International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Privacy Preservation using Deep Learning Methods

Amreen Ayisha M[1], Ankit Kumar[2], Gasti Harshini[3], Keerthana S[4],Mrs. Samatha R Swamy[5]

[12345] ayishaamreen78@gmail.com, ankit.astaim@gmail.com, harshinisweety61@gmail.com, twinklekee026@gmail.com, samatha-ise@dsatm.edu.in

[1234]Student, Department of Information Science and Engineering, DSATM, Bangalore-88, Karnataka

[5]Faculty, Department of Information Science and Engineering, DSATM, Bangalore-88, Karnataka

Abstract- Significant technologicaladvancements have occurred over the past 10years, which have the ability to make daily living routines more convenient on both a corporate and personal level. The sharing ofdata with other global web applications thatkeep tabs on your daily actions, however, is the next real-life problem. Building a collaborative platform and maintaining individual privacy are the main concerns for training a global Deep Learning (DL) model.Deep learning is a subset of machine learning that makes use of multiple-layered neuralnetworks to extract patterns from data. Thistechnology has been used to develop several privacy-preserving techniques, including data anonymization, differential privacy, and homomorphic encryption. Deep Neural Network (DNN) has been appearing incredible potential in sorts of real-world applications such as extortion discovery and trouble expectation. In the meantime,information separation has gotten to be a genuine issue right now, i.e., diverse parties cannot share information with each other. To unravel this issue, most investigate leverages cryptographic strategies to prepare secure DNN models for multi-parties without compromising their private information. In spite of the fact that such strategies havesolid security ensure, they are troublesome to scale to profound systems and expansive datasets due to its tall communication and computation complexities.

Keywords- Differential Privacy, Adversarial Learning, Secret Sharing, Encrypted Deep Learning, Security, Federated Learning.

I. INTRODUCTION:

The extraction of hidden patterns, which businesses can utilize to base business choices on the outputs produced by these algorithms, isa crucial function of machine learning (ML) and deep learning (DL) algorithms. All of the domains employ ML/DL algorithms. The ML/DL algorithms were trained using data that was stored in a central location. Security issues,single points of failure, increased latency, and other difficulties could be caused by centralizing data storage [11]. To solve the drawbacks of centralized storage for machine learnings, the concept of distributed learning was brought into the IoT context [14]. The training data is stored in several locations and sent to the ML/DL algorithms during distributed learning [20]. With distributed ML, the trainingtime for ML/DL algorithms was greatly decreased. Using the use of federated learning (FL), a development of distributed ML, ML/DLalgorithms can be trained on data that is available on a variety of platforms [2].

FL is a method of deep learning that requires training a centralized model cooperatively across numerous client's data, as a result itencourages the protection of client privacy while developing trained models that make use

of the data of all involved customers. FL does not entirely protect against malicious attacks, inference attacks in particular are a major concern. However, we examine and thendemonstrate how the theoretical privacy may be accomplished in the federated situation by usingthe differential privacy method at the specific level in order to promote trust [3],[15]. Nowadays one of the most applicable issues for machine learning has been the privacy preserving issue. The best method for privacy preserving machine learning (PPML) to assure robust security in the sense of cryptography and fulfil communication succinctness is FHE. FHEencryption method allows ciphertext to be processed by any deep arithmetic or Boolean circuit without having access to the original data[4].

II. OVERVIEW OF PRIVACYPRESERVATION

Privacy preservation refers to the protection of sensitive information from unauthorized access,use, disclosure, or modification. In recent years,privacy has become a growing concern as largeamounts of personal data are being collected and analyzed for various purposes. Privacy preservation techniques aim to balance the needfor data analysis with the need to protect individual privacy.

There are different types of privacy preservation methods, they are Differential Privacy, Homomorphic encryption, multi-party communication, Federated learning, Ensemble privacy preserving techniques.

A type of encryption called homomorphic encryption enables calculations to be made on ciphertext without exposing the plaintext. Inother words, it makes it possible to execute calculations on encrypted data, which is advantageous in situations when data privacy iscrucial.

A type of encryption called functional encryption enables access control to be appliedto encrypted data. It provides fine grained access control by encrypting data with a specific function or attribute [12].

Both techniques have important applications inareas such as cloud computing, data privacy and secure computation.

Without the need to first decode the data, Fully Homomorphic Encryption enables arbitrary calculations to be done on encrypted data. FHE is viewed as an extension of PHE, where computations on encrypted data can be performed for any operation. Advantage of homomorphic encryption is it prevents the dataleakage or breaches by storing the sensitive dataand processing the data in a secured and private manner [4].

III. CHALLENGES OF PRIVACY PRESERVATION:

The several challenges associated with preserving privacy are:

A. Data Protection:

One of the privacy preserving using deep learning is ensuring that sensitive data is protected. When deep learning models are trained on sensitive data, there is a risk that thedata could be compromised if the model ishacked [9],[14],[22],[34].

B. Anonymization:

Anonymization is a key technique used to preserve privacy, but it can be challenging to implement effectively. Anonymization involves removing personal identifying information from data, but it can be difficult to ensure that data remains anonymous without sacrificing itsutility for training deep learning models [12],[13].

C. Adversarial attacks:

Deep learning models are susceptible to adversarial assaults, in which a perpetrator changes inputs knowingly in an effort to deceive the model. These attacks have the potential to violate the privacy of people whosedata were used to train the model or to extract sensitive information from it [11],[20].

D. Data poisoning:

Data poisoning is the deliberate addition of false or harmful information to a dataset with the goal of compromising information or the privacy of persons whose information was utilized to train the model [11].

E. Transparency:

It can be difficult to read deep learning models, which makes it difficult to understand how they process data and how they could harm privacy. To make sure that deep learning models are not jeopardizing privacy, transparency is essential [10],[15],[18].

F. Security:

Security is a significant challenge in privacy preservation because sensitive information that is being protected must be safeguarded from unauthorized access, modification, or disclosure. Privacy preservation techniques such as data anonymization, differential privacy, and homomorphic encryption all rely on robust security mechanisms to ensure that sensitive information is protected while still allowing for effective data analysis [18].

Overall, preserving privacy requires careful attention to design and implementation of models, as well as ongoing monitoring and adaptation to address new threats and vulnerabilities.

IV. SECURITY ISSUES ON PRIVACY PRESERVATION:

Privacy preservation is an essential aspect of modern-day digital communication, as it ensures that individuals' personal information remains protected and secure from unauthorized access. However, despite advancements in technology, there are still security issues related to privacy preservation that need to be addressed.

A. Data breaches:

One of the biggest security issues related to privacy preservation is data breaches. When organizations collect and store personal information, there is always a risk of the data being hacked or stolen by cybercriminals. These breaches can lead to identity theft, financial loss, and other security issues [11],[13],[15],[18],[39].

B. Lack of encryption:

Encryption is a critical tool for privacy preservation. It secures data by encoding it in a format that only authorized users can interpret. However, if data is not encrypted or if weak encryption is used, it can be easily hacked or intercepted [11],[19],[28].

C. Inadequate access controls:

Access controls are critical in ensuring that only authorized personnel can access sensitive data. However, if these controls are not adequately implemented or managed, it can lead to security breaches and data leaks [11],[13],[23].

D. User error:

Another security issue related to privacy preservation is user error. This can occur when individuals fail to properly secure their devices, use weak passwords, or fall prey to phishing scams. It is essential to educate users on best practices for privacy preservation to minimize the risk of user error [14],[17].

E. Lack of transparency:

Lack of transparency in data collection and usage can also be a security issue related to privacy preservation. Users may be less inclined to trust companies and run the danger of their data being exploited if they are unaware of how their personal information is gathered and handled [14],[16],[19].

V. COUNTERMEASURES TO SECURITY IN PRIVACY PRESERVATION:

Strong security measures must be implemented in order to safeguard personal data and ensure privacy preservation. This requires a combination of encryption, access controls, user

education, and transparency to minimize therisk of security breaches and data leaks. Few ofthe methods are:

A. Convolutional Neural Networks(CNNs):

A particular kind of neural network that excels at processing images is the CNN. They use a technique called convolution to identify patterns in images, such as edges, corners, and shapes [23]. CNNs have become a popular choice for tasks such as image recognition, object detection, and segmentation [17][19].

B. Recurrent Neural Networks (RNNs):

RNNs are a type of neural network where sequential data can be processed such as text, speech. Unlike traditional neural networks, which process all inputs independently, RNNs use feedback connections to retain information from previous inputs. This allows them to remember context and understand the meaning of a sentence, for example [11],[13],[17].

C. Generative Adversarial Networks(GANs):

A particular kind of neural network called a GAN is used to create new data based on old data. They are made up of a generator network,which generates fresh data, and a discriminatornetwork, which assesses the quality of the created data. In a procedure known as adversarial training, the two networks are trained simultaneously while the generator triesto trick the discriminator and the discriminator tries to accurately identify the generated data [6].

D. Long Short-Term Memory (LSTM):

It's a kind of RNN that can remember information for a longer time than traditional RNNs. They are designed to solve the "vanishing gradient" problem that can occur in deep neural networks, where information is lost as it propagates through the network. LSTMs have been used successfully for tasks such as speech recognition, language translation, and music generation [24].

Method	Effects	Solutions
CNNs	Can identify patterns in images. Can be used for object detection, segmentation, and recognition	Use convolution to identify features. Apply filters to extract relevant information from images
RNNs	Can process sequential data such as speech and text. Can retain information from previous inputs to understand context.	Use feedback connections to retain information. Use gating mechanisms tocontrol information flow
LSTMs	Can remember information for longer periods than traditional RNNs. Can solve the vanishing gradient problem in deep neural networks.	Use memory cells to store information. Use gating mechanisms to control the flow of information
GANs	Can generate new data based on existing data. Can be used for image and music generation.	Use two networks that compete with each other. Train the generator to produce data that fools the discriminator.

Table 1: Countermeasures to Security

VI. CONCLUSION:

The preservation of privacy is a crucial component of any private data and poses a significant obstacle to its widespread adoption because privacy preservation techniques are largely dependent on internet connections, making them susceptible to various attacks and security risks that could have either minor or major repercussions. We have looked at the articles that include important assaults that jeopardize data security. Deep Learning techniques have demonstrated considerable promise for protecting privacy across a range of applications. We provide answers and potential defenses as a point of comparison for comparative study.

REFERENCES:

1. Agrawal, Shaashwat, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Mamoun Alazab, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. "Federated learning for intrusion detection system: Concepts, challenges and future directions." Computer Communications(2022).

2. Singh, Saurabh, Shailendra Rathore, Osama Alfarraj, Amr Tolba, and Byungun Yoon. "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology." Future Generation Computer Systems 129 (2022): 380-388.

3. Durrant, Aiden, Milan Markovic, David Matthews, David May, Jessica Enright, andGeorgios Leontidis. "The role of cross-silo federated learning in facilitating data sharing inthe agri-food sector." Computers and Electronics in Agriculture 193 (2022): 106648.

4. Lee, Joon-Woo, HyungChul Kang, Yongwoo Lee, Woosuk Choi, Jieun Eom, Maxim Deryabin, Eunsang Lee et al. "Privacy-preserving machine learning with fully homomorphic encryption for deep neural network." IEEE Access 10 (2022): 30039- 30054

5. Dou, Qi, Tiffany Y. So, Meirui Jiang, Quande Liu, Varut Vardhanabhuti, Georgios Kaissis, Zeju Li et al. "Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study." NPJ digital medicine 4, no. 1 (2021): 60.

6. Ali, Mansoor, Faisal Naeem, Muhammad Tariq, and Geroges Kaddoum. "Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey." IEEE journal of biomedical and healthinformatics (2022).

7. Nguyen, Tham, Naveen Karunanayake, SicongWang, Suranga Seneviratne, and Peizhao Hu. "Privacy-preserving spam filtering using homomorphic and functionalencryption." Computer Communications 197(2023): 230-241.

8. Shorten, Connor, Taghi M. Khoshgoftaar, and Borko Furht. "Deep Learning applications for COVID-19." Journal of big Data 8, no. 1 (2021): 1-54.

9. Alguliyev, Rasim M., Ramiz M. Aliguliyev, and Fargana J. Abdullayeva. "Privacy- preserving deep learning algorithm for big personal data analysis." *Journal of Industrial Information Integration* 15 (2019): 1-14.

10. Alkhelaiwi, Munirah, Wadii Boulila, Jawad Ahmad, Anis Koubaa, and Maha Driss. "An efficient approach based on privacy-preservingdeep learning for satellite image classification." *Remote Sensing* 13, no. 11 (2021): 2221.

11. Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, and Gautam Srivastava. "P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot." IEEE Transactions on Industrial Informatics 18, no. 9 (2022): 6358-6367.

12. Huang, Qi-Xian, Wai Leong Yap, Min-Yi Chiu,and Hung-Min Sun. "Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images." IEEE Access 10 (2022): 66345-66355.

13. Popescu, Andreea Bianca, Ioana Antonia Taca, Anamaria Vizitiu, Cosmin Ioan Nita, Constantin Suciu, Lucian Mihai Itu, and Alexandru Scafa-Udriste. "Obfuscation Algorithm for Privacy-Preserving Deep Learning-Based Medical Image Analysis." Applied Sciences 12, no. 8 (2022): 3997.

14. Gupta, Deepti, Smriti Bhatt, Paras Bhatt, Maanak Gupta, and Ali Saman Tosun. "Game Theory Based Privacy Preserving Approach for Collaborative Deep Learning in IoT." In Deep Learning for Security and Privacy Preservationin IoT, pp. 127-149. Singapore: Springer Singapore, 2022.

15. Dash, Bibhu, Pawankumar Sharma, and Azad Ali. "Federated Learning for Privacy- Preserving: A Review of PII Data Analysis in Fintech." *International Journal of Software Engineering & Applications (IJSEA)* 13, no. 4 (2022).

16. Ali, Mansoor, Faisal Naeem, Muhammad Tariq, and Geroges Kaddoum. "Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey." IEEE journal of biomedical and health informatics (2022).

17. Han, Gang, Tiantian Zhang, Yinghui Zhang, Guowen Xu, Jianfei Sun, and Jin Cao. "Verifiable and privacy preserving federated learning without fully trusted centers." Journalof Ambient Intelligence and Humanized Computing (2022): 1-11.

18. Tsouvalas, Vasileios, Tanir Ozcelebi, and Nirvana Meratnia. "Privacy-preserving speech emotion recognition through semi-supervised federated learning." In 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 359-364. IEEE, 2022.

19. Yadav, Santosh Kumar, Siva Sai, Akshay Gundewar, Heena Rathore, Kamlesh Tiwari, Hari Mohan Pandey, and Mohit Mathur. "CSITime: Privacy-preserving human activity recognition using WiFi channel state information." Neural Networks 146 (2022): 11-21.

20. Liu, Shengheng, Chong Zheng, Yongming Huang, and Tony QS Quek. "Distributedreinforcement learning for privacy-preserving dynamic edge caching." IEEE Journal on Selected Areas in Communications 40, no. 3 (2022): 749-760.

21. R. Parekh et al., "GeFL: Gradient Encryption- Aided Privacy Preserved Federated Learning for Autonomous Vehicles," in IEEE Access, vol. 11, pp. 1825-1839, 2023, doi: 10.1109/ACCESS.2023.3233983.

22. Rasim M. Alguliyev, Ramiz M. Aliguliyev, Fargana J. Abdullayeva, Privacy-preserving deep learning algorithm for big personal data analysis,Journal of Industrial Information Integration,Volume 15, 2019 Shorten, Connor, Taghi M. Khoshgoftaar, and Borko Furht. "Deep Learning applications for COVID-19." *Journal of big Data* 8, no. 1 (2021): 1-54.

23. Alkhelaiwi, Munirah, Wadii Boulila, Jawad Ahmad, Anis Koubaa, and Maha Driss. "An efficient approach based on privacy-preserving deep learning for satellite image classification." *Remote Sensing* 13, no. 11 (2021): 2221.

24. Zhang, Zhixiang, Qian Lu, Hansong Xu, Guobin Xu, and Fanyu Kong. "Privacy-preserving Deep Learning For Electricity Consumer CharacteristicsIdentification." *Frontiers in EnergyResearch* (2022): 1273.

25. Diethe, Tom, Oluwaseyi Feyisetan, Borja Balle, and Thomas Drake. "Preserving privacyin analyses of textual data." (2020).

26. Seyedi, Salman, Zifan Jiang, Allan Levey, and Gari D. Clifford. "An investigation of privacy preservation in deep learning-based eye- tracking." *Biomedical engineering online* 21, no. 1 (2022): 1-12.

27. Javaid, Ahmad, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. "A deep learning approach for network intrusion detection system." In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, pp. 21-26. 2016.

28. Topaloglu, Mustafa Y., Elisabeth M. Morrell, Suraj Rajendran, and Umit Topaloglu. "In the pursuit of privacy: the promises and predicaments of federated learning in healthcare." *Frontiers in ArtificialIntelligence* (2021): 147.

29. Kaissis, Georgios, Alexander Ziller, Jonathan Passerat-Palmbach, Théo Ryffel, DmitriiUsynin, Andrew Trask, Ionésio Lima Jr et al. "End-to-end privacy preserving deep learning on multi-institutional medicalimaging." *Nature Machine Intelligence* 3, no. 6(2021): 473-484.

30. Lee, Joon-Woo, HyungChul Kang, Yongwoo Lee, Woosuk Choi, Jieun Eom, Maxim Deryabin, Eunsang Lee et al. "Privacy-preserving machine learning with fully homomorphic encryption for deep neural network." *IEEE Access* 10 (2022): 30039- 30054.