iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49632

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

Differential Privacy Preserving Using TensorFlow DP-SGD and 2D-CNN for Large-Scale Image Data

Amit Rajput[1], Suraksha Tiwari[2]
Shriram College of Engineering & Management, Banmore, Dist. Morena, Pin-476444, India

Abstract: ***Although smart wearables have many potential advantages, their widespread and ongoing use raises a number of privacy issues and difficult information security challenges. This article, present a thorough analysis of current wearable sensor-based big data analytics applications that protect user privacy. We draw attention to the fundamental aspects of privacy and security for applications on wearable technology. Then, we look at how deep learning techniques like 2D CNN are used for better evaluation and privacy preservation as well as for differential privacy of Tensor flow. DP-SGD (Differentially private stochastic gradient descent)The metrics are epsilon as well as accuracy, with 0.56 epsilon and 85.17% accuracy for three epochs and 100.09 epsilon and 95.28 accuracies for twenty epochs, respectively. Model training Accuracy is 94.71%. Also, present a case study on privacy-preserving machine learning techniques. Herein, we theoretically and empirically evaluate the privacy-preserving deep learning framework's performance. We explain the implementation details of a case study of a secure prediction service using the 2D convolutional neural network (2D CNN) model.***

Keywords: Privacy Preserving, Differential Privacy, Deep Learning, Convolutional Neural Network.

I. INTRODUCTION

Massive data collection is an essential component of Artificial Intelligence (AI) methods, and Machine Learning (ML), the core component of Deep Learning, uses this data to build predictive models. However, gathering data and using it to look for patterns in data behavior are two distinct processes. Additionally, it comes with a number of challenges that must be overcome by an individual or entity, including privacy issues like data breaches, monetary loss, and reputational damage[1]. Machine learning is largely responsible for most private information data analysis, which primarily consists of search algorithms, algorithms, & ad tech networks. To bridge the gap between privacy and reaping the rewards of machine learning, privacy-preserving machine learning was created[2]. It is an essential tool for adhering to data confidentiality laws and privatizing acquired data. In this article, the fundamental concepts of privacy-preserving computer vision are presented. This article demonstrates how to solve issues by combining machine learning & privacy techniques. Check out a few of the available tools. The goal of this article is to fully explain privacy-preserving machine knowledge for a variety of applications[3][4]. A methodical approach to preventing privacy risks in machine learning algorithms is privacy-preserving machine learning. As shown in the following Figure, PPML enables a variety of privacy-enhancing techniques to enable various input sources to prepare ML models collaboratively without disclosing their secret data in their original form[5].

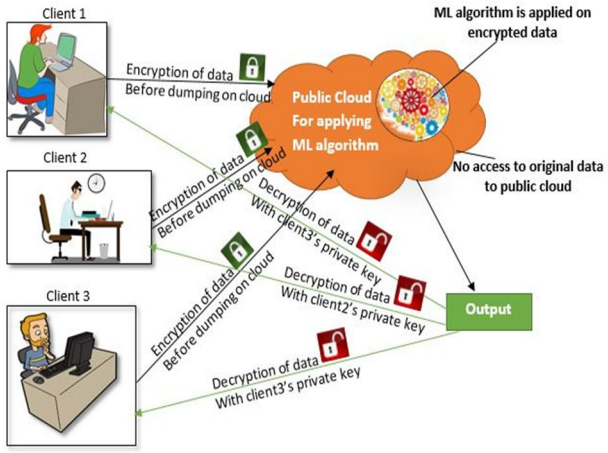


Fig. 1 The concept of PPML

Two main models of PPTs (Privacy preserving technologies) are:

A. *Soft Privacy Technologies*

This model is built on the pillars of compliance, consent, control, & audit, and it employs reputable third-party partners for the processing of data. Differential privacy (DP) and tunnel encryption are two such examples [6].

B. *Hard Privacy Technologies*

With this model in place, no third party can ever compromise users' personal information, making it an ideal choice for situations in which users' data is at risk of being misused. Voting via a virtual private network is one such instance. The Netflix recommender system and the Google search engine are two examples of companies whose business models have been based on machine learning. Other businesses have a sizable investment in machine learning models like 2D CNN, despite this not being their main line of business. Business leaders must be aware of a few things involving machine learning and its limitations even though it is an allowing technology that can help employees or open up opportunities for businesses[7]. Machine learning models occasionally cause or aggravate social issues. When people are exposed to incendiary, partisan, or imprecise content, it can polarise society and fuel the dispersion of conspiracy theories. For instance, Facebook uses machine learning to show users ads & content that would interest but also engage them[8][9].

II. LITERATURE REVIEW

Tao 2022 et. al [10] has attracted a lot of interest in the academic and professional worlds. This article suggests a brand-new, effective, and privacy-preserving mathematical accumulation system (EPPSA) for WSNs, which enables the calculation of statistical data without disclosing to the control centre the exact number of sensor devices. A number of statistical aggregation functions, such as geometric average, algebraic mean, weighted mean, and variance, are supported by the EPPSA scheme. Additionally, the EPPSA scheme uses customised Clayton exponentiation algorithms to boost edge aggregator aggregation efficiency. The performance assessment demonstrates that the EPPSA scheme outperforms the current statistical aggregation schemes in terms of aggregation efficiency and communication load.

Aljably 2020 et. al [11] have various security measures to protect user data, taking additional information into account. In order to preserve privacy more clearly, physical access models could be used in conjunction with machine learning algorithms. To identify unusual users, the models could make use of additional data derived first from user profiles. In this study, we introduce a data hiding algorithm that combines access control models with unsupervised and supervised learning anomaly detection methods. Our control strategy contain the information the list of variables used to categorise users as a result of both the rich and quite well policies. With over 95% correctness using Bayesian classifiers and 95.53% on the receiver characteristic curve when using deep learning models and long short attention span recurrent neural network classifiers, it has been recently demonstrated on real datasets. According to experimental findings, this method outperforms other detection methods like the Kolmogorov-Smirnov test, principal component analysis, isolation forest, support vector machines, and principal forestry.

Zou 2020 et. al [12]. are open to listening in when uploading personal information and re-encryption keys. In addition, the management of multiple users' keys adds to the workload. Additionally, users with ulterior motives cannot be effectively filtered out by profile matching using the inner product between vectors. We first enhance an elgamal s actually structure (HRES) to enable a single elgamal multiplication and an infinite number of homomorphic additions in order to address the aforementioned difficulties. Users' data is encrypted using the public key that the clouds have agreed upon, which avoids key management and key leakage problems while also protecting user privacy. Furthermore, our method computes the approximation result between the normalised vectors as the benchmark for gauging the proximity of users using the elgamal polynomials land of the enhance HRES algorithm. As a result, we can successfully enhance users' social interactions. Chen 2018 et. al [13] Recently, [3] has gotten more attention. The V2I information sharing scenario is still undecided as to how to securely and effectively accumulation the sensory data from vehicles. This paper proposes a lightweight & unverified aggregation protocol for the V2I communication scenario based on fog computing. The proposed protocol enables the RSU to efficiently and privately gather the information collected by the vehicles. In particular, we first propose and demonstrate the security of the signature scheme cumulative signcryption (CL-A-SC) scheme in the random oracle model. The proposed CL-A-SC strategy, which is of impartial interest, can simultaneously achieve certificateless cryptography's benefits and signcryption's. Then, as an addition to the suggested CL-A-SC scheme, we present the unidentified accumulation proper procedure for V2I communication scenarios. The inclusion complexes protocol achieves the desired security properties, according to security analysis. The performance comparison demonstrates that, when compared to the most recent protocols in this area, the suggested technique significantly lowers the communication and computation overhead.

Kang 2017 et.al [14] was suggested. The integrity of the data that is stored is crucial in cloud-assisted medical systems. He et al. previously suggested a cryptographic public internal audit scheme for platform WBANs based on cryptographic public key cryptography. However, the plan put forth by He et al. does not protect privacy. The actuary can elicit these data blocks after performing numerous checks on a specific set of data blocks.

In this manuscript, we propose a privacy-preserving attribute - based encryption public auditing scheme for cloud-assisted WBANs. The proof data is shielded from the auditor during the proof stage of the proposed scheme. Thus, the inquisitive auditor was unable to determine the data blocks. We also demonstrate the proposed scheme's security in the random oracle, assuming that the Attribute based problem is difficult, and we compare it to He et alproposed .'s system in terms of reliability and computational expense.

III. PROPOSED METHODOLOGY

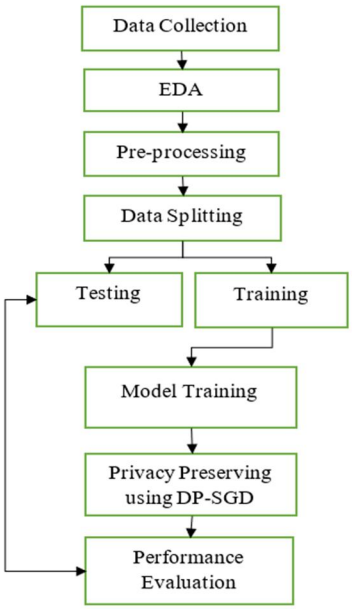


Fig. 2 Proposed Model

How to preserve privacy is covered in this section. The process starts with gathering the data, after which EDA is used to visualise the data. It also involves data preparation, which includes data cleaning as well as removal from the data. Data splitting communities the data into sections for testing and training, then chooses the models for a better evaluation.

A. Data collection

The information from MNIST Fashion has been compiled in this section. https://www.kaggle.com/datasets/zalando-research/fashionmnist [15] Fashion-MNIST is just a set of data of Zalando article images, with 60,000 examples in the training set and 10,000 examples in the test set. A label from one of ten classes is linked to a 28x28 grayscale in each example. For the purposes of comparing machine learning algorithms, Zalando wants Fashion-MNIST to stand for the initial MNIST dataset. The size of the images and the splits' structures are the same for training and testing.

B. Exploratory Data Analysis (EDA)

The process of investigating a set of data as well as summarising its key features is known in data analytics as exploratory data analysis. It's an instance of descriptive analytics. The purpose of EDA is to spot trends and patterns, spot anomalies, and test preliminary hypotheses. And even though exploratory data analysis is possible at different stages of a data analytics process, it is typically done before a firm hypothesis as well as end goal is defined. Typically, before deciding what to do with a dataset, EDA [16] concentrates on understanding its characteristics. Exploratory data analytics frequently makes use of visual tools like graphs, plots, as well as other visualisations. This is because trends and anomalies are much easier to spot when they are represented visually thanks to our natural pattern-detecting abilities.

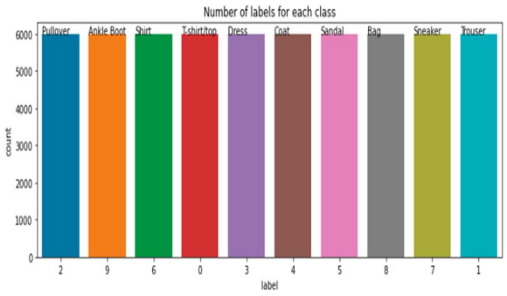


Fig. 3 Number of labels each class for training

The quantity of labels assigned to each class in the training data is shown in Fig. 3. Each class has 6000 image datasets for training, resulting in 10 classes altogether.

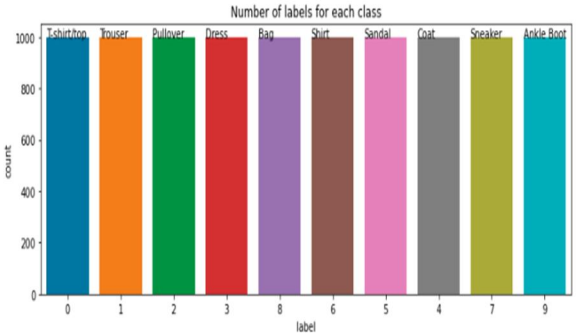


Fig. 4 Number of labels each class for training

Fig. 4 displays the number of labels allotted per each class inside the testing data. There are 10 classes total, with 1000 images in each class's testing dataset.

C. Pre-processing

Perform image conversion into a numpy array during preprocessing. We need to be able to load as well as manipulate images in order to improve the predictive model's performance. One task can be carried out in various ways in Python. After that, normalise 255 and reshape this same information (28, 28, 1) Basically, reshaping means altering the shape of such an array. Additionally, the quantity of elements for each dimension affects the shape of such an array. then start decoding the categorical features to 10 classes into 0s and 1s, which a computer can only understand indirectly. These numbers are interpreted by the device as commands for displaying information, sound, images, and other forms of media that have meaning for people. Similar to this, since algorithms just understand numbers, we must send data to machine learning (ML) models in the correct format. Additional important details about the data are contained in these categorical variables[17].

D. Data Splitting

The data will be split into 60,000 and 10,000 for training and testing even before a classification model is created. 10,000 for testing and 60,000 for training. The data that a machine learning tool uses for training is used to teach the tool how to recognise patterns or carry out tasks in accordance to predefined criteria[18]. The model's accuracy is instead evaluated using testing data and validation data.

E. Model Selection

The term "prediction problem" refers to the process of selecting a framework from a large pool of potential models. In relation to model performance, other factors such as difficulty, maintainability, and resource availability may also be taken into account when choosing a model[19]. The application of a 2D CNN architecture has indeed been done for evaluation and prediction.

C. 2D Convolutional Neural Network

Convolution is an operation that transforms one function into another through the orderly intertwining of two sources of information. Traditionally, convolutions are employed in image analysis to blur as well as sharpen pictures, but they can also be used for other tasks. CNNs impose a connection oriented pattern among neurons of adjacent layers (for instance, by embossing and enhancing edges)[20].The 2D convolution layer, which is frequently referred to by the acronym conv2D, is the most widely used type of convolution. In a conv2D layer, an elementwise multiplication is carried out by a filter or kernel as it "slides" over the 2D input data. Therefore, it will combine the outcomes into such an output data pixel. A same operation, which converts each 2D feature matrix into some other 2D feature matrix, will happen at every location this same kernel crosses. FIG. 4 depicts the 2D CNN[21].

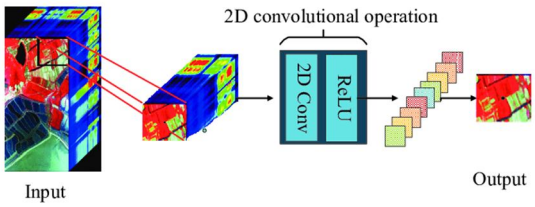


Fig. 5 Architecture of 2D CNN[22]

Table 1 Hyperparameter Used

Model	2D CNN
Neurons	16,32,32,10
Activation	Relu
Padding	Valid
Straid	2
Final Output layer	10 Neurons
Epochs	20

F. Differential Privacy

Differential Privacy is just a framework for evaluating the privacy protections an algorithm offers[23]. Designing algorithms for machine learning that responsibly train designs on private data is possible using the perspective of differential privacy. Machine learning risks of exposing sensitive data for training are reduced by learning with differential privacy, which offers verifiable privacy guarantees[24]. Any single training example or small group of training examples in a model's data set shouldn't have any impact on the model's performance that was trained with differential privacy. Information contained in a training step cannot be memorised if it has no effect on the learning process, and the privacy of the person who provided this piece of data to our set of data is respected[25].

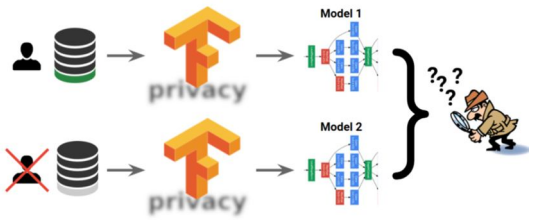


Fig. 6 Differential Privacy Architecture

D. Tensor Flow Privacy

Illustrating our demonstration of DP-SGD and giving a practical tutorial by using TensorFlow Privacy library, that also offers an implementation of DP-SGD. The only requirement for completing this tutorial is the ability to use TensorFlow to train a basic neural network. We advise reading the above tutorial first to get started to TensorFlow and machine learning if you are unfamiliar to convolutional neural networks or with how to train them[26].

IV. RESULT & DISCUSSION

DP-SGD Optimizer must be used with hyperparameters like Accuracy and loss are the metrics, and 20 epochs were used for the assessment. The Noise Multiplier is 1.3, the Norm clip appears to be 1.5, the Micro batches are 250, the Learning Rate is 0.25%, as well as Loss categorical cross Entropy has been employed. The greatest Euclidean (L2) norm of the each gradient that is used to keep updating model parameters. the quantity of noise that is sampled & added to gradients throughout training. Each data batch is divided into smaller groups called micro batches. Each microbatch should by default include just one training example. This enables us all to clip gradients per example basis as opposed to after they have been averaged from across minibatch. This hyperparameter is already present in standard SGD. Each update matters more as learning rate increases.

Table 2 Performance Evaluation of Model Training

Model	Training Accuracy	Training Loss	Validation Accuracy	Validation loss
CNN	94.71 %	36.17%	95.29%	27.87%

The terms "training accuracy," "training loss," "validation accuracy," and "validation loss" are defined in Table 2. The validation accuracy was 95.29%, the validation loss was 27.87%, and the training accuracy was 94.71%.

A. Comparatively Evaluate the Privacy Guarantees

To evaluate the DP guarantee a training algorithm achieves, perform a privacy analysis. The ability to compare two training runs side-by-side objectively to see which is more privacy-preserving depends on knowing the amount of DP attained. On a broad scale, the privacy analysis assesses the extent to which a possible adversary might enhance their prediction about the characteristics of any given training point by looking at the results of the training process. The DP guarantees of such an ML algorithm is expressed using one metric.

Epsilon (∈) - The privacy budget is as follows. The extent to which the likelihood of a specific model output may vary by including (or removing) any single training point serves as a measure of the privacy guarantee's robustness. More privacy protection is implied by a lower value for. The value is merely an upper bound, therefore a high value can really indicate strong privacy in practise.

Table 3 Evaluation of DP guarantee

Epochs	Epsilon	Accuracy
3	0.56	85.17%
20	100.09	95.28%

The assessment of DP guarantee is presented in Table 3. Epochs, Epsilon, and Accuracy are the parameters; for 3 epochs, the Epsilon value was 0.56 and the accuracy was 85.17%. After 20 epochs, the epsilon value is 100.09, and the accuracy is 95.28 percent.

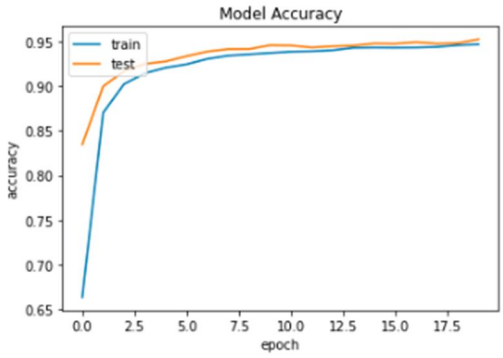


Fig. 7 Displays the model's accuracy during training and testing.

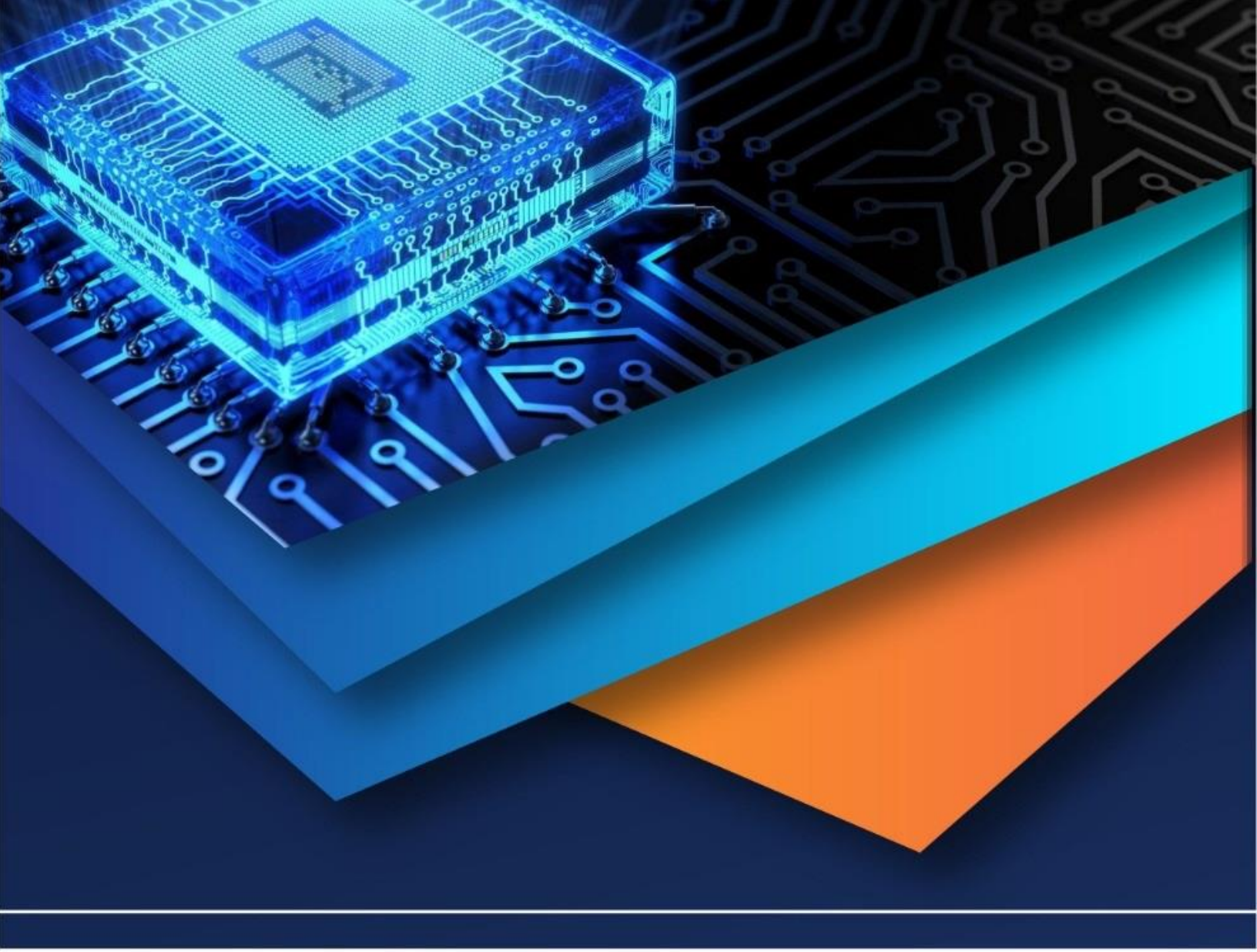
According to a prior study, the neutrally interesting CL-A-SC technique can simultaneously achieve the advantages of certificateless cryptography and signcryption. Accuracy and loss were measured using 20 epochs in our research, which was based on the DP-SGD Optimizer. The Loss categorical cross Entropy has been used, and the Noise Multiplier is 1.3, the Norm clip looks to just be 1.5, the Micro batches are 250, the Learning Rate is 0.25%.

V. CONCLUSION

Smart wearables have a lot of potential benefits, but their widespread as well as ongoing use also poses serious privacy concerns and information security difficulties. Present a thorough analysis of current wearable sensor-based big data analytics apps that safeguard user privacy in this article. We call attention to the essential components of security and privacy for wearable technology applications. Then, we examine how deep learning methods, such as 2D CNN, are used for differential privacy of Tensor flow as well as for better evaluation & privacy preservation. DP-SGD Epsilon and accuracy are the metrics, with epsilon of 0.56 and accuracy of 85.17% for three epochs and epsilon of 100.09 and accuracy of 95.28 for twenty epochs, respectively.

REFERENCES

[1] M. Abdel-Basset, H. Hawash, N. Moustafa, I. Razzak, and M. Abd Elfattah, “Privacy-preserved learning from non-iid data in fog-assisted IoT: A federated learning approach,” Digit. Commun. Networks, 2022, doi: 10.1016/j.dcan.2022.12.013.
[2] V. Terziyan, D. Malyk, M. Golovianko, and V. Branytskyi, “Encryption and Generation of Images for Privacy-Preserving Machine Learning in Smart Manufacturing,” Procedia Comput. Sci., vol. 217, no. 2022, pp. 91–101, 2023, doi: 10.1016/j.procs.2022.12.205.
[3] M. Khan, F. G. Glavin, and M. Nickles, “Federated Learning as a Privacy Solution - An Overview,” Procedia Comput. Sci., vol. 217, pp. 316–325, 2023, doi: 10.1016/j.procs.2022.12.227.
[4] M. Field et al., “Infrastructure platform for privacy-preserving distributed machine learning development of computer-assisted theragnostics in cancer,” J. Biomed. Inform., vol. 134, no. April, p. 104181, 2022, doi: 10.1016/j.jbi.2022.104181.
[5] S. Zapechnikov, “Contemporary trends in privacy-preserving data pattern recognition,” Procedia Comput. Sci., vol. 190, no. 2019, pp. 838–844, 2021, doi: 10.1016/j.procs.2021.06.098.
[6] Y. Sun, Q. Wen, Y. Zhang, and W. Li, “Privacy-preserving self-helped medical diagnosis scheme based on secure Two-party computation in wireless sensor networks,” Comput. Math. Methods Med., vol. 2014, 2014, doi: 10.1155/2014/214841.
[7] N. Wang et al., “A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles,” Digit. Commun. Networks, 2022, doi: 10.1016/j.dcan.2022.05.020.
[8] S. Sav, J. P. Bossuat, J. R. Troncoso-Pastoriza, M. Claassen, and J. P. Hubaux, “Privacy-preserving federated neural network learning for disease-associated cell classification,” Patterns, vol. 3, no. 5, p. 100487, 2022, doi: 10.1016/j.patter.2022.100487.
[9] T. Veeramakali, A. Shobanadevi, N. R. Nayak, S. Kumar, S. Singhal, and M. Subramanian, “Preserving the Privacy of Healthcare Data over Social Networks Using Machine Learning,” Comput. Intell. Neurosci., vol. 2022, no. June 2012, 2022, doi: 10.1155/2022/4690936.
[10] Y. Tao, F. Kong, J. Yu, and Q. Xu, “EPPSA: Efficient Privacy-Preserving Statistical Aggregation Scheme for Edge Computing-Enhanced Wireless Sensor Networks,” Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/7359134.
[11] R. Aljably, Y. Tian, and M. Al-Rodhaan, “Preserving Privacy in Multimedia Social Networks Using Machine Learning Anomaly Detection,” Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/5874935.
[12] Y. Zou et al., “Improved Cloud-Assisted Privacy-Preserving Profile-Matching Scheme in Mobile Social Networks,” Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/4938736.
[13] Y. Chen, Z. Lu, H. Xiong, and W. Xu, “Privacy-Preserving Data Aggregation Protocol for Fog Computing-Assisted Vehicle-to-Infrastructure Scenario,” Secur. Commun. Networks, vol. 2018, 2018, doi: 10.1155/2018/1378583.
[14] B. Kang, J. Wang, and D. Shao, “Certificateless Public Auditing with Privacy Preserving for Cloud-Assisted Wireless Body Area Networks,” Mob. Inf. Syst., vol. 2017, 2017, doi: 10.1155/2017/2925465.
[15] “No Title”, [Online]. Available: https://www.kaggle.com/datasets/zalando-research/fashionmnist
[16] “What is Exploratory Data Analysis | Tutorial by Chartio.”
[17] X. Ma, Y. Zhou, L. Wang, and M. Miao, “Privacy-preserving Byzantine-robust federated learning,” Comput. Stand. Interfaces, vol. 80, 2022, doi: 10.1016/j.csi.2021.103561.
[18] K. Lakshmanna, R. Kavitha, B. T. Geetha, A. K. Nanda, A. Radhakrishnan, and R. Kohar, “Deep Learning-Based Privacy-Preserving Data Transmission Scheme for Clustered IIoT Environment,” Comput. Intell. Neurosci., vol. 2022, 2022, doi: 10.1155/2022/8927830.
[19] F. Yu, Z. Xu, Z. Qin, and X. Chen, “Privacy-preserving federated learning for transportation mode prediction based on personal mobility data,” High-Confidence Comput., vol. 2, no. 4, p. 100082, 2022, doi: 10.1016/j.hcc.2022.100082.
[20] Q. Liu, “Privacy Protection Technology Based on Machine Learning and Intelligent Data Recognition,” Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/1598826.
[21] R. Venugopal, N. Shafqat, I. Venugopal, B. M. J. Tillbury, H. D. Stafford, and A. Bourazeri, “Privacy preserving Generative Adversarial Networks to model Electronic Health Records,” Neural Networks, vol. 153, pp. 339–348, 2022, doi: 10.1016/j.neunet.2022.06.022.
[22] “The 2D-CNN model consisting 2D convolutional operation with kernel size... | Download Scientific Diagram.”
[23] K. Mivule, C. Turner, and S. Y. Ji, “Towards a differential privacy and utility preserving machine learning classifier,” Procedia Comput. Sci., vol. 12, pp. 176–181, 2012, doi: 10.1016/j.procs.2012.09.050.
[24] C. Wang, X. Wu, G. Liu, T. Deng, K. Peng, and S. Wan, “Safeguarding cross-silo federated learning with local differential privacy,” Digit. Commun. Networks, vol. 8, no. 4, pp. 446–454, 2022, doi: 10.1016/j.dcan.2021.11.006.
[25] “Differential Privacy Series Part 1 | DP-SGD Algorithm Explained | by PyTorch | PyTorch | Medium.”
[26] “Machine Learning with Differential Privacy in TensorFlow | cleverhans-blog.”



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY