DOI: https://doi.org/10.52756/ijerr.2024.v39spl.015 *Int. J. Exp. Res. Rev.*, Vol. 39: 190-199 (2024)

Original Article | *Peer Reviewed* | *Open Access*

International Journal of Experimental Research and Review (IJERR)
© Copyright by International Academic Publishing House (IAPH)
ISSN: 2455-4855 (Online)
www.iaph.in

Providing Highest Privacy Preservation Scenario for Achieving Privacy in Confidential Data

Pinkal Jain*, Vikas Thada and Deepak Motwani

Department of Computer Science & Engineering, Amity University Gwalior -474001, Madhya Pradesh, India

E-mail/Orcid Id:

PJ, pinku029jain@gmail.com, https://orcid.org/0000-0001-8002-320X; *VT,* vthada@gwa.amity.edu, https://orcid.org/0000-0002-8131-9616; *DM,* dmotwani@gwa.amity.edu, https://orcid.org/0000-0002-0217-7155

Article History:

Received: 24th Dec., 2023
Accepted: 25th May, 2024
Published: 30th May, 2023

Keywords:

Confidential Data, Data Modification, Machine Learning, Noisy Data, Privacy, Privacy Preservation

How to cite this Article:
Pinkal Jain, Vikas Thada and Deepak Motwani (2024). Providing Highest Privacy Preservation Scenario for Achieving Privacy in Confidential Data. *International Journal of Experimental Research and Review*, *39*(spl.) 190-199.
DOI:
https://doi.org/10.52756/ijerr.2024.v39spl.015

Abstract: Machine learning algorithms have been extensively employed in multiple domains, presenting an opportunity to enable privacy. However, their effectiveness is dependent on enormous data volumes and high computational resources, usually available online. It entails personal and private data like mobile telephone numbers, identification numbers, and medical histories. Developing efficient and economical techniques to protect this private data is critical. In this context, the current research suggests a novel way to accomplish this, combining modified differential privacy with a more complicated machine learning (ML) model. It is possible to assess the privacy-specific characteristics of single or multiple-level models using the suggested method, as demonstrated by this work. It then employs the gradient values from the stochastic gradient descent algorithm to determine the scale of Gaussian noise, thereby preserving sensitive information within the data. The experimental results show that by fine-tuning the parameters of the modified differential privacy model based on the varied degrees of private information in the data, our suggested model outperforms existing methods in terms of accuracy, efficiency and privacy.

Introduction

IoT devices are data-driven, and the world should concentrate more on safeguarding data than anything else. The cybersecurity law developed in 2017 contains a stipulation regarding personal privacy protection, including the personal information of network operators. The illegal use of sensitive information, i.e., personal information, is prohibited by law (Jain et al., 2023). Furthermore, in 2018, the European Union issued substantial directives governing how businesses handle personal data. These principles require the ethical treatment of individual information, creating trust and responsibility in data management procedures, and making it illegal for business models to gather, exchange, or analyze data without the user's permission (Abadi et al., 2016; Jain et al., 2023). Beyond legal methods to avoid information leaks, effective privacy protection in ML needs the unique properties of ML itself (Bettini and Riboni, 2015; Mondal et al., 2023). It necessitates building model structures and training procedures with privacy protection as a top priority, guaranteeing that sensitive personal information is inaccessible to unauthorized parties throughout the learning process.

Traditional machine learning techniques have a centralized method, with data collectors gathering information from numerous sources before being examined by data specialists (Feng et al., 2019; Samadder et al., 2023). This method is known as centralized learning (Fig. 1). First, In the centralized learning paradigm, after collecting data, users can hardly have control over the data

*Corresponding Author: pinku029jain@gmail.com and don't know how the data will be used or where it will be used (Gupta et al., 2020). Second, in the modern environment, scholars have tried computing global models using localized data. For instance, federated learning by Google has been in use since 2017. Despite giving users partial power over their private data, this definition does not enable users to mitigate privacy vulnerabilities fully (Owusu et al., 2021).

At the same time, privacy protection in machine learning is ensured using differential privacy algorithms and their diverse modifications. Differential privacy is improved by researchers from three primary perspectives: differential privacy based on gradients, function-based differential privacy, and label-based differential privacy (Truex et al., 2019; Kumar et al., 2023). In all cases, differential privacy is based on a shared goal, which is to add specific noise in diverse ways and directions when zeroing in on the machine learning process (Pei et al., 2022; Pal et al., 2023).

Majorly, few authors have creatively developed ADLM, a new differential privacy immune mechanism. During the training, ADLM dynamically adjusts the noise level by boosting the noise in insufficiently correlated neurons. Therefore, while this modification led to a striking improvement in model accuracy, it reduced the accuracy value by reporting 84.8 percent performance in the CIFAR-10 dataset (Jain et al., 2022). Furthermore, few authors implement a novel deep learning approach for semi-supervised learning using knowledge transfer techniques (Claerhout et al., 2005). To achieve high model accuracy and other robust protections for privacy, train several teacher models on different data sets to predict their deployment. They add noise to the student model while training, and the student model with high accuracy needs an accurate teacher model (Bu et al., 2021).

Although there are many privacy-preserving algorithms developed to ensure high levels of data privacy, adding noise may actually lead to a decrease in a model's ability to fit data with high accuracy (Miller et al., 2009). Such a trade-off between data authenticity and privacy security can considerably decrease the performance of machine learning models based on the classifications. Recently, advanced intelligent data or pattern recognition technologies, especially deep learning, have become drastically popular. Advanced intelligent data recognition technologies, particularly deep learning, have attracted significant attention (Zheng et al., 2017). This facilitates improved prediction accuracy in differential privacy models. Given these insights, this article proposes a novel approach to safeguarding privacy through the integration of differential privacy with convolutional networks. In addition to enhancing privacy protection, this method improves data availability; it still protects sensitive information in the datasets. In addition, it can restore

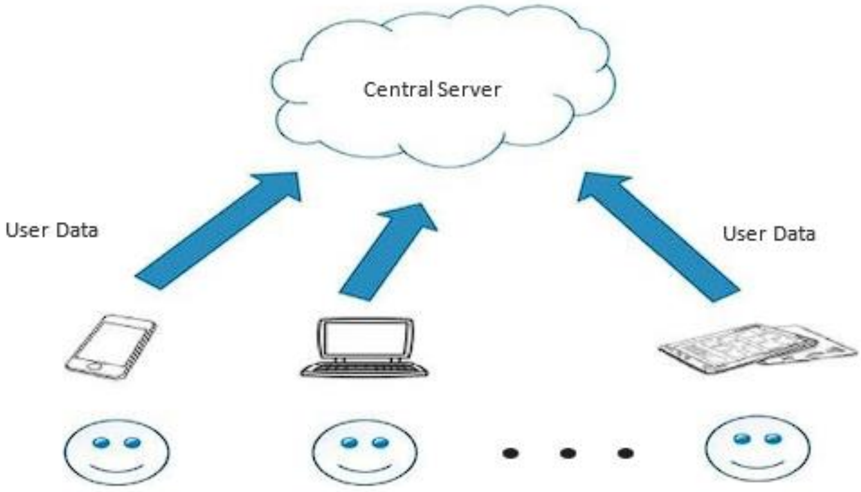

Figure 1. Centralized Learning Process: A Central Server Collects Data from Numerous Sources.

For example, Abadi and colleagues used the method to define the connection between the relationships and stabilize the gradient descent amplifications to maintain privacy. The challenge associated with the method was its inability to concentrate on complex models. In addition, the optimization of the DP-GAN method adds noise-protected data to the gradient calculation through the Wasserstein distance (Shokri et al., 2015). Despite the current use of the generators to improve the quality of the training data, the approach has effectiveness issues on complex datasets. Moreover, Jain and coworkers further used privacy methods, including the new layer of privacy reporting and the gradient descent-based global sensitivity computing layer. In addition, the addition of the network layer, which had limitations on complex networks (Wang et al., 2020; Yadav and Singh, 2023).

training in very small sample sizes for large sample sizes by a multi-factor of ORd4, which lowers the success of the attack. These are the only types of attacks available prior to our study and are only usable via equation-solving methods, most effective on a simple linear binary model (Wang et al., 2020).

Therefore, the paper contains a literature review in Section 2, a comprehensive presentation of our algorithm in Section 3, methodology in Section 4, results and discussion in Section 5, and a conclusion in Section 6.

Literature Review

Following are the privacy challenges and how machine learning methodologies are applied to mitigate them:

Navigating Privacy Challenges

The quick evolution of data processing has raised security fears regarding sensitive information from many quarters. In the domain of machine learning, confidential data breaches commonly appear in two ways:

Direct Privacy Disclosure

These stem from extensive data collection practices by untrustworthy data collectors who acquire personal data and share or trade data without individuals' consent (Zhu et al., 2020).

Indirect Privacy Disclosure

This arises from the inadequate generalization ability of machine learning models. In a significant advancement, they developed ADLM, a novel mechanism for differential privacy protection (Jain et al., 2023).

The adjustment mentioned above uniquely boosted the accuracy, which reached an outstanding 84.8% when applied to the CIFAR-10 dataset. Furthermore, there is a deep learning mechanism that uses knowledge distillation-based techniques. They designed a novel approach for training deep learning models by training multiple teacher models with different datasets and combining their predictions to introduce noise while training the model. Not only does this approach guarantee high model accuracy, but it also guarantees strong privacy protection. However, having accurate student-teacher models requires highly accurate teachers, who need data to train the model. However, they developed a novel mechanism for differential values called ADLM (Pei et al., 2022). This compromise between data authenticity and privacy security could ultimately harm the classification accuracy of a machine-learning model.

Advanced intelligent data recognition technologies, notably deep learning, have sparked great interest and allow for enhanced prediction accuracy in differential privacy models. Given these findings, this study presents a novel technique for protecting privacy by combining differential privacy with convolutional networks. This technique not only improves the accuracy of data but also increases its availability (Feng et al., 2019). It can reconstitute training with small sample numbers while reducing the efficacy of attacks with large samples. Early model theft attacks are generally based on equation-solving algorithms (Kairouz et al., 2019).

Reconstruction Attack

Adversaries attempt to recreate sensitive details or a specific model for individuals from training datasets. These initiatives involve techniques, including model inversion attacks and model theft (Gupta et al., 2020). Model inversion attacks attempt to extract sensitive information about people via dynamic analysis or similarity evaluations. The model uses data to strengthen defences against such breaches, using confidence algorithms to detect built-in virtual profiles to disclose genuine data. Model-stealing attacks use early methods based on equation-solving techniques, but they can be expanded to complicated models with predictive confidence (Arachchige et al., 2019).

Member Inference Attack (MIA)

Attackers seek to check whether a given sample correlates with the training dataset. Such inference can have serious repercussions, such as diagnostic models created with sensitive medical data (Yuan et al., 2013). In this case, the attacks are primarily motivated by the similarity between data distribution and model structures.

In addition to the privacy preservation risks, machine learning suffers from several security challenges. Unlike privacy issues, which can lead to data leaks, security flaws can jeopardize the operation and accuracy of machine learning models (Jain et al., 2022). Poisoning and anti-sample attacks are two security concerns that might occur during the model training and application stages.

Machine Learning for Privacy Preservation

Privacy preservation scenarios are responsible for privacy disclosure, require suitable methods to protect privacy, and need to consider some scenarios to obtain an approach. These two factors play a vital role in executing these approaches: the first is reliability, which depends on the distribution of training data, and the second is that the model outperforms noise (Zhu et al., 2020; Malin et al., 2004).

Machine Learning Techniques

Machine learning techniques include supervised, unsupervised, and reinforcement learning. Training approaches include centralized, distributed, and collaborative learning models. Each approach handles training datasets differently and influences privacy concerns (Bonawitz et al., 2019).

DOI: https://doi.org/10.52756/ijerr.2024.v39spl.015

Classification of Privacy Protection Technologies

Typical privacy protection methods include DP (Differential Privacy), HE (Homomorphic Encryption), and SMC (Secure Multiparty Computing). Depending on different levels of data privacy we have to ensure a high level of security (Zhang et al., 2020).

To sum up, it takes consistent efforts on multiple fronts—regulation, building a better model, and utilizing various PPT research—to address privacy concerns in machine learning (Cui et al., 2019).

Proposed Work

This section provides the details of the proposed work and related definitions. The proposed work incorporates the properties of the modified differential privacy technique and Gaussian distributions. It then determines the privacy of each layer in the neural network. It then uses the gradient values from stochastic gradient descent to calculate the amount of Gaussian noise, preserving sensitive data.

Corresponding Terminology

Microsoft announced differential privacy in 2006. It creates a rigorous mathematical framework for analyzing privacy. Privacy can be achieved by adding noise to the original data while maintaining its integrity.

Two remarkable things about it are that it is indifferent to any particular concept of an attacker and concerned only with data privacy. What is formally called differential privacy is (ε, δ)-differential privacy, where ε is the level of privacy guarantee while δ is the additive error. To put it in simple terms, this means that for any two training data sets, i.e., D and D', the latter having just one record at most different from the former, A produces results complying with some criterion. The formula for this is Pr[(A(D′)) = R)] ≤(e^(ε))* Pr[(A(D) = R)] + ε, where algorithm A satisfies (ε, δ), i.e., differential privacy. If ε is smaller, then it indicates better privacy protection.

How Algorithms Work

There are two main challenges to deploying the (ε, δ) DPP (Differential Privacy Preservation) technique:

1. Select where to insert the noise.
2. Effective deployment of resources

The proposed technique addresses these difficulties by incorporating different levels of privacy into neural network training.

Methodology

The proposed method effectively integrates the properties of adjusted DP (differential privacy) and Gaussian accumulations. This makes it possible to determine the explicit privacy budgets of every layer within a neural network model. It uses the gradient values from the SGD (Stochastic Gradient Descent) algorithm to check how much Gaussian noise should be added. Outcomes show that by fine-tuning the value of parameters in the modified DPM (Differential Privacy Model), our suggested model is good in terms of accuracy, efficiency, and privacy.

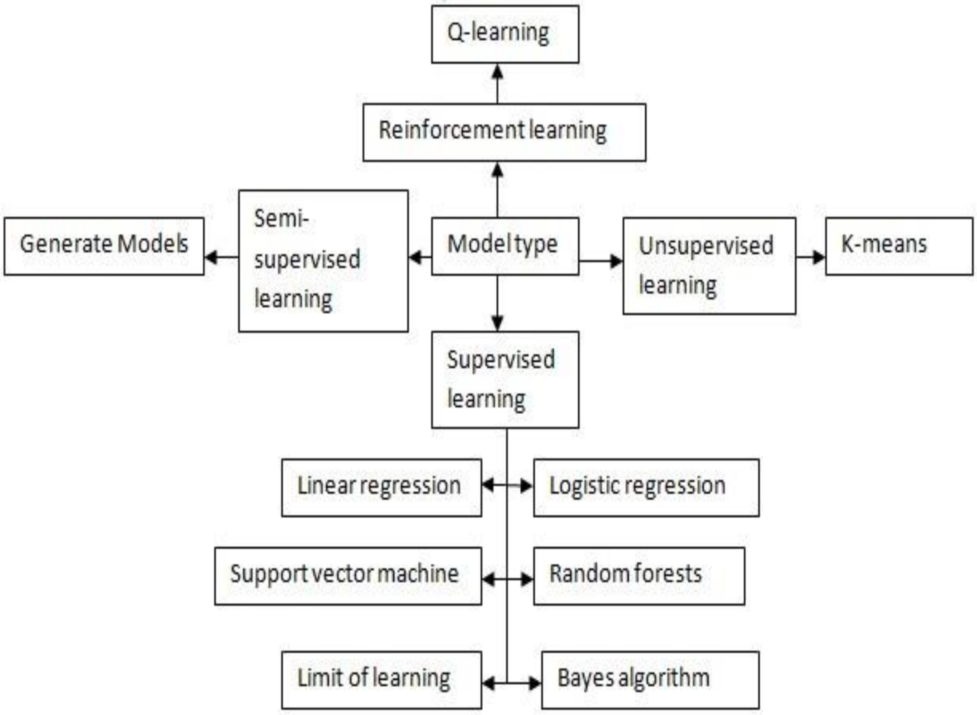

Figure 2. Model Generation Process Using Machine Learning.

The (ε, δ)-DPP (Differential Privacy Protection) technique is implemented and tested for experimental purposes. Results focus on the privacy-preserving capabilities of the algorithm while ensuring that data utility is also not compromised. The evaluation would also involve privacy preservation and model availability to ascertain how well the algorithm performed under real-world conditions. This work aims to evaluate the performance of DCGAN (Deep Convolutional Generative Adversarial Network).

To achieve these goals, the proposed algorithm generates synthetic data using DCGAN and compares it with the original dataset to check for closeness. When the similarity is above a certain predetermined threshold, we need to fine-tune the model to align perfectly with these criteria.

Through experiments, we strive to prove that our algorithm is able to ensure the privacy-utility trade-off. Finally, the performance of the algorithm is measured through the preservation of privacy and the availability of the model.

For our experiments, we used an Intel (R), Xeon (R), CPU E5-2603 V3 @ 1.60 GHz with 8 GB of memory. In addition, the system comprises two Titan X GPUs and is based on the Ubuntu 16.04. For all of our experiments, we used Python with the TensorFlow 1.0 framework, built using Bazel 0.3.1. The MNIST dataset used for the experiment contains 60,000 training and 10000 testing samples.

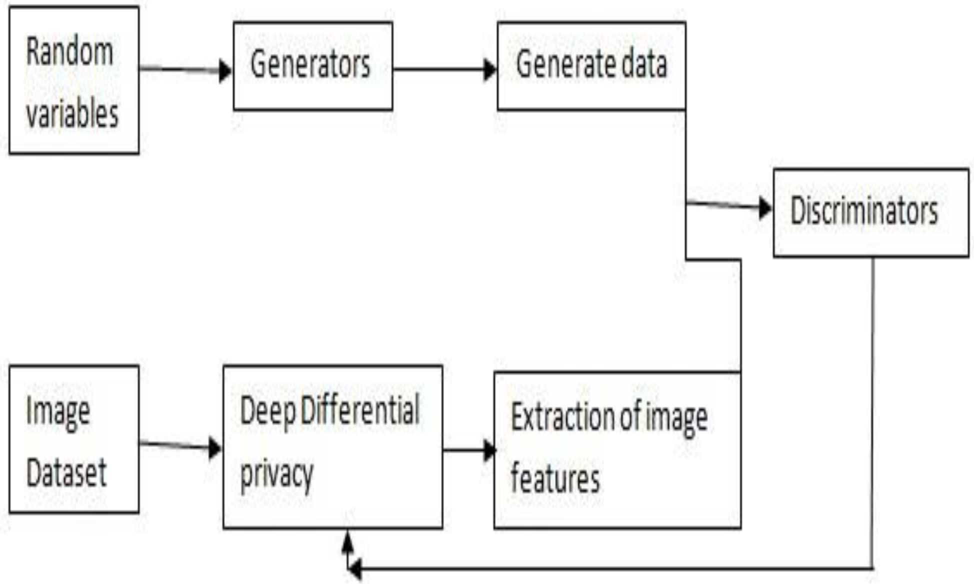

Figure 3. Methodology of the Proposed Work.

Results & Discussions

Dataset Used

For experimental purposes, we consider the MNIST dataset with C = 4(Gradient threshold) and PCA reduced to 60 dimensions. The Bork assesses to measure the effectiveness and efficiency of functions provided different privacy constraint ε along with allowable limit bias, i.e., δ, which spends much on variance scale, i.e., σ.

Experimental work

For σ = 8 (Figure 4), our algorithm performs poorly against the training set and test set, i.e., larger noise scales should undermine training quality while still maintaining the privacy of the testing dataset (Jain et al., 2023).

Table 1. Classification Accuracy and Success Rate on Different Size of Data.

Size of Data	Epoch	Accuracy %	Attack success %
10000	10	98.52	12.14
20000	10	92.34	20.74
30000	10	90.42	26.05
10000	25	85.18	33.54
20000	25	56.75	46.98
30000	25	52.25	41.25
10000	50	48.74	59.56
20000	50	22.89	79.52

For σ set to 4 (Figure 5), the algorithm's performance diminished over time, indicating improved balance.

The most consistent results were produced with σ = 2, and the model's performance was observed. We also conducted single-sample label inference attacks to assess the robustness of this kind of attack. The results indicated a significant ($p < 0.05$) negative correlation between the success rate and accuracy of the model classification. Overfitting decreased the model's ability to generalize and how well it defended against inference.

DOI: https://doi.org/10.52756/ijerr.2024.v39spl.015

As expected, increasing the number of training samples and epochs led to higher overfitting, reduced classification accuracy, and an increased inference attack success rate. However, we take 10,000 samples for model training and perform 10 epochs. The trained model gives an effective classification accuracy of 98.75% and a 13.14% inference attack success rate.

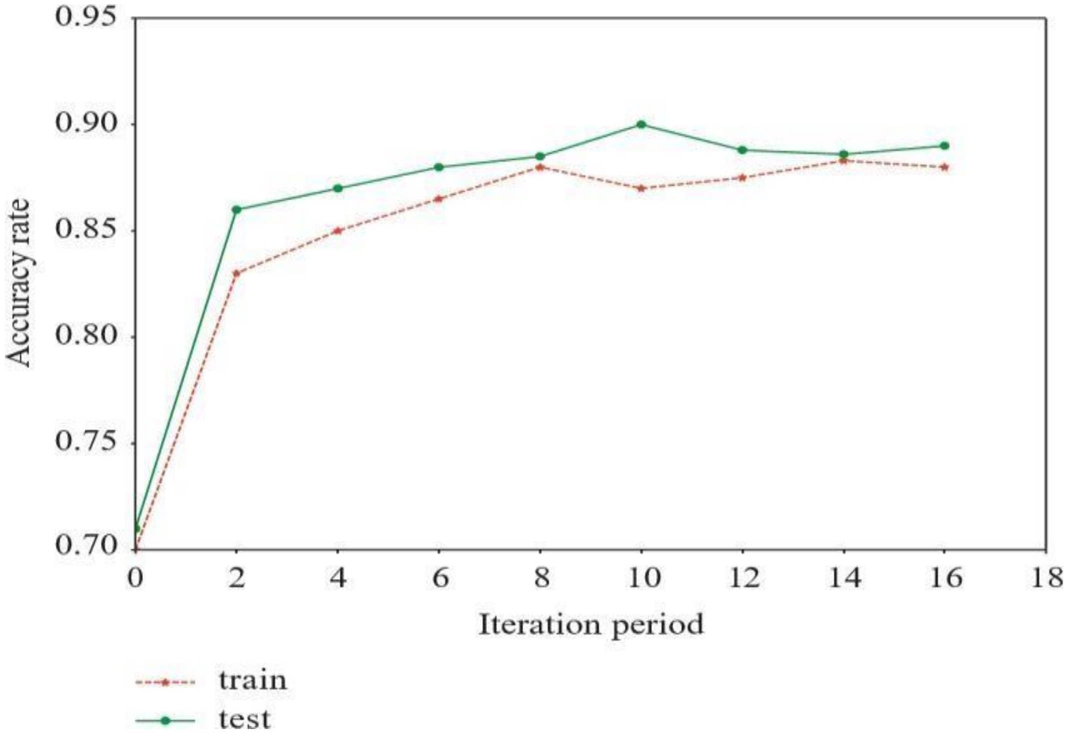

Figure 4. Outcomes at Variance σ=8 & Level of Privacy Guarantee ε=0.5.

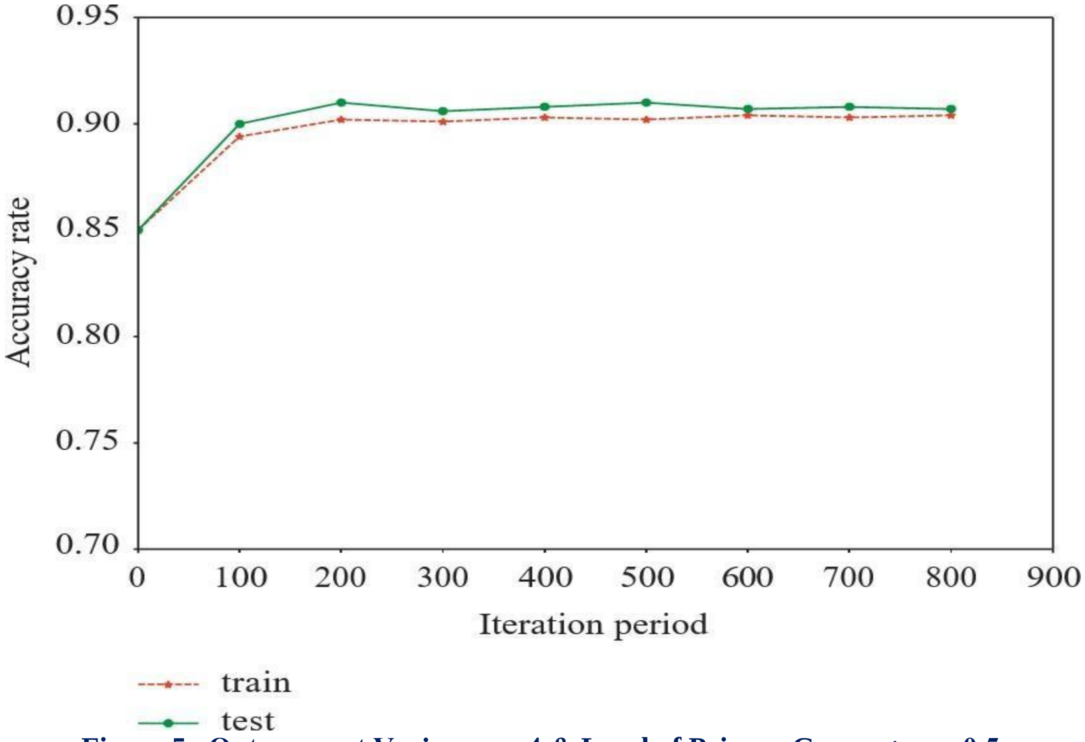

Figure 5. Outcomes at Variance σ=4 & Level of Privacy Guarantee ε=0.5.

Comparison between the Proposed and Existing Systems

The proposed technique is compared with the existing one. The difference between the proposed model and a CNN model based on classification accuracy and inference attacks is shown in Table 2.

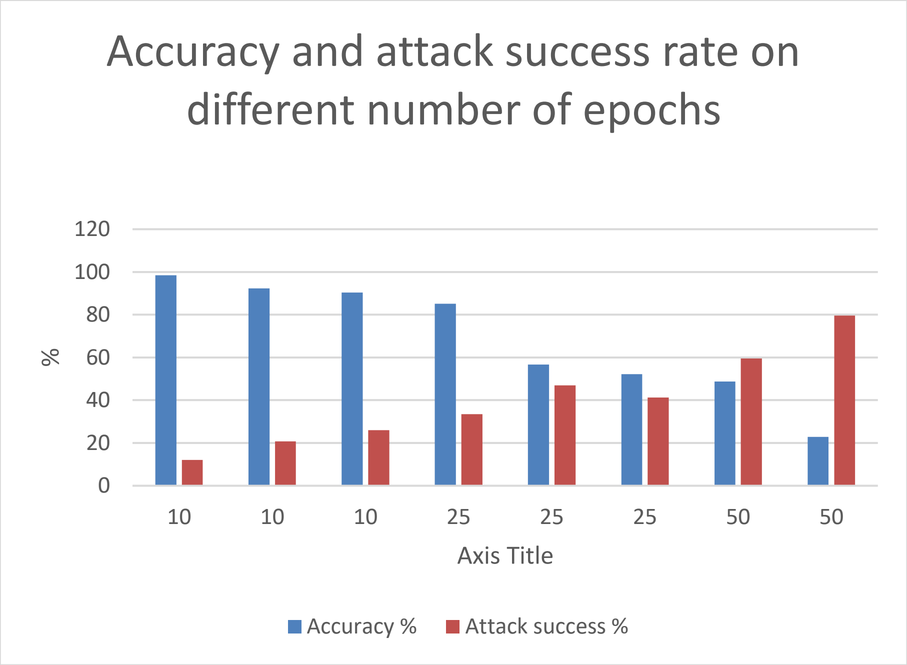

Figure 6. Accuracy And Attack Success Rate on Different Number of Epochs.

Table 2. Comparison of Classification Accuracy between Proposed and Existing Works.

Size Data	Total Epoch	Proposed Model accuracy (%)	Success Rate of Attacks (%)	Existing (CNN) (%)	Success Rate of CNN Attacks (%)
10000	10	98.97	10.75	95.38	95.25
20000	10	98.52	12.16	95.12	87.56
30000	10	97.91	12.33	93.65	66.12
10000	25	97.59	13.75	94.74	78.15
20000	25	99.02	11.94	95.78	64.22
30000	25	96.78	12.12	94.77	60.57
10000	50	97.36	12.28	94.29	65.72
20000	50	98.22	10.74	93.15	59.87
30000	50	99.02	11.72	96.46	53.85

Table 2 shows the comparison of classification accuracy and inference attacks between the proposed work and a CNN-based work (Pei et al., 2022). The proposed work outperformed CNN in terms of classification accuracy and defence against attacks. With 50 training rounds for CNN, its attack accuracy and classification accuracy decreased, indicating overfitting. A comparison between proposed and existing techniques is shown in Figure 7.

Conclusion and Future Work

This paper tries to tackle the privacy issue, i.e., is it possible to get privacy in machine learning tasks without losing classification accuracy? The proposed approach addresses this issue by blending tailored differential privacy methods with deep learning, which effectively preserves private information in the training data. During the process of parameter optimization for a network model, we inject noise data into an entirely modified DP framework. Our experimental results show that there is a trade-off between the accessibility of DNN training datasets and privacy leakage. This method guarantees high classification accuracy without revealing too much information. Such an approach can form a solid foundation for concepts of privacy regarding users and machine learning problems at scale. Collectively, they offer significantly more granular control over their own data. Going forward, we are going to focus on the efficiency and robustness of the technique.

DOI: https://doi.org/10.52756/ijerr.2024.v39spl.015

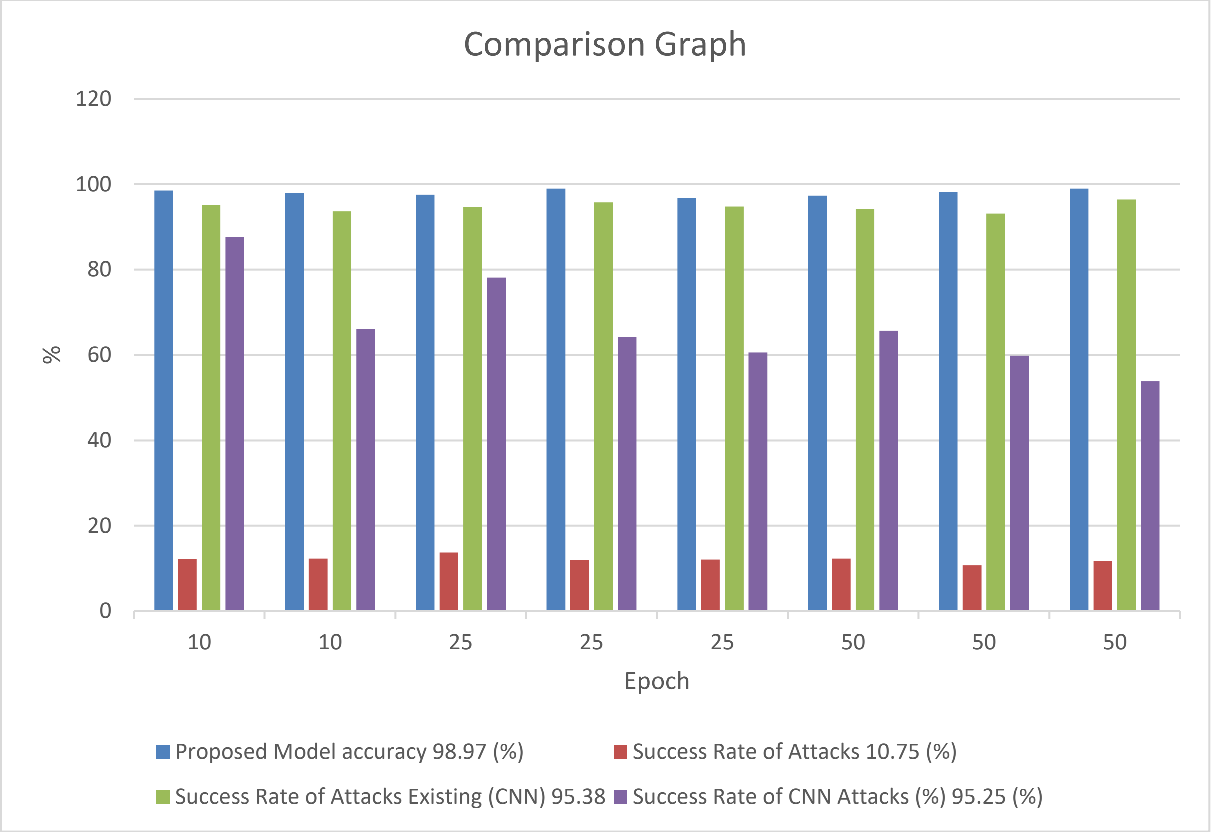

Figure 7. Comparison graph between proposed and existing works.

Acknowledgement

The authors express gratitude to their family members for their invaluable assistance, as well as to the reviewers for their feedback.

Conflict of Interest

The authors declare no conflict of interest.

References

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. ACM, *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 308-318. https://doi.org/10.1145/2976749.2978318.

Arachchige, P. C. M., Bertok, P., Khalil, I., Liu, D., Camtepe, S., & Atiquzzaman, M. (2019). Local differential privacy for deep learning. *IEEE Internet of Things Journal*, *7*(7), 5827-5842. https://doi.org/10.1109/JIOT.2019.2942801.

Bettini, C., & Riboni, D. (2015). Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing*, *17*, 159-174. https://doi.org/10.1016/j.pmcj.2014.08.004.

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., & Seth, K. (2019). Towards federated learning at scale: System design. *In Proceedings of Machine Learning and Systems (MLSys) 2020*.

Bu, Z., Wang, H., & Long, Q. (2021). On the convergence of deep learning with differential privacy. *arXiv preprint arXiv:2106.07830.*

Claerhout, B., & De Moor, G. J. E. (2005). Privacy protection for clinical and genomic data. *International Journal of Medical Informatics*, *74*(2-4), 257-265. https://doi.org/10.1016/j.ijmedinf.2004.06.010.

Cui, L., Qu, Y., Nosouhi, M.R., & Yu, S. J.W.G. (2019). Improving data utility through game theory in personalized differential privacy. *Journal of Computer Science and Technology*, *34*(2), 272-286. https://doi.org/10.1007/s11390-019-1918-1.

Feng, Q., He, D., Zeadally, S., & Khan, M.K.N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45-58. https://doi.org/10.1016/j.jnca.2018.10.020.

Gupta, R., Tanwar, S., Al-Turjman, F., & Italiya, P. A. S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *IEEE Access*, *8*, 24746-24772. https://doi.org/10.1109/ACCESS.2020.2970576.

DOI: https://doi.org/10.52756/ijerr.2024.v39spl.015

https://doi.org/10.1109/JSAC.2019.2904348.

Jain, P., & Shakya, H. K. (2023). Achieving privacy preservation in data mining using hybrid transformation and machine learning techniques. *MSEA, 71*(4), 7883.

Jain, P., Shakya, H. K., & Lala, A. (2023). Advanced privacy-preserving model for smart healthcare using deep learning. *In Proceedings of the IEEE International Conference IC3I 2023*. https://doi.org/10.1109/IC3I59117.2023.10397954.

Jain, P., Shakya, H. K., Nigam, A., Chandanan, A. K., & Murthy, C. R. (2022). Machine learning-based privacy preservation in data mining. *CIMS, 28*(12), 350-360.

Jain, P., Thada, V., & Lala, A. (2023). Design of advanced privacy-preserving model for protecting privacy within a fog computing scenario. *Proceedings of the IEEE International Conference UPCON 2023*. https://doi.org/10.1109/UPCON59197.2023.10434728.

Jain, P., & Shakya, H. K. (2022). A Review of Different Privacy Preserving Techniques in Data Mining. *Paper presented at the International Conference on Innovative Computing & Communication* (ICICC) 2022. Retrieved from SSRN: https://ssrn.com/abstract=4021149.

Jaiswal, S., & Gupta, P. (2023). GLSTM: A novel approach for prediction of real & synthetic PID diabetes data using GANs and LSTM classification model. *Int. J. Exp. Res. Rev.*, *30*, 32-45. https://doi.org/10.52756/ijerr.2023.v30.004

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Yang, H. (2019). *Advances and open problems in federated learning. arXiv preprint arXiv*, 1912.04977.

Kumar, A., Dutta, S., & Pranav, P. (2023). Supervised learning for Attack Detection in Cloud. *Int. J. Exp. Res. Rev.*, *31*(Spl Volume), 74-84. https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.008

Malin, B. A. (2004). An evaluation of the current state of genomic data privacy protection technology and a roadmap for the future. *Journal of the American Medical Informatics Association, 12*(1), 28-34. https://doi.org/10.1197/jamia.M1603.

Miller, A. R., & Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. *Management Science, 55*(7), 1077-1093. https://doi.org/10.1287/mnsc.1090.1014.

Mondal, S., Nag, A., Barman, A., & Karmakar, M. (2023). Machine Learning-based maternal health risk prediction model for IoMT framework. *Int. J. Exp. Res. Rev.*, *32*, 145-159. https://doi.org/10.52756/ijerr.2023.v32.012

Owusu, A. K., Qin, Z., Xiong, H., Liu, Y., Zhuang, T., & Qin, Z. (2021). MSDP: Multi-Scheme Privacy-Preserving Deep Learning via Differential Privacy. *Personal and Ubiquitous Computing, 26*(4), 221-233. https://doi.org/10.1007/s00779-021-01545-0.

Pal, R., Pandey, M., Pal, S., & Yadav, D. (2023). Phishing Detection: A Hybrid Model with Feature Selection and Machine Learning Techniques. *Int. J. Exp. Res. Rev.*, *36*, 99-108. https://doi.org/10.52756/ijerr.2023.v36.009

Pei, J., Zhong, K., Jan, M. A., & Li, J. (2022). Personalized federated learning framework for network traffic anomaly detection. *Computer Networks, 209*. https://doi.org/10.1016/j.comnet.2022.108906.

Samadder, M., Barman, A., & Roy, A. (2023). Examining a generic streaming architecture for smart manufacturing's Big data processing in Anomaly detection: A review and a proposal. *Int. J. Exp. Res. Rev.*, *30*, 219-227. https://doi.org/10.52756/ijerr.2023.v30.019

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, Colorado, pp. 1310–1321. https://doi.org/10.1145/2810103.2813687.

Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., & Zhou, Y. (2019). A hybrid approach to privacy-preserving federated learning. *In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, London, UK*, pp. 1–11. https://doi.org/10.48550/arXiv.1812.03224.

Wang, D., Zhao, J., & Wang, Y. (2020). A survey on privacy protection of blockchain: the technology and application. *IEEE Access, 8*, 108766–108781. https://doi.org/10.1109/ACCESS.2020.3006452.

Wang, S., Tuor, T., Salonidis, T., Leung, K. K., Makaya, C., He, T., & Chan, K. (2019). Adaptive Federated Learning in Resource Constrained Edge Computing Systems. *IEEE Journal on Selected Areas in Communications, 37*(6), 1205-1221.

Wu, H.T., & Tsai, C.W. (2018). Toward b for health-care systems: applying the bilinear pairing technology to ensure privacy. *IEEE Consumer Electronics Magazine, 7*(4), 65–71. https://doi.org/10.1109/MCE.2018.2831482.

Xu, R., Baracaldo, N., Zhou, Y., Anwar, A., & Ludwig, H. (2019). Hybrid alpha: An efficient approach for privacy-preserving federated learning. *In*

Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, London, pp. 13–23. https://doi.org/10.48550/arXiv.1912.05897.

Yadav, R., & Singh, R. (2023). Enhancing Software Maintainability Prediction Using Multiple Linear Regression and Predictor Importance. *Int. J. Exp. Res. Rev.*, *36*, 135-146. https://doi.org/10.52756/ijerr.2023.v36.013

Yin, C., Xi, J., Sun, R., & Wang, J. (2018). Location privacy protection based on differential privacy strategy for big data in industrial internet of things. *IEEE Transactions on Industrial Informatics,14*(8), 3628–3636.https://doi.org/10.1109/TII.2018.2794700

Yuan, J., & Yu, S. (2013). Privacy Preserving Back-Propagation Learning Made Practical with Cloud Computing. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 106*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-36883-7_18.

Zhang, C., Li, S., Xia, J., Wang, W., Yan, F., & Liu, Y. Batchcrypt (2020). Efficient homomorphic encryption for cross-silo federated learning. *In Proceedings of the USENIX Annual Technical Conference (USENIX ATC 20)*, pp. 493–506. https://doi.org 10.5555/3485970.3486018.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE, In 2017 IEEE International Congress on Big Data* (BigData Congress), pp. 557-564. https://doi.org/10.1109/BigDataCongress.2017.85

Zhu, T., Ye, D., Wang, W., Zhou, W., & Yu, P.S. (2020). More than privacy: applying differential privacy in key areas of artificial intelligence. https://arxiv.org/abs/2008.01916.

How to cite this Article:

Pinkal Jain, Vikas Thada and Deepak Motwani (2024). Providing Highest Privacy Preservation Scenario for Achieving Privacy in Confidential Data. *International Journal of Experimental Research and Review*, *39*(spl.) 190-199.

DOI : https://doi.org/10.52756/ijerr.2024.v39spl.015