Journal of Basrah Researches (Sciences) **48**(1), 10 (2022)
DOI: https://doi.org/10.56714/bjrs.48.1.2

Survey: Privacy-Preserving in Deep Learning based on Homomorphic Encryption

Sura M. Abdullah[*]

Department of Computer Sciences, University of Technology, Baghdad, Iraq

ARTICLE INFO

Received 25 February 2022
Accepted 26 March 2022
Published 31 July 2022

Keywords:

Homomorphic Encryption, Deep Learning, and Privacy-Preserving.

ABSTRACT

When deep learning techniques succeed, the amount of data accessible for training grows rapidly, the main successor is the collecting of user data at scale in huge enterprises. Because users' data is sensitive, and the manner of preserving this information (pictures and audio recordings) indefinitely, data collecting raises privacy concerns. The terms privacy and confidentiality are related to avoiding sharing this information, and deep learning cannot be accrued on a larger scale in the amount of data. There are some challenges in machine learning algorithms when needing to access data for the training process. There several technologies in deep learning for privacy-preserving have been evolving to assign the issues, including the multi-lateral computation secrecy and the symmetric encryption in the term of the neural network. This survey deals with the deep learning techniques concerning the privacy issue mainly related to input data and the ability of interesting directions in these learning processes. Finally, as a side contribution, we analyze and introduce some variations to the bootstrapping technique of deep learning. That offers an improved parameter in efficiency at the cost of increasing privacy.

Citation: S. M. Abdullah, J. Basrah Res. (Sci.) **48**(1), 10 (2022). DOI:https://doi.org/10.56714/bjrs.48.1.2

1. Introduction

Recent advances in deep learning methodologies based on artificial neural networks (ANN) have led to advancements in Artificial Intelligence (AI) tasks for a variety of areas, including picture, audio, and text recognition, as well as translation across many languages. Large information technology businesses, such as Facebook, Apple, and Google, benefit from the massive amount of data received from consumers and apply deep learning computations driven by GPU farms. The model that emerged from the previous steps was accurate enough to be employed in a variety of services and applications, including picture recognition [1], and Text categorization is the task in which documents are classified into one or more of predefined categories based on their contents [2]. The value of deep learning is undeniable, as the same training data can be successful in addressing privacy concerns. Millions of people have been subjected to a privacy risk as a result of the practice of collecting data (picture, speech, and video) in a central form. The firms keep the data forever, and the users have no control over it in terms of deleting it or influencing what is

[*]**Corresponding author email :** Sura.M.Abdullah@uotechnology.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://bjrs.uobasrah.edu.iq

learned from it. Second, photos and audio recordings frequently contain sensitive and personal information like as faces, license plates, computer screens, other people's voices, and ambient noises that are captured by mistake. [3], etc. Third, national security and intelligence agencies have access to user data through subpoenas, warrants, and unwarranted spying. Selecting data sets that can yield a suitable response in machine learning is one of the most difficult difficulties. It is necessary to ensure that the data is not leaked because it must be distributed to many individuals. Sensitive users are hesitant to hand over their personal information to external provider [4]. Due to a compromised server-side, there is a possibility of data leakage, as in the case of cloud storage. Users prefer no save sensitive data in the cloud because they are concerned that others may read their information and encroach on their privacy. To reassure consumers of their data security and privacy, researchers combined privacy-protected data with deep learning training procedures. In order to employ the neural network in a private situation, several strategies can be used. The rapid growth of the multimedia and communication sectors has generated worries about the security of digital photographs transmitted across open or stored networks [5, 6]. The issue statement for this study is that the privacy of the data, which is normally encrypted and accessible only to those who are permitted to see it, should be safeguarded. However, the problem statement when we need to execute mathematical operations on this encrypted data, such as categorizing it using artificial intelligence algorithms, the problem arises since homographic encryption techniques only support two operations: addition and multiplication. To produce reliable categorization results, artificial intelligence algorithms require more than addition and multiplication processes. The main objective is to present deep learning techniques used in recent years to implement a high-precision classification on encrypted data. For that, the contribution in these paper summaries the solutions' effects, performance-based determines the deep learning difficulties. It also offers a wide variety of choices that include more than many recent solutions articles different privacy-preserving deep learning techniques. Finally, determine the problems associated with Deep learning in the case of its use within encrypted data. In this survey, all methods addressing problems and challenges in privacy preservation through deep learning and privacy preservation practices are reviewed and evaluated.

2. Deep Learning in Artificial Intelligent

The basic function of the Deep Learning algorithm is to extract complicated attributes from high-dimensional data and develop a model between input and output based on the acquired data. Multi-layered networks are commonly used in deep learning architectures to abstract more attributes computed as nonlinear functions of low-level attributes. Layered neural networks are the most common type of Deep learning architecture. [3]. the structure of Deep's learning is represented by different layers.

2.1. Convolutional Neural Network background (CNN)

Multilayer perceptron's are not well suited to various forms of data, particularly photographs. Indeed, they are designed to work with vectors as input data, therefore in order to use them with photos, we must first convert them to vectors, losing any spatial information contained in the images, such as shapes. Prior to the introduction of deep learning for computer vision, learning was based on the extraction of variables of interest, known as features, but these approaches for image processing require a lot of expertise[7, 8]. A convolution layer is commonly employed and defined by CNN, and its purpose is to learn the characteristics retrieved from the dataset for picture classification. To make convolution, the CNN model has a dimension of N x N, It will produce a dot product seen between values of the neighborhood. As an outcome, the convolutional layer only has addition and multiplication functions. This layer does not need for changed because it may be used for symmetric encrypted 'HE' data [9], can explains in the blow Fig.

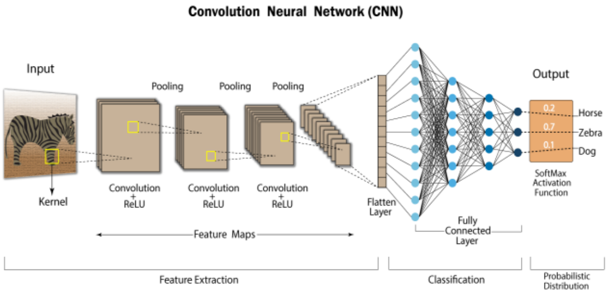

Fig. 1. Convolutional Neural Network.

2.2. Activation Layer in neural networks

When neural networks have a large number of layers (as in deep learning), the back propagation algorithm has difficulty estimating the parameter. This is why the rectified linear function has replaced the sigmoid function. This process is not differentiable in 0, however this isn't a problem in reality because the likelihood of having an entry equal to 0 is usually zero. In Fig. 2 explains the activation function [10]. This determines whether or not the data is triggered at one or zero. The activation layer is a nonlinear feature that applies the convolution layer's output to a mathematical algorithm. Because these tasks are nonlinear, they become substantially more difficult when used to measure Homomorphic Encrypted (HE) data. As a result, we'll have to come up with a replacement element that only has to be multiplied and added [5].

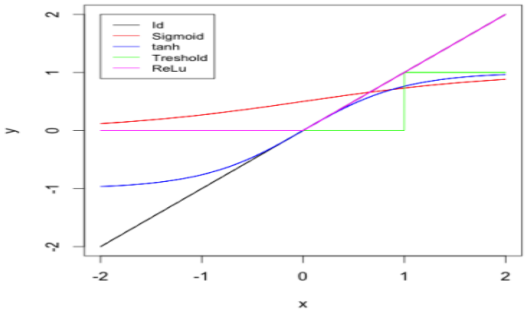

Fig. 2. Activation Function in neural networks Pooling Layer.

2.3. Pooling Layer

It's a sampling layer with the goal of keeping data as small as feasible. Pooling can take numerous forms, including maximum and average pooling, mean pooling, and so forth. We won't use HE's max-pooling option in this case, therefore we won't check the total value of encrypted data. The 'average pooling' solution is what we'll be used 'HE.' Because average in pooling determines values amount, there is just one additional process that must be performed on the 'HE' encrypted data [11]. The principle pooling layer can show in Fig. 3.

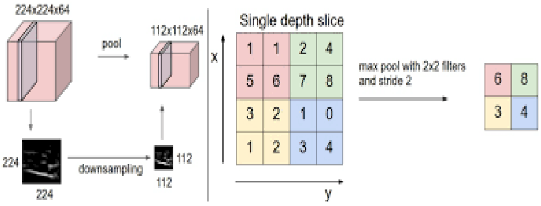

Fig. 3. Pooling Layer.

2.4. Fully Connected Layer

Feed forward neural networks are the focus of the Fully-Connected layers. The Fully Connected Layers are the network's final levels. The output from the final Pooling or Convolutional Layer, which is flattened and then fed into the fully connected layer, is the input to the completely connected layer [4]. Because each neuron in this layer is connected to the neuron in the previous layer, it is called the Fully Connected Layer. This layer, which consists of multiplication and addition functions, only has a dot product function. As a result, it can utilize it to decrypt HE data [12], can explain in Fig. 4.

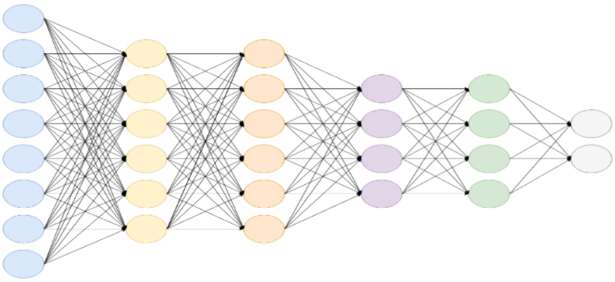

Fig. 4. Fully Connected Layer.

2.5. Dropout Layer

The Dropout layer, which helps minimize over fitting, sets input units to 0 at random with a rate frequency at each step during training time. It's worth noting that the Dropout layer only applies if the training parameter is set to true, in Fig. 5, which means that no data are dropped during inference. When working with a model. It's a layer created to deal with the problem of over-fitting. When training our machine learning model, the classification results are frequently perfect for specific types of data, indicating bias in the training set [13].

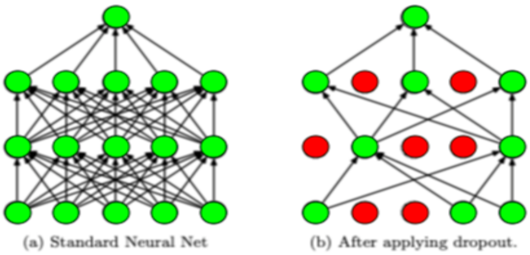

Fig. 5. Dropout Layer.

3. Homomorphic Encryption (HE)

Homomorphic encryption is a cryptographic technique that allows mathematical operations on data to be performed on cipher text rather than the original data. The cipher text is a version of the input data that has been encrypted (also called plain text). To achieve the necessary output, it is operated on and then decrypted. Different tools are employed to protect privacy. At the top are differential privacy techniques and homomorphic encryption, both of which are usually connected with polynomial approximation [14].In general, homomorphism is a mapping function from a domain set input element to an algebraic set range output element. To achieve encrypted results, HE encryption performs a special type of computation on cipher tests. By restricting the cloud service provider, standard encryption techniques do not allow actions on encrypted data. Customers don't have to worry about their data security or privacy while using cloud services because of this. This requires the development of an algorithm that performs computations on encrypted data, as proposed by Rivest, Adleman, and Dertouzous in 1978. This concept was dubbed "Privacy

Homomorphism". HE can be classified into three types according to the computational operations and the number of performed iterations [15]. Partially Homomorphic Encryption (PHE), this provides only one encrypted data process, either multiplication or addition. Somewhat Homomorphic Encryption (SWHE), it provides more processes, like addition and multiplication, nevertheless with limited operations. Fully Homomorphic Encryption (FHE), this provides multiple and addition and multiplication processes without restricting the functions. Can explain the type of HF in Fig. 6.

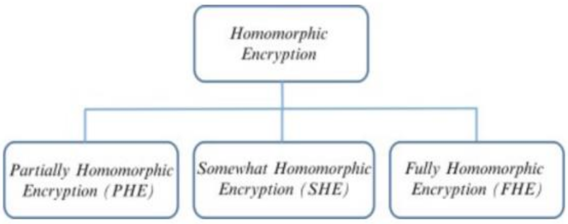
Homomorphic Encryption
Partially Homomorphic Encryption (PHE)
Somewhat Homomorphic Encryption (SHE)
Fully Homomorphic Encryption (FHE)

Fig. 6. Homomorphic Cryptography types.

So, in Eq. (1) and Fig. 7 the HE is the encryption algorithm E over an operation '∘' & is illustrated and where M represents the space of the messages:

$$(m1) \circ (m2) = (m1 \circ m2), \forall\, m1, m2 \,\epsilon\, \mathrm{M} \tag{1}$$

For the encryption in HE, this method include four stages [16].

- **Key Generation (KeyGen):** In this stage, security parameters are generated. In asymmetric type, a single key is generated, while in an asymmetric type, a pair of secret and public keys is generated.
- **Encryption Algorithm (Enc):** This stage encrypts the plaintext inputs message, m ϵ M, with the encryption key. The ciphertext is generated by $c = (m)$, where c ∈ C, C is the cipher text space.
- **Decryption Algorithm (Dec):** In this stage, the original message is recovered by decrypting ciphertext c using the decryption key $((c) = m)$.
- **The Evaluation Algorithm (Eval):** This stage performs the evaluations of the ciphertexts $(c1, c2)$, $(c1, c2) = Eval\ \{(m1, m2)\}$, without revealing the messages $(m1, m2)$, i.e. $\{(c1, c2)\} = (m1, m2)$.

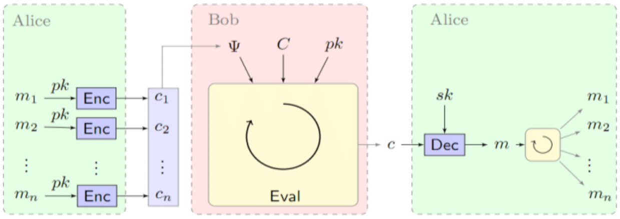

Fig. 7. Homomorphic Encryption Structure.

3.1. Secure Multi-Party Computation (SMPC)

Secure multiparty computing (MPC / SMPC), of which HE is a component, is a cryptographic approach for spreading a calculation across numerous parties while ensuring that none of the participants has access to the data of the others. Information scientists and analysts can compliantly, quietly, and discretely compute on different datasets using secure multiparty computation protocols without ever exposing or moving them. This is a new way of thinking that emphasizes participant connectedness. Data can be partitioned, and each actor only shares a fraction of their data with others, allowing them to interact and do calculations without having to re-create the original data.

As a result, it can be aggregated until each participant has completed it and is informed of the results of the production. In contrast to HE, parties in a protected MPC employ a protocol rather than a single entity to collectively measure a function on their inputs. The parties' secrets must be kept hidden during the process. In secure MPC, the parties have a low calculation cost but a high communication cost. In contrast to MPC, servers have a high processing cost and a low communication cost. It is far too broad to be used in training [17].

3.2. Differential Privacy

One way in HE is differential privacy is a method that allows academics and database analysts to extract meaningful information from databases containing people's personal information without disclosing personal information about individuals. Deals in cases were made without revealing any data there have been several studies on machine learning methods including decision trees, support vector machines, and logistic regressions with differential privacy. The three components of this algorithm are Differential Private Model Parameters, Input Data, and Mimic Learning [18].

4. Related Work

Deep Neural Networks (DNNs) have been adopted in production systems as a result of the ever-growing breakthroughs of deep learning in various fields, including vision, recommendation systems, and natural language processing, and so on. These advancements are primarily due to the availability of massive datasets and significant processing power. In this study we comparison in many directions as collaboration, non-collaboration and Multi parties [19].

4.1. Collaboration

CryptoNets, the researchers presented a new privacy-preserving learning architecture that addresses the three difficulties raised by earlier FHE-based systems such as CryptoNets. The name given to it is Globally Encrypted, Locally Unencrypted Deep Neural Network (GELU-Net). Every neuron is divided into linear and nonlinear elements in the intrinsic technique, which are subsequently executed individually on non-colluding participants. Paillier, a homomorphic cryptosystem, is used to do linear computations. It gives enough security confidence to keep data encrypted globally while still being significantly more efficient than CryptoNets' FHE. As a result, the first problem is resolved. It would be difficult to use Paillier without the original strategy of splitting the two components because it does not allow nonlinear polynomials. The cryptographic incomputable signals are handled in a locally unencrypted but privacy protected manner to maintain the existing correctness, which addresses problems two and three. To include privacy components into back propagation algorithms, the random masking technique was used for a loss-free model with little communication cost and computation. [20]. this work describes Deep Secure, the first secure key architecture for scaling DL-based analysis of data acquired by scattered clients. Deep secure makes it possible to employ cutting-edge architectures on sensitive data without sacrificing precision for security. For a generic case where both DL parameters and input data must always be kept hidden, we present an honest yet curious opponent model that is consistent with the literature.Deep Secure proposes using Yao's Garbled Circuit (GC) protocol to secure DL execution, this new study, unlike prior work based on homomorphic encryption, is based on homomorphic encryption [5], there is no among both in privacy with utility in the methods we used. When the sample size is smaller than 2600 samples acquired by each distributed client, our architecture is the best option for arrived data server from client with the least amount of delay. They provide a set of low-overhead pre-processing algorithms in the context of deep learning that reduce the GC total runtime even more [21].

4.2. Non-collaboration

Two methods for implementing a multi-key learning system are suggested in this study. Both solutions allow many data owners with various datasets to learn neural network architecture in the cloud while remaining secure. Before uploading sensitive data to a cloud server, data owners use multi-key fully homomorphic encryption (MK-FHE) and a hybrid framework that combines the dual decryption method Bresson, Catalano, and Pointcheval scheme (BCP) and completely homomorphic encryption (FHE) [18]. RG-RP is a privacy-preserving method that uses two phases of perturbation and randomization. To reduce the Maximum Posteriori (MAP) approximation from training data, the Repeated Gompertz (RG) nonlinear perturbation is applied. Second, a row orthogonal projection matrix is used to convert high-dimensional data to low-dimensional data. This is done via Independent Component Analysis to preserve precision, save transmission energy, and increase assault resistance (ICA). Depending on the participants' converted data, the cloud constructs model in deep learning.The suggested LSTM in CNN model combined with the RGRP privacy technique gives you an excellent balance of precision with privacy, according to the evaluation results. In terms of efficiency, the LSTMCNN outperforms other comparable model, both with and without confidentiality; however the privacy version of the LSTM-CNN performs marginally worse [22]. In the context of mobile sensed, this study established a unique lightweight framework for privacy-preserving CNN extracting features. They may be able to greatly lessen the burden on mobile sensors and end users by applying the encryption approach based on secret sharing and relocating demanding computing tasks to edge servers. Interaction between the server and the end user is also not required. As a result, they've developed a set of cryptographic building many blocks that aren't using computationally intensive for cryptographic techniques like homomorphic cryptography or damaged circuits. The CNN attributes privacy protection and extraction approach does not require any calculations for preferred familiar CNN layers, unlike earlier homomorphic encryption-based systems. As a result, empirical trials can be employed to test hypotheses [23].

4.3. Multi parties

The Edge Computing paradigm was used in this work to solve the data training problem by reducing or eliminating the transfer of user information to the cloud entirely, instead shifting computing to where the data actually exists under the user's discretion, which may reduce concerns about data breach and manipulation by simply preventing it from being gathered at scale in the first place. Attack motivations are reduced because, instead of a single cloud service, the offender must gain access to millions of devices in order to acquire data for millions of consumers. This idea was implemented in this paper by (i) Develop a personal machine learning approach where the majority of data remains on controlled devices; (ii) employing this technique to two learning tasks and get the results i.e., supervised (accelerometer traces activity recognition) and unsupervised(text documents modeling topic), and (iii) They look at the resilience of our approach against antagonistic attacks, as well as the practicality of putting such approaches into practice on a realistic constrained resource personal device: a Raspberry Pi 3 Model [24]. All servers own a component to neural network, which contains biases and weights matrices and is partitioned by the system administrator. A client who seeks a result encrypts their data and separates it into two secret postings, which are delivered to dual non-complicit many servers. Because the symmetric coding, the activation function layers are expected to be continuous, small-degree polynomials. Model is continuously run in servers, with encrypted forecasts are generated, which the client decodes for final prediction. According to the authors' theoretical research, the solution satisfies data and model in particular. The authors' analysis found that their approach outperformed the competition in terms of connections and computing complexity in terms of efficiency. They offer a new image processing technique based on Generative Adversarial Systems (GAS). The proposed technique allows us to apply images to DNN without requiring visual input, increasing its resilience to Crypto-Text Only Attacks (COAs), particularly those based on DNN. In this study, the proposed transformation method is shown to be capable of preserving visual information on normal photos, and optically secured images are directly applied to DNN for image categorization for secrecy. Because the offered technique makes use of GANs, there is no need to deal with encryption keys. In the Image Classification Experiment, they investigated the efficiency of the provided technique on assessing precision robustness to COAs [25]. In server-assisted collaborative PP model learning, coaches exchange model weights rather than gradients, assuming that they are more resistant to data leakage. The principal server trainer recovers the most recent weights and completes local training in the server-assisted network topology (SNT). The weights are then encoded using a key shared by the coaches and uploaded to the vector server. The best weight carriers are shared with others after all coaches repeat the procedure. The FNT version uses the same technique, except the weights are passed directly between coaches, either randomly or in a predetermined order. On the basis of ideas, the authors have theoretically proved a secure level of performance assurance and privacy. However, it is said that reversing the input is difficult, the authors consider the results effective based on computation and effectiveness as described in [26].

After an analytical trial of the face identification job within white square conditions, the approach generated good visual and numeric outcomes using road distance. However, there is a trade-off between detail and subtlety that has been presented. [27] Proposed FedOpt, a novel strategy to improve communication and privacy protection in Florida. A new compression technique was created in conjunction with the Scattered Compression Method (SCA) for efficient communication and combination with an extra algorithm to accomplish Symmetric encryption with differential privacy to prevent data leaking for FedOpt. To embrace the learning purpose, the suggested FedOpt improves communication efficiency while maintaining order privacy. FedOpt outperforms the most recent FL techniques, according to empirical evidence, especially when looking at the three separate evaluations [28].The recommended training to partition the distributor class with DNN scalable activation functions provides an additional level of protection from malicious attach on original data. Initial testing revealed that the methodology we suggest causes significant challenges in recovering primary data, even if metadata is recorded and underlying weights are tampered with by the adversaries. The trade-offs between data privacy and precision were also discussed. The hospital can set the time pause settings based on observations to achieve the desired balance of specificity and precision. As part of our ongoing research, we will investigate appropriate time intervals and expand on the concept by working on tasks such as object detection and segmentation, as shown. [29], the goal is to chain differential privacy with LRP at these level parameters to boost precision. The LRP is used to determine if a neuron's value is high or low. The related privacy budget is then used to pump Laplace noise into neurons based on their significance group. The larger the budget for Privacy, the greater the amount of noise produced. Furthermore, the loss function disrupted the goal value at each batch, ensuring that each point of data access is secured, resulting in a consistent paradigm of privacy preservation. The loss function is polynomial approximated and disrupted using the Laplace mechanism and the Maclaurin series is employed. The results of the solution's examination showed that even with a huge amount of noise, the accuracy achieved was high. [30]. Architectures must be chosen from the ground up in order to provide differentiated privacy assurances. Individual training points must be able to impact model modifications; hence it must be bound as narrowly as feasible to provide guarantees under the gold standard of differential privacy. The first to recognize that the activation function has been selected is crucial in reducing the Privacy-Preserving sensitivity of deep learning. The tempered sigmoid, a generic family of bounded activation functions, routinely beat unbounded activation functions like ReLU, both analytically and empirically. Using this approach, we were able to achieve new state-of-the-art accuracy on MNIST, Fashion-MNIST, and CIFAR10 without changing the fundamentals of the learning process or doing differential privacy analysis [30]. A Semi-Generative Adversarial Privacy-Preserving Network (PPSGAN) that selectively enhances noise to each image's class-independent landscapes to allow the processed image to keep its original class mark is suggested in differentially private input data. Our investigations on synthetic datasets anonymized with various approaches reveal that PPSGAN outperforms other traditional methods like as blurring, noise-adding, filtering, and GAN generation in terms of usefulness [31]. The algorithm for differentially private learning of DGM parameters was proposed. Our technique optimizes and adds noise that is specific to the attributes of the private input dataset and the DGM graph structure for the utility of inference queries over the DGM.This is the first time we've heard of a data-dependent privacy budget allocation technique for DGMs. On a number of criteria, we compare our methods to the usual data-independent strategy, and we find that our solution requires a privacy budget that is around three times lower to give the same or more benefit [32].

5. Mechanisms and outcome for comparison in privacy-preserving in deep learning (PPDL).

The methods employed are briefly described in this paragraph. Tables 1, Tables 2, And Tables 3 shows the most comprehensive and transparent Privacy Preserving for deep learning based on method used.

Table 1. Summarized of PPDL methods based on server-client PP model level.

Researchers	Year	Mechanisms	Outcomes
[18]	2020	• Mechanism of double decryption (BCP scheme) • Multi-party safe computing • Completely homomorphic multi-key encryption (MK-FHE)	• Honest-but-curious, all participants • Non-colluding cloud and approved core • Request for Face recognition
[19]	2019	• RG (Repeated Gompertz) for data disruption • A random projection (RP) matrix is used to project strong data into smaller spaces.	• Semi-honest Cloud service • The LSTM-CNN model
[24]	2019	• MPSC, additive encryption for secret-sharing, & edge Computing - Dual Edge Server Non-Colluding • Safe Channels of Communication	• Edge computing based in CNN function extraction, the model honest-but-curious are independent with non-colluding Edge Servers, and Transparent and honest third party
[25]	2019	• MORE scheme - Completely homomorphic encryption	• Use an independent deep learning computing services to process client data.
[16]	2018	• Generative Adversarial Networks and ciphertext-only attacks (COAs), including DNN-based attacks	• The scheme helps us not only to maintain high pixel-based classification accuracy but also to improve robustness against DNN attacks

Table 2. Summarized of PPDL methods based on server-assisted PP model level.

Researchers	Year	Mechanism	Outcomes
[20]	2011	• Symmetric Encryption. • Optional improvements: Privacy difference, • Stable channels for TLS/SSL	• Over the Five UCI, MNIST, and CIFAR-10/100 datasets, learn one deep network of numerous data owners. • The server is considered honest-but-curious
[21]	2020	• Privacy Cancellable Noise Differential & Network anonymization	• Two honest customers at least • A malicious server that can collide with up to two clients
[22]	2017	• Augmentation of Mix-up data	• Settings for the white & black box • DNN model by VLL - CIFAR datasets, Train deep model in a distributed information
[23]	2020	• Scattered Compression Algorithm. • FedOpt to enhance communication efficiency. • Privacy difference	• For both local users and the cloud server, FedOpt can mitigate security threats and honest-the-users. • In terms of precision, performance, and Privacy, both MNIST and CIFAR-10 datasets show that the proposed FedOpt is the best
[27]	2020	• Splitting Model, Breaking the DNN model, and Stepwise activation functions for activation	• Trade-off between accuracy and Privacy, regulated by the stepwise activation functions interval value.
[28]	2019	• selection algorithm	• The smooth improvement of inference accuracy by CNN Select while preserving SLA achievement in 88.5 %

Table 3. Summarized of PPDL methods based differentially private model level.

Researchers	Year	Mechanism	Outcomes
[29]	2021	• Parameters of the differentially private model, Laplace function suited to the importance of functionality, propagation of Layer-wise Importance, and approximation of polynomials - Taylor Expansion	• Release a deep network ad model that protects Privacy • Applicable in various deep networks using multiple activations, the features
[30]	2019	• Parameters of the model in differentially private that interrupt objective procedures & affine process • Laplace mechanism – difference privacy, propagation of Layer wise Importance, approximation of polynomials, and Macular in sequence	• Narrow down the gap in accuracy between DNN model privacy-preserving and non-privacy preserving
[31]	2021	• Privacy-preserving semi-generative adversarial network (PPSGAN)	• PPSGAN shows greater usefulness than other traditional methods, including blurring, noise-adding, filtering, and GAN generation.
[32]	2019	• DGMs model	• Optimizes and adds noise that is tailored to the private input dataset's properties & DGM graph structure.

6. Conclusion

Over the last few years, deep learning has progressed in a variety of application contexts. Deep learning raises privacy risks, according to some information security experts. The dangers are examined, and several privacy protection solutions, such as homographic cryptography and differential privacy, are evaluated. The paper also compares different protection mechanisms and evaluates the current performance of the solutions. The combination of the LSTM-CNN model and the RG+RP privacy method was shown to be the best compromise between privacy and accuracy. The authors of this work show in Tables 1, Tables 2, And Tables 3 how in a set of theories, a sharing model can accomplish a given amount of privacy and success guarantees. They believe that the input data can leak information regardless of the model weight. In this context, differential anonymity, leakage, and anonymous transmission have all been proposed as possible solutions. Mix-up Augmentation Methodology The model has a stronger capacity to generalize with disruption than VL, and the data is sufficient for identifying images. Because rounding was unneeded, the Extracted CNN privacy features utilizing random division proved that the method is consistent with every CNN architectures without sacrificing precision. The strategy is safe if the buyer is untrustworthy and makes genuine but strange demands, as is the situation here. The solution's accuracy was nearly equal to the non-coding variant on FHE encryption with MORE schemas MNIST and other relevant datasets. Despite this, the MORE cipher variant has been chastised for its security flaws. So, HE and deep learning are an intriguing combination since they allow data to be inferred fully anonymously, and they might also be employed for training to dramatically improve privacy in client-server contexts like ours. We've adapted encrypted deep learning to a whole new application; we assume the method in authors Tables 1, Tables 2, And Tables 3 trade of with application about accuracy and time.

References

[1] D. van, D. Sander, preprint arXiv **1706**, 06302 (2017).

[2] T. S. Ahmed, M. A. Sura, International Conference on Advanced Computer Science Applications and Technologies (ACSAT) **23**(3), 238 (2012).

[3] J. Bolibar, R. Antoine, G. Isabelle, G. Clovis, C. Thomas, S. Eric, The Cryosphere **14**(2), 565 (2020).

[4] M. Hao, Y. Hwang, K. Wang, IEEE Access **5**(6), 8869 (2017).

[5] D. Zhang, X. Chen, D. Wang, J. Shi, In: IEEE Third International Conference on Data Science in Cyberspace **70**(6), 652 (2018).

[7] S. Reza, S. Vitaly, In Indrajit Ray, Conference on Computer and Communications Security **72**, 1310 (2015).

[8] G. Ian, B. Yoshua, C. Aaron, MIT Press **105**, 12 (2016).

[9] Y. LeCun, P. Haffner, L. Bottou, Y. Bengio, Springer **1681**(19), 319 (1999).

[10] V. Sze, Y. H. Chen, T.J. Yang, Proceedings of the IEEE **105**(12), 2295 (2017).

[11] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, S. Liu, IEEE Trans. Ind. Inform **17**(8), 80 (2019).

[12] M. V. Valueva, N.N. Nagornov, P. A. Lyakhov, G. V. Valuev, N. I. Chervyakov, Mathematics and Computers in Simulation **3**, 83 (2020).

[13] S. Reza, S. Vitaly, In Proc. of ACM SIGSAC Conf. on Computer and Communications Security **21**,1310 (2015).

[14] S. Ioffe, C. Szegedy, arXiv preprint **1502**, 03167 (2015).

[15] E. Hesamifard, H. Takabi, M. Ghasemi, arXiv **1711**, 05189 (2017).

[16] W. Liu, F. Pan, X. A. Wang, Y. Cao, International Conference on Network-Based Information Systems **62**, 752 (2017).

[17] A. Senosi, G. Sibiya, IEEE AFRICON, Cape Town **93**, 849 (2017).

[18] V. Anamaria, I. N. Cosmin, P. Andrei, S. Constantin, M. I. Lucian, Computational and Mathematical Methods in Medicine **250**, 26 (2020).

[19] X. Ma, X. Chen, X. Zhang, Information Sciences **481**, 507 (2019).

[20] K. Chaudhuri, C. Monteleoni, A.D. Sarwate, J. Mach. Learn. Res **12**, 1069 (2011).

[21] B. Amine, D. Abdelouahid, C. Yacine, Elsevier B.V. **384**, 21 (2020).

[22] L. Ping, L. Jin, H. Zhengan, T. Li, C. Z. Gao, S. M. Yiu, K. Chen, Future Generation

Computer Systems **74**, 76 (2017).

[23] L. Lyu, X. He, Y. W. Law, M. Palaniswami, Proceedings of the ACM on Conference on Information and Knowledge Management **32**, 1219 (2020).

[24] L. Phong, T. T. Phuong, IEEE Transactions on Information Forensics **72**, 1809 (2019).

[25] V. Hartmann, R. West, arXiv preprint **1906**, 11993 (2019).

[26] H. Wang, Y. Fu, K. Xu, H. Mi, Y. Wang, In IEEE International Conference on Service-Oriented System Engineering (SOSE) **19**, 275 (2019).

[27] M. Asad, A. Moustafa, T. Ito, Appl. Sci **10**(2864), 3390 (2020).

[28] K. Huang, X. Liu, S. Fu, D. Guo, M. Xu, IEEE Transactions on Dependable and Secure Computing **70**, 55 (2019).

[29] A. Durrant, M. Markovic, D. Matthews, D. May, G. Leontidis, J. Enright, Glob. Food Secure **28**(100493), 40 (2021).

[30] C. Niţă, A. Vizitiu, A. Puiu, C. Suciu, L. M. Itu, In IEEE International Symposium on Medical Measurements and Applications (MeMeA) **20**, 1 (2019).

[31] Sirichotedumrong, Warit, K. Hitoshi, 28th European Signal Processing Conference (EUSIPCO) 2021.

[32] E. Chang, C. H. Yu, C. N. Chou, In IEEE Conference on Multimedia Information Processing and Retrieval (MIPR) **33**, 343 (2019).

Journal of Basrah Researches (Sciences) **48**(1), 10 (2022)
DOI: https://doi.org/10.56714/bjrs.48.1.2

دراسة: الحفاظ على الخصوصية في التعلم العميق القائم على التشفير المتماثل

سُـــرى محمود عبـــــدالله*

قسم علوم الحاسوب، الجــــامعة التكنولوجيــــه، بغداد، العراق

معلومات البحث

الاستلام	٢٥ شباط ٢٠٢٢
القبول	٢٦ اذار ٢٠٢٢
النشر	٣١ تموز ٢٠٢٢

الكلمات المفتاحية

التشفير المتماثل، التعلم العميق ، الحفاظ على الخصوصية.

Citation: S.M. Abdullah, J. Basrah Res. (Sci.) **48**(1), 10 (2022). DOI:https://doi.org/10.56714/bjrs.48.1.2

الملخص

عندما تنجح تقنيات التعلم العميق ، فإن كمية البيانات التي يمكن الوصول إليها للتدريب تنمو بسرعة, والخلفية الرئيسية هي جمع بيانات المستخدم على نطاق واسع في المؤسسات الضخمة. نظرًا لأن بيانات المستخدمين حساسة ، وطريقة الاحتفاظ بهذه المعلومات (الصور والتسجيلات الصوتية) إلى أجل غير مسمى يثير مخاوف بشأن الخصوصية. ترتبط شروط الخصوصية والسرية بتجنب مشاركة هذه المعلومات ، ولا يمكن الاستفادة من التعلم العميق على نطاق أوسع في كمية البيانات. هناك بعض التحديات في خوارزميات التعلم الآلي عند الحاجة إلى الوصول إلى البيانات لعملية التدريب. هناك العديد من التقنيات في التعلم العميق للحفاظ على الخصوصية تتطور لتعيين المشكلات ، لتشمل سرية الحساب متعدد الأطراف والتشفير المتماثل في مصطلح الشبكة العصبية. تتعامل هذه الدراسة مع تقنيات التعلم العميق المتعلقة بمسألة الخصوصية والمتعلقة بشكل أساسي ببيانات الإدخال وقدرة الاتجاهات المثيرة للاهتمام في عمليات التعلم هذه.

***Corresponding author email :** Sura.M.Abdullah@uotechnology.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://bjrs.uobasrah.edu.iq