Privacy-Preserving in the Context of Data Mining and Deep Learning

Amjaad Altalhi[1], Maram AL-Saedi[1], Hatim Alsuwat[2] and Emad Alsuwat[1]

[1] Department of Computer Science, College of Computers and Information Technology, Taif University, Saudi Arabia
[2] Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

Summary
Machine-learning systems have proven their worth in various industries, including healthcare and banking, by assisting in the extraction of valuable inferences. Information in these crucial sectors is traditionally stored in databases distributed across multiple environments, making accessing and extracting data from them a tough job. To this issue, we must add that these data sources contain sensitive information, implying that the data cannot be shared outside of the head. Using cryptographic techniques, Privacy-Preserving Machine Learning (PPML) helps solve this challenge, enabling information discovery while maintaining data privacy.

In this paper, we talk about how to keep your data mining private. Because Data mining has a wide variety of uses, including business intelligence, medical diagnostic systems, image processing, web search, and scientific discoveries, and we discuss privacy-preserving in deep learning because deep learning (DL) exhibits exceptional exactitude in picture detection, Speech recognition, and natural language processing recognition as when compared to other fields of machine learning so that it detects the existence of any error that may occur to the data or access to systems and add data by unauthorized persons.

Key words: Privacy-Preserving Machine Learning; Data Mining; Deep Learning.

1. Introduction

Machine learning techniques have shown their ability to help in the derivation of valuable inferences in various necessary fields, including healthcare and finance. The sensitive and confidential existence of the data in these industries naturally raises questions about data privacy. This sparked the area to (PPML) Privacy-Preserving Machine Learning, which ensures data privacy. [1]. on the other side, prediction is collecting existing data and then applying that information to produce new data that isn't yet available [2]. Artificial Neural Network (ANN) and Random Decision Tree (RDT) are examples of machine learning techniques (MLT), Support Vector Machine (SVM), and Deep learning are widely used in data mining to explore information from distributed data, such as finding exciting patterns, association in between entities, the effect of the specific entity on the result, prediction, classification [3][4].

Deep learning (DL) exhibits exceptional exactitude in image detection, production of natural language, and speech recognition compared to other fields of machine learning [5]. The (DL) is a kind of artificial intelligence that can learn and categorize objects and similarly interpret data to a human brain. When we train a machine, we can make predictions and make decisions based on current data, which serves as our education data a deep learning model, by leveraging deep learning capabilities [2].

In the present era, with the utilization of better Machine Learning Techniques, data mining has become a fascinating research domain in communication industry. Business intelligence is an application of many applications of data mining, medical diagnostic systems, image processing, web search, scientific discoveries [3]. Traditional data mining applications use data generated and maintained by a single source for training the algorithms. The accuracy of applications of depend on the number of cases, a.k.a. volume, of data samples used in training [6]. Advancement in computing allows data mining algorithms on distributed data samples, where two or more parties share their data for training and execute a collaborative learning process. The performance and accuracy of distributed data mining applications are better than traditional data mining applications due to the movement of learning algorithms on the large volume of data samples shared by multiple parties [6][7].

This paper contains four-section; the first one is the introduction; it includes the primary information about not only Machine Learning (ML) domain but also its Privacy-Preserving. The second section includes a wealth of information about (PPML) machine learning in two areas. The first is about primary data and the second in deep understanding. The third section is the discussion about the paper contents. The last section shows the conclusion and potential directions of this paper.

2. Related Work

This section mainly introduces several information about the Privacy-preserving Machine Learning in two areas, the first thing in data mining and the second in deep learning; therefore, some researchers have given huge attention to providing Privacy-preserving. Their proposed approaches are discussed as follow: When sensitive data is used to build a machine-learning model, data privacy must be prioritized. Academic endeavors in the field of medicine, as well as for-profit companies, cannot advance until they can access confidential patient information in a format that protects your privacy. It can be disastrous to use a machine learning model without first understanding what is going on within

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.18

its hidden layers. With legal ramifications. Data anonymization in the training collection, which eliminates all publicly identifiable information, is an excellent place to start when it comes to protecting privacy. Privacy-preserving has been developed as a significant concern regarding the accomplishment the research of data mining. PPDM aims to secure the privacy of sensitive data without violating its value. Once a person has enough knowledge and awareness about data privacy, he/she becomes more and more not willing to share secret information with untrusted parties. This prompts the unintentional consequences of data mining. A few methods have been proposed inside privacy constraints, yet this part of the research is in its early stage. The success of algorithms of PPDM are estimated as far as its level of vulnerability and resilience to cyberattacks. Indeed, no privacy-preserving algorithm exists that surpasses all other privacy-preserving algorithms on every conceivable basis. Maybe, an algorithm may perform better compared to another on one explicit basis. Thus, this paper aims to introduce PPDM tools and procedures and recommend some future research paths [24]. Netflix held a Million-Dollar Proposal [8] for the community of data scientists, in which anonymous users submitted anonymous movie reviews exceeding 500,000 for a total of 17,770 films. Using publicly accessible Internet Movie Database (IMDB) data, Arvind Narayanan and Vitaly Shmatikov demonstrated a dependable de-anonymization process. [3] That successfully identified Netflix records of known users and other potentially sensitive information. According to C. Dwork's[4] [9] study, differential privacy is a privacy philosophy that is customized to the personal data processing with the goal of learning information about the entire population while maintaining the secrecy of each individual. Differential privacy ascertains that the system behaves similarly, regardless of whether everyone can choose to enter or leave a database in the system [7]. Intuitively, this implies that no single person's data significantly influences the mechanism's distribution of production. Personal data-handling organizations, such as Patients' health records or the other kind of data, are apprehensive because of their capacity to participate in ML, partly because of the absence of simplicity in the legislation governing the use of such information, and partly because of concerning about accidentally breaching people' privacy when mining such data (ML) [6].

A. Privacy-Preserving Techniques in Data Mining

By translating plain values into ciphertext, privacy protection techniques secure users' personal information. Data mining applications that preserve privacy were initially created in 2000, employing two distinct styles: data randomization and cryptography. Randomization-based Approaches: Agarwal [7] invented and used randomization (data perturbation) techniques for privacy protection by introducing noise to the source data.

Cryptographic-based Approaches:

Yao [10] and Goldreich [11] pioneered many privacy-preserving data mining techniques with their pioneering work Safe Multi-party Computation (SMC). Lindell and Pinkas [12] used cryptographic tools to construct a stable decision tree classifier that was more effective than the perturbing data process. Cryptographic methods are excellent at preserving privacy and precision, but they are challenging to use for large data sets because they need more time. Researchers are designing various privacy-preserving data mining applications in supervised and unsupervised learning processes based on the directions of these two landmark contributions. The homomorphic encryption property of RSA was demonstrated for the first time by Adleman and Dertouzous [13][14]. The effects of homomorphic encryption operations on ciphertexts are the same as operations on their respective plaintexts without ciphertext decryption [15], making it more effective in privacy-preserving data mining. Homomorphic encryption, a cryptographic-based method, has a more vital ability to perform stable multiparty computation [16].

a) Additive Homomorphic Encryption – Product of two ciphertexts Ek(PT1) and Ek(PT2) is equivalent to the addition of their plaintext: Ek(PT1 + PT2) is equal to Ek (PT1) times Ek (PT2). E.g., Okamoto-Uchiyama [17], Pallier [18]

b) Multiplicative Homomorphic Encryption- Multiplication of two ciphertexts Ek(PT1) and Ek(PT2) equal to the product of their plaintexts: Ek(PT1 * PT2) is equal to Ek (PT1) times Ek (PT2). Rivest et al. [13] and ElGamal [19] are two examples.

Machine learning techniques for protecting privacy users analyze data and extract categories as classes in data classification, an important data mining application. The training phase and the testing phase are the two phases in the creation of a classifier. Machine learning techniques such as ANN, RDT, SVM, Nave Bayesian Classification [3], and Deep Learning Model [11] are used to construct a classifier.

B. Deep Learning Privacy Security

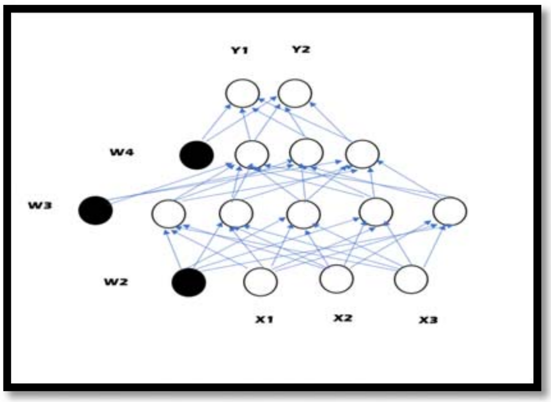

Fig. 1: Two hidden layers in a neural network that is normal the inputs are Xi, the outputs are Yi, the prejudices are black circles, and the weight vectors are Wi.

As shown in Figure 1, deep learning architectures multi-layer neural networks (MLNs) are a form of neural network that has made up many layers: inputs and outputs, as well as one or more hidden layers that link them together. The layers are connected in a typical neural network by neuron. Data transformation mathematically takes the total input, which is the average weighted of all of the information. A bias signal is introduced, and it is activated using a nonlinear activation function called a sigmoid activation function. The two stages of deep learning are as follows:

- The training process, during which the deep learning classifier assigns random weights to each data layer. A standard neural two secret layers in the network is shown in Figure1. The inputs are xi, the outputs are yi, the biases are black circles, and for computing the weighted averages of inputs, the weight vectors are Wi. [4]. to make predictions about class labels and grades, run a forward pass through the results. A mistake, or loss function, is determined by comparing the class scores to the actual labels. The weights are modified due to his mistake propagating across the network. Following a single sample or a group of samples, the weights are changed.
- Inference process: by conducting a forward pass equivalent to the preparation stage, a trained model is used to infer/predict results from research and real-world data. Since the aim isn't to memorize the blueprint. The inference method does not provide a phase for back-propagation to measure, fix the problem and recalculate the weights. [20].

Artificial Intelligence Machine learning is "a region of research this enables computers to pick up without being explicitly programmed," relatively to Arthur Samuel, the trailblazer around artificial intelligence and video games. Machine learning algorithms are designed to generalize results, and you can learn how to perform specific tasks. A collection of samples is commonly used as the input data to a machine learning algorithm. An assortment of feature values will be present in each sample. Consider a picture with a resolution of 100x100 pixels, with a single digit identifying each pixel (0-255 grayscale). These pixel values can be mixed and matched to make a new image. A 10,000-dimensional vector is known as a function vector. A function vector is associated with each image .Can have a sticker attached to it (for example, the person's name depicted in the photograph). To construct an ML model, a training set of multiple feature vectors and their labels will be used by an ML algorithm. The training or learning phase refers to this process. When a new sample for testing is introduced to this ML model, it should offer the expected mark. (In facial recognition systems, a person's name or identifier). The ability of machine learning the ability of a model to calculate how well you can correctly predict the label is how well you can correctly predict the label. It generalizes to new data. The test error (generalization error) is an empirical statistic that varies with the amount and quality of data used to train the model. How were the proper parameters of the ML technique found, and what machine learning strategy was employed to generate the model? (e.g., cross-validation), and how were the features extracted? (if any were needed).

Organizations nowadays are very reliant on results of Data Mining and machine learning to not only offer better assistance but also achieve more prominent profit and better decision-making. That is why companies gather enormous measure of data, which combines confidential data about not only individuals but also businesses. When we run a DM algorithm against such a dataset, the algorithm can extract knowledge and uncovers the information viewed as private. The real danger occurs once information gets presented to a malicious person. This information will be abused. Privacy, for example, can be compromised when DM techniques are utilized [25]. A feature extraction method can be needed to extract raw data with valuable features, such as during a pre-processing stage for images (as unprocessed data). The information is then cropped and resized to 100x100 pixels to match the function vector length3, or PCA4 is used to protect the data to smaller dimensions. While feature engineering is needed for many, it has been reduced to merely pre-processing steps in many applications. In many modern applications. Feature vectors are used to generate data sets whatever the case could be the data is tagged or not, depending on the application or learning method. [21].

3. Discussion

We covered privacy preservation in data mining in this work. Because Data mining has a wide variety of uses, including business intelligence, medical diagnostic systems, image processing, web search, and scientific discoveries, and we discuss the privacy-preserving in deep learning because deep learning (DL) exhibits exceptional exactitude in image detection, production of natural language, and speech recognition as when compared to other fields of machine learning so that it detects the existence of any error that may occur to the data or access to systems and add data by unauthorized persons.

According to C. Dwork's [4] [9] study, it is a concept of a level of privacy suited to personal information processing to gather data on the entire population while preserving each individual's privacy.

Then, we discussed privacy-preserving techniques. I was using two different techniques: data randomization and cryptography. The first technique was a randomization-based approach by introducing noise to the source data. Agarwal [7] invented and used randomization (data perturbation) techniques for privacy protection. Then we had a cryptographic-based approach,

Yao [10] and Goldreich [11] pioneered many privacy-preserving data mining techniques with their pioneering work Safe Multi-party Computation (SMC). Lindell and Pinkas [12] used cryptographic tools to construct a stable decision tree classifier that was more effective than the perturbing data process. Cryptographic methods are excellent at preserving privacy and precision, but they are challenging to use for large data sets because they need more time. Researchers are designing various privacy-preserving data mining applications in supervised and unsupervised learning processes based on the directions of these two landmark contributions.

On the other hand, machine learning techniques for protecting privacy users analyze data and extract categories as classes in data classification, an important data mining application. The training phase and the testing phase are the two phases in the creation of a classifier. Machine learning techniques such as ANN, RDT, SVM, Nave Bayesian Classification [3], and Deep Learning Model [11] are used to construct a classifier.

Finally, we discourse Among Artificial Intelligence Machine learning is "According to Arthur Samuel, a tech visionary games and AI, "an area of science that gives machines the desire to learn without having to be taught directly programmed. Machine learning algorithms are designed to find out how to do specific tasks by combining data. A collection of samples is commonly used as the input data to a machine learning algorithm. An assortment of feature values will be present in each instance.

Table 1.1: Summary

	Performance Measurement	***Model implementation for data mining***
Yuan and S. Yu [4]	Comparison of learning time, contact costs, and error rates	Each party prepares a BPN network that is well trained.
Jaideep Vaidya et al. [22]	Build a classification tree Accuracy of Time Classification	For classification, each site had its RDTs installed.
Y Rahulma Dhavan [23]	Computation time, classification accuracy	Two-class and multi-class SVM classifiers are built on a centralized server.
Zhang Qingchen [11]	Accuracy of classification	A centralized server manages the deep computational model.

Table 1.2: Summary

	Machine Learning algorithm	***Data Distribution***	***Privacy Concerns***	***Method Description***
Yuan and S. Yu [4]	Neural Network with BackPropagation	Distributed (Arbitrary Partitioned)	Model who is semi-honest Input data and intermediate outcomes are kept entirely private.	Secure Scalar Product and Addition based on SMC, Scalar Product Protected Share, and Sum.
Jaideep Vaidya et al. [22]	Random Decision Tree	Distributed (Partitioned in a Horizontal way and in Vertical way)	Data privacy is maintained using a semi-honest model, semantically secure homomorphism, and threshold cryptography. Leakage of the average sum from class distribution vector during classification	Structured randomness, Paillier cryptosystem, Secure Share Protocol Secure Sum Protocol
Y Rahulma Dhavan [23]	Computer to Support Vectors	Distributed	When clients communicate with servers, they become adversaries.	Stable Two-Party Computation, Paillier Cryptosystem, Semi-Honest Model
Zhang Qingchen [11]	Model of Deep Computing	Distributed	The client can only decrypt the values.	Completely homomorphic encryption, secure addition, and fast multiplication are all features of BGV.

4. Conclusion Future Work:

This paper includes introduction Includes the primary information about machine learning and Privacy-preserving Machine Learning and we Since data mining has a broad range of applications, including business intelligence, medical diagnostic systems, image processing, web search, and scientific discoveries, we discussed the issue of privacy preservation in the domains of data mining. When DL is compared to other fields of study machine learning, it demonstrates excellent precision in image detection, speech recognition, and natural language processing, so it detects any data errors as well as unauthorized access to systems and data addition. This research article aims to train data privacy preserving challenges and solution approaches from an ERP perspective. Future research can include other aspects like the model or hyperparameter theft. More privacy-preserving algorithms will be integrated into the system for industrial use. GPU/FPGA acceleration will be investigated for further speed optimization.

References

[1] A Patra, A Suresh - arXiv preprint arXiv:BLAZE: Blazing Fast Privacy-Preserving Machine Learning2005.09042, 2020 - arxiv.org

[2] H. C. Tanuwidjaja, R. Choi, S. Baek, and K. Kim, "Privacy-Preserving Deep Learning on Machine Learning as a Service—a Comprehensive Survey," in IEEE Access, vol. 8, pp. 167425-167447, 2020, DOI: 10.1109/ACCESS.2020.3023084.

[3] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In IEEE Symposium on Security and Privacy, pages 111–125, 2008.

[4] C. Dwork, G. J. Pappas, "Privacy in information-rich intelligent infrastructure," 2017.

[5] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe and M. Atiquzzaman, "A Trustworthy Privacy-Preserving Framework for Machine Learning in Industrial IoT Systems," in IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6092-6102, Sept. 2020, DOI: 10.1109/TII.2020.2974555

[6] Carlini, Nicholas, et al., The Secret Sharer: Evaluating and testing unintended memorization in neural networks (2019), 28th USENIX Security Symposium (USENIX Security 19)

[7] R. Agrawal and R. Srikant, "Privacy-preserving data mining," Proc. 2000 ACM SIGMOD Int. Conf. Manag. data - SIGMOD '00, vol. 29, no. 2, pp. 439–450, 2000

[8] Netflixchallenge-https://dl.acm.org/doi/10.1145/1345448.1345465

[9] C. Dwork, G. N. Rothblum, and S. Vadhan, "Boosting and Differential Privacy," 2010 IEEE 51st Annual Symposium on Foundations of Computer Science, Las Vegas, NV, 2010, pp. 51- 60.

[10] A. C. Yao, "Protocols for secure computations," 23rd Annu. Symp. Found. Comput. Sci. (secs 1982), pp. 1–5, 1982.

[11] O. Goldreich, S. Micali, and A. Wigderson, "How to Play any Mental Game," Stoc '87, pp. 218–229, 1987

[12] Wu, B., Chen, C., Wang, L., Wang, L., Tan, J., Chen, C., ... & Sun, G. (2020). Poster: Nebula: an Industrial-purpose Privacy-preserving Machine Learning System. In 2020 IEEE Symposium on Security and Privacy (SP). IEEE.

[13] Gaur, M. (2020). Privacy-Preserving Machine Learning Challenges and Solution Approach for Training Data in ERP Systems. International Journal of Computer Engineering and Technology.

[14] Reddy, S. M., & Miriyala, S. (2020). Security and privacy-preserving deep learning. arXiv preprint arXiv:2006.12698.

[15] Raynal, M., Achanta, R., & Humbert, M. (2020). Image Obfuscation for Privacy-Preserving Machine Learning. arXiv preprint arXiv:2010.10139.

[16] Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving, and federated machine learning in medical imaging. Nature Machine Intelligence, 2(6), 305-311

[17] Tanuwidjaja, H. C., Choi, R., Baek, S., & Kim, K. (2020). Privacy-Preserving Deep Learning on Machine Learning as a Service—a Comprehensive Survey. *IEEE Access*, *8*, 167425-167447.

[18] Xu, K., Yue, H., Guo, L., Guo, Y., & Fang, Y. (2015, June). Privacy-preserving machine learning algorithms for extensive data systems. In 2015 IEEE 35th international conference on distributed computing systems (pp. 318-327). IEEE.

[19] Rachuri, R., & Suresh, A. (2019). Trident: efficient 4PC framework for privacy-preserving machine learning. arXiv preprint arXiv:1912.02631.

[20] Boulemtafes, A., Derhab, A., & Challal, Y. (2020). A review of privacy-preserving techniques for deep learning. Neurocomputing, 384, 21-45.

[21] Behler, J. (2016). Perspective: Machine learning potentials for atomistic simulations. The Journal of chemical physics, 145(17), 170901.

[22] J. Vaidya, B. Shafiq, W. Fan, D. Mehmood, and D. Lorenzi, "A Random Decision Tree Framework for Privacy-Preserving Data Mining," IEEE Trans. Dependable Secure. Comput., vol. 11, no. 5, pp. 399–411, 2014.

[23] M. Rajarajan, K. Cumanan, S. Veluru, R. C.-W. Phan, and Y. Rahulamathavan, "Privacy-Preserving Multi-Class Support Vector Machine for Outsourcing the Data Classification in Cloud," IEEE Trans. Dependable Secure. Comput., vol. 11, no. 5, pp. 467–479, 2013.

[24] The IEEE computer society, 2004, "Privacy-Preserving Data Mining: Why, How, and When."

[25] Mahesh Dhande, N.A.Nemade and Yogesh Kolhe, 2013, "Privacy Preserving in K- Anonymization Databases Using AES Technique"

Amjaad Altalhi received her bachelor’s degree in Information Technology from Taif University, Saudi Arabia, in 2012. Currently, she is a graduate student at Taif University. She is doing her master’s degree in cybersecurity studies. Amjaad’s research interests are in cybersecurity, which includes information security, machine-learning security, privacy-preserving, and intrusion detection systems.

Maram ALSaedi received her bachelor's degree in computer science Umm Al Qura University, Saudi Arabia, 2016. Currently, she is a graduate student at Taif University, doing her master's degree in cybersecurity studies. Maram's research interests are in cybersecurity, which includes information security, privacy-preserving in machine learning and data mining, and intrusion detection systems.

Hatim Alsuwat is an assistant professor of Computer Science in the College of Computers and Information Systems at Umm Al-Qura University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Information Security, Cryptography, Model Drift, and Secure Database Systems.

Emad Alsuwat is an assistant professor of computer science in the College of Computers and Information Technology at Taif University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Probabilistic Graphical Models (esp. Bayesian Networks), Artificial Intelligence, Information Security, and Secure Database Systems.