that expresses the model's capacity to find pertinent data and reduce false positives. The evaluation of the proposed and existing f1-score procedures is shown in Fig. 3. By comparing our proposed methodology with the existing ResNet 50 (93.2%) and VGG sixteen (88.7%) methodologies, research might achieve an SDPFNN rating of 96.8%. This indicates that our approach for strategy hiding approach for financial cloud safety is higher (Figure 3).

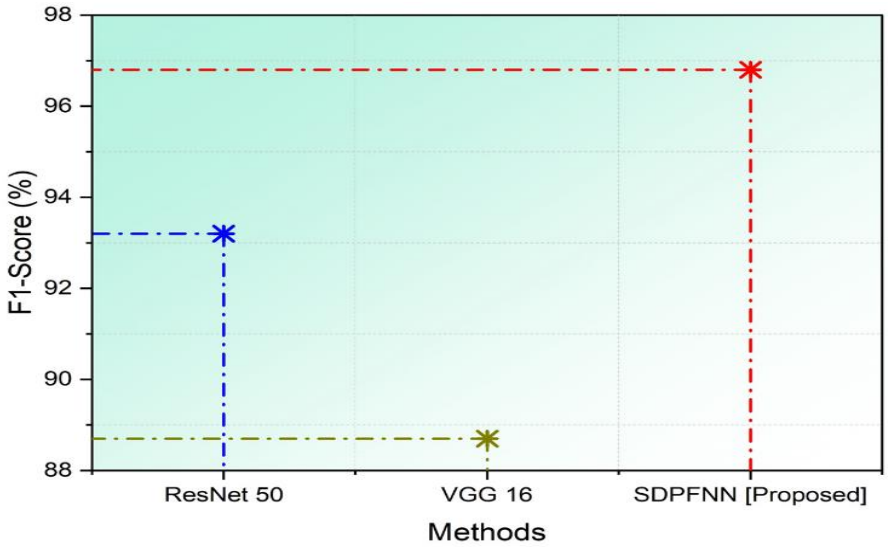

Figure 3: Output of F1-score

The accuracy evaluates the precision with which private monetary records are hidden inside cloud systems, in addition to the effectiveness of safety methods in defensive facts privateness and security. The accuracy assessment of the recommended and current techniques is proven in Figure 4. Comparing our proposed methodology to the present ResNet 50 (94.5%), VGG sixteen (90.5%) tactics, research will achieve an SDPFNN rating of 95.8%, proving our superiority for the records hiding approach for financial cloud security.

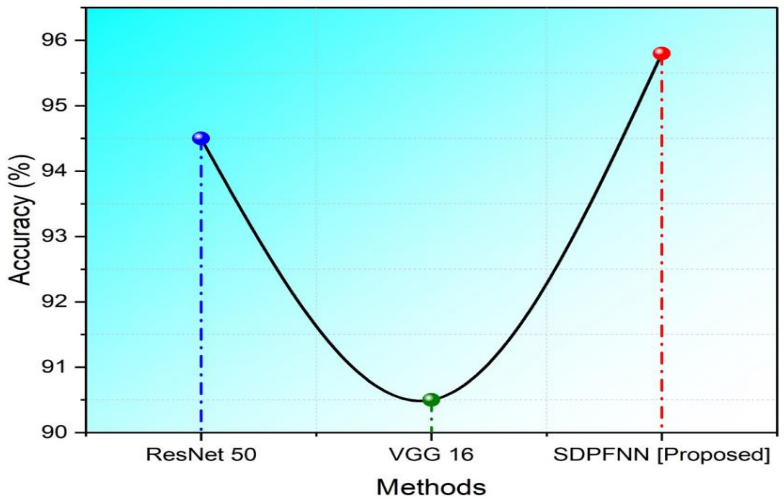

Figure 4: Result of Accuracy

The recall evaluates the percentage of pertinent hidden financial information that security protections in cloud systems properly identify, demonstrating the efficacy of hiding sensitive data. In Figure 5, the recall evaluation of the proposed and existing approaches is displayed. By comparing our proposed method with the present ResNet 50 (93.2%) and VGG sixteen (87.4%) methodologies, research could acquire an SDPFNN score of 97.1%. This suggests that our method for data hiding technique for financial cloud security is greater.

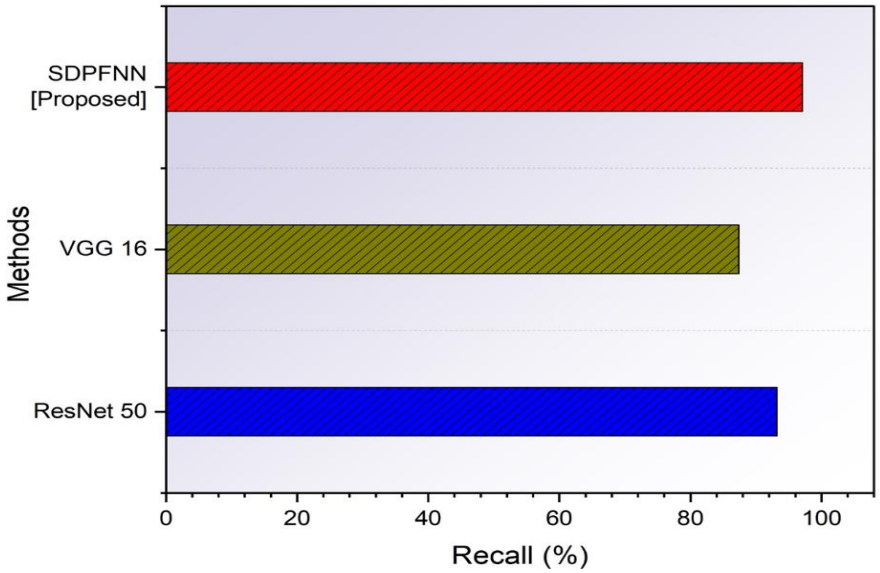

Figure 5: Output of recall

Precision evaluates the reliability with which sensitive financial data remains private within cloud systems, resulting in limited exposure or leakage, which is critical for protecting against unauthorized access and attacks. Figure 6 displays the precision evaluation of the proposed and existing techniques. Research can achieve an SDPFNN score of 95.6% by comparing our suggested methodology with the current ResNet 50 (92.6%) and VGG 16 (89.7%) approaches. This indicates that our technique is exceptional in phrases of facts hiding method for monetary cloud safety.

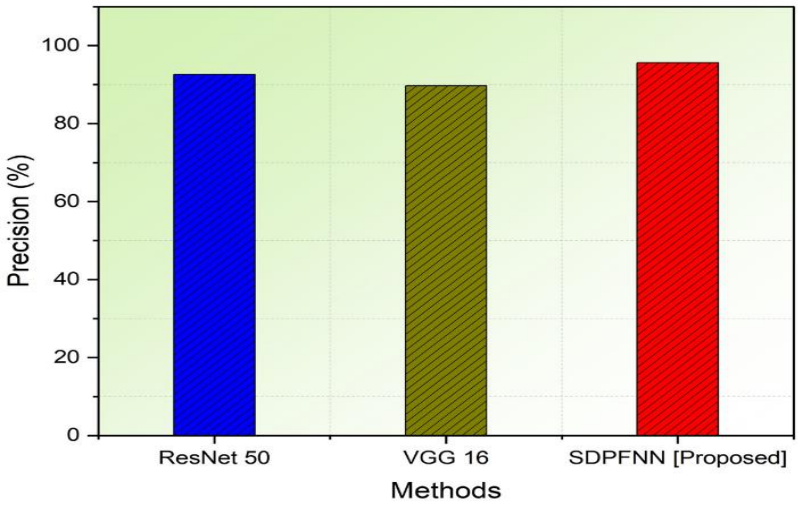

Figure 6: Result of Precision

5 Conclusion

The novel idea of statistics hiding protects the technical components of a class or module such that only the maximum critical facts are on the market in the outdoor world. In this observation, research added a completely unique encryption algorithm known as Secured Dynamic Paillier Federated Neural Network (SDPFNN) for hiding records in allotted ML-incorporated economic cloud programs. To evaluate the efficacy of the proposed methodology, research executed an outcomes analysis utilizing diverse metrics such as accuracy (95.8%), precision (95.6%), recall (97.1%), and F1-score (96.8%). The drawbacks involve a lack of resistance in opposition to state-of-the-art assaults as a result of in all likelihood defects in Paillier's encryption and statistics hiding approach, which threatens economic cloud protection. Future work will focus on strengthening data-hiding strategies, increasing financial cloud safety protocols to reduce vulnerabilities, and improving Paillier encryption to increase resilience against sophisticated attacks.

References

[1] Aldhyani, T. H., & Alkahtani, H. (2022). Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments. *Sensors*, *22*(13), 4685. https://doi.org/10.3390/s22134685

[2] Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., ... & Shen, H. (2018). A manifesto for future generation cloud computing: Research directions for the next decade. *ACM computing surveys (CSUR)*, *51*(5), 1-38. https://doi.org/10.1145/3241737

[3] Chen, Y. Y., & Chi, K. Y. (2019). Cloud image watermarking: high quality data hiding and blind decoding scheme based on block truncation coding. *Multimedia Systems*, *25*(5), 551-563. https://doi.org/10.1007/s00530-017-0560-y

[4] Deußer, T., Ali, S. M., Hillebrand, L., Nurchalifah, D., Jacob, B., Bauckhage, C., & Sifa, R. (2022, December). KPI-EDGAR: A novel dataset and accompanying metric for relation extraction from financial documents. In *2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 1654-1659). IEEE. https://doi.org/10.1109/ICMLA55696.2022.00254

[5] Elankavi, R., Kalaiprasath, R., & Udayakumar, R. (2017). A fast clustering algorithm for high-dimensional data. *International Journal of Civil Engineering and Technology (Ijciet), 8*(5), 1220-1227.

[6] Hameed, M. A., Abdel-Aleem, O. A., & Hassaballah, M. (2023). A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 4639-4657. https://doi.org/10.1007/s12652-022-04366-y

[7] Jose, A., & Subramanian, K. (2021). High-capacity reversible data hiding using quotient multi pixel value differencing scheme in encrypted images by fuzzy based encryption. *Multimedia Tools and Applications*, *80*(19), 29453-29479. https://doi.org/10.1007/s11042-021-11122-5

[8] Kapoor, P., & Malhotra, R. (2025). Zero Trust Architecture for Enhanced Cybersecurity. *Essentials in Cyber Defence*, 56-73.

[9] Karimov, Z., & Bobur, R. (2024). Development of a food safety monitoring system using IoT sensors and data analytics. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(1), 19-29.

[10] Kaur, K., & Chandra, G. (2024). Demographic Data Gaps and the Challenges of Population Modeling in Low-resource Settings. *Progression Journal of Human Demography and Anthropology*, *2*(1), 13-16.

[11] Liu, L., Wang, L., Shi, Y. Q., & Chang, C. C. (2019). Separable data-hiding scheme for encrypted image to protect privacy of user in cloud. *Symmetry*, *11*(1), 82. https://doi.org/10.3390/sym11010082

[12] Luo, Y., Yao, C., Mo, Y., Xie, B., Yang, G., & Gui, H. (2021). A creative approach to understanding the hidden information within the business data using Deep Learning. *Information Processing & Management*, *58*(5), 102615. https://doi.org/10.1016/j.ipm.2021.102615

[13] Ma, X., Zhang, F., Chen, X., & Shen, J. (2018). Privacy preserving multi-party computation delegation for deep learning in cloud computing. *Information Sciences*, *459*, 103-116. https://doi.org/10.1016/j.ins.2018.05.005

[14] Mawgoud, A. A., Taha, M. H. N., Abu-Talleb, A., & Kotb, A. (2022). A deep learning based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system. *Journal of Cloud Computing*, *11*(1), 97. https://doi.org/10.1186/s13677-022-00339-w

[15] Moyou Metcheka, L., & Ndoundam, R. (2020). Distributed data hiding in multi-cloud storage environment. *Journal of Cloud Computing*, *9*(1), 68. https://doi.org/10.1186/s13677-020-00208-4

[16] Narayanan, E., & Muthukumar, B. (2022). A machine learning framework for providing data integrity and confidentiality for sensitive data cloud applications. *International Journal of System Assurance Engineering and Management*, 1-12. https://doi.org/10.1007/s13198-022-01741-y

[17] Pillai, N., & Panigrahi, I. (2024). Global Health Security and SDG 3: Strengthening Pandemic Preparedness through South-south Cooperation. *International Journal of SDG's Prospects and Breakthroughs*, *2*(2), 10-13.

[18] Ren, W., Tong, X., Du, J., Wang, N., Li, S. C., Min, G., ... & Bashir, A. K. (2021). Privacy-preserving using homomorphic encryption in Mobile IoT systems. *Computer Communications*, *165*, 105-111. https://doi.org/10.1016/j.comcom.2020.10.022

[19] Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (2022). Cloud computing and information security. In Cloud Computing with Security and Scalability. *Concepts and Practices* (pp. 113-146). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-07242-0_7

[20] Sharma, A., & Iyer, R. (2023). AI-powered Medical Coding: Improving Accuracy and Efficiency in Health Data Classification. *Global Journal of Medical Terminology Research and Informatics*, *1*(1), 1-4.

[21] Shrestha, R., Bajracharya, R., Mishra, A., & Kim, S. (2023). AI accelerators for cloud and server applications. In *Artificial intelligence and hardware accelerators*, 95-125. https://doi.org/10.1007/978-3-031-22170-5_3
[22] Shrivastava, V., & Ahmed, M. (2024). The Function of the Blockchain System in Enhancing Financial Integrity and the Confidence of Society. *Global Perspectives in Management*, *2*(4), 36-45.
[23] Singh, A., Mushtaq, Z., Abosaq, H. A., Mursal, S. N. F., Irfan, M., & Nowakowski, G. (2023). Enhancing ransomware attack detection using transfer learning and deep learning ensemble models on cloud-encrypted data. *Electronics*, *12*(18), 3899. https://doi.org/10.3390/electronics12183899
[24] Thabit, F., Can, O., Wani, R. U. Z., Qasem, M. A., Thorat, S. B., & Alkhzaimi, H. A. (2023). Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms. *Concurrency and Computation: Practice and Experience*, *35*(21), e7691. https://doi.org/10.1002/cpe.7691
[25] Xu, S., Horng, J. H., Chang, C. C., & Chang, C. C. (2022). Reversible data hiding with hierarchical block variable length coding for cloud security. *IEEE transactions on dependable and secure computing*, *20*(5), 4199-4213. https://doi.org/10.1109/TDSC.2022.3219843

Authors Biography

Shikha Singh is an Assistant Professor in the Department of Computer Application at Anand Engineering College, Agra, India. With a strong academic background and a passion for teaching and research, her interests include computer science education, software engineering, and emerging technologies in computing. She is dedicated to fostering innovative thinking among her students and contributing to the academic community through scholarly work.

Akash Kumar Bhagat is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. His academic and research interests span areas such as computer science education, data analytics, and information technology. He is committed to promoting quality education and actively engages in research and development to contribute to the evolving field of computer science.

Wamika Goyal is affiliated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. Her work focuses on enhancing research quality and societal impact through evidence-based approaches and interdisciplinary collaboration. She is engaged in supporting academic initiatives that drive innovation and measurable outcomes.

Dr. Shashikant Patil is a Professor in the Department of uGDX at ATLAS SkillTech University, Mumbai, Maharashtra, India. With extensive academic and research experience, he specializes in areas related to design, innovation, and technology-driven education. Dr. Patil is committed to nurturing creative thinking and interdisciplinary learning, contributing significantly to both academic development and industry-oriented skill advancement.

M.S. Nidhya is an Associate Professor in the Department of Computer Science and Information Technology at Jain (Deemed-to-be University), Bangalore, Karnataka, India. With a strong academic foundation and a dedication to excellence in teaching and research, her interests include data science, machine learning, and advanced computing technologies. She actively contributes to scholarly activities and aims to bridge the gap between academic research and real-world applications.

Dr. Mohit Sharma is an Associate Professor at Symbiosis Law School, Noida, a constituent of Symbiosis International (Deemed University), Pune. He brings rich academic and research experience in the field of law, with particular interests in legal education, interdisciplinary legal studies, and contemporary legal reforms. Dr. Sharma is actively involved in guiding students and contributing to academic discourse through his research and publications.