International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol.10, No.2, 2023, pp.153-163.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Survey: Homomorphic Encryption-based Deep Learning that Preserves Privacy

Rasha Hani Salman [a*], Esraa Saleh Alomari [b]

[a] Presidency University, Wasit University, Wasit, Iraq. E-mail: Rsalman@uowasit.edu.iq, Orcid: https://orcid.org/0009-0009-9615-2079*
[b] College of Education for Pure Sciences, Computer Department Wasit University, Wasit –Iraq.

Abstract

When deep learning methods are effective, the volume of information accessible for training is expanding quickly, with large-scale user data collection in businesses taking the lead. Due to the sensitive nature of user data and the way. Data collection creates privacy concerns because of the potential for this material (images and audio recordings) to be preserved forever. The concepts of privacy and secrecy pertain to the avoidance of sharing this data, and a higher volume of data is required for deep learning to be achieved. When data must be accessed for training, machine-learning algorithms face certain difficulties. Several privacy-preserving deep learning solutions, such as multi-lateral computation secrecy and symmetric encryption within neural networks, have been developed to address these concerns.

Keywords: Deep Learning, Privacy Preserving and Homomorphic Encryption.

DOI:10.71086/IAJSE/V10I2/IAJSE1019
Received: 27 March 2023/Revised: 28 April 2023/Accepted: 22 May 2023/Published: 29 June 2023

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 pictures, 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 The process of classifying documents into one or more predetermined categories according to their contents is known as categorization [2]. Given that privacy problems may be effectively addressed with the same training data, deep learning is valuable. The practice of gathering data (voice, video, and picture) in a central format has put millions of people's privacy at risk. Users have no control over the data, including the ability to remove it or change what is learned from it; corporations retain the information indefinitely. Second, inadvertently taken images and audio recordings of faces, license plates, computer screens, other people's voices, and background noise frequently contain private and sensitive information. [3], among other things. Lastly, the process of classifying documents into one or more predetermined categories according to their contents is known as categorization [2]. Given that privacy problems may be effectively addressed with the same training data, deep learning is valuable. The practice of gathering data (voice, video, and picture) in a central format has put millions of people's privacy at risk. Users have no control over the data, including the ability to remove it or change what is learned from it; corporations retain the information indefinitely. Second, inadvertently taken images and audio recordings of faces, license plates, computer screens, other people's voices, and background noise frequently contain private and sensitive information. [3], among other things. Lastly, they were worried that someone else would access their data and violate their privacy. Researchers paired deep learning training methods with privacy-protected data to reassure customers about their data security and privacy. Several techniques can be applied to use the neural network in a private setting. The swift expansion of the multimedia and communication domains has led to concerns regarding the safety of digital photos transferred via stored or open networks. [5][6]. The study's core claim is that data privacy should be protected; generally, the data is encrypted and only accessible to those who are authorized to view it. Nevertheless, the problem statement is that homographic encryption solutions only support addition and multiplication, which presents a challenge when we need to do mathematical operations on this encrypted data, such as classifying it using artificial intelligence algorithms. Artificial intelligence algorithms need more than addition and multiplication operations to yield trustworthy classification results. The primary goal is to introduce deep learning methods that have been applied recently to do a high-precision classification of encrypted data. Because of this, the contribution of these papers summarizes the impacts of the solutions and establishes the deep learning challenges. Additionally, it provides a broad range of options, including more privacy-preserving deep learning techniques than many recent solution articles. Ultimately, ascertain the issues surrounding deep learning when applied to encrypted data. All approaches that solve issues and difficulties with privacy preservation using deep learning and privacy preservation procedures examined and assessed in this survey.

Deep Learning in the Context of AI

The fundamental job of the deep learning algorithm is to take complex features out of high-dimensional data and use that information to build a model that connects input and output. Deep learning architectures frequently use multi-layered networks to abstract additional qualities that are computed as nonlinear functions of low-level variables. Deep learning architectures most frequently use layered neural networks. [3]. A variety of layers represent the structure of Deep Learning.

Background of Convolutional Neural Networks (CNN)

Multilayer perceptron does not work well with many types of data, especially picture data. Since they are made to operate with vectors as input data, we must first convert photos to vectors to use them; otherwise, we will lose any spatial information, such as forms, that may be present in the images. Learning was predicated on the extraction of variables of interest, or features before deep learning for computer vision was introduced. However, these image-processing techniques demand a high level of skill [7][8]. CNN frequently uses and defines a convolution layer, whose job is to learn the properties taken from the dataset to classify pictures. The CNN model's N × N dimension allows for the convolution of a dot product observed between neighborhood values. Thus, the convolutional layer is limited to addition and multiplication operations. This layer does not need to be modified because symmetric encrypted "HE" data may be utilized with it [9], as the above figure illustrates:

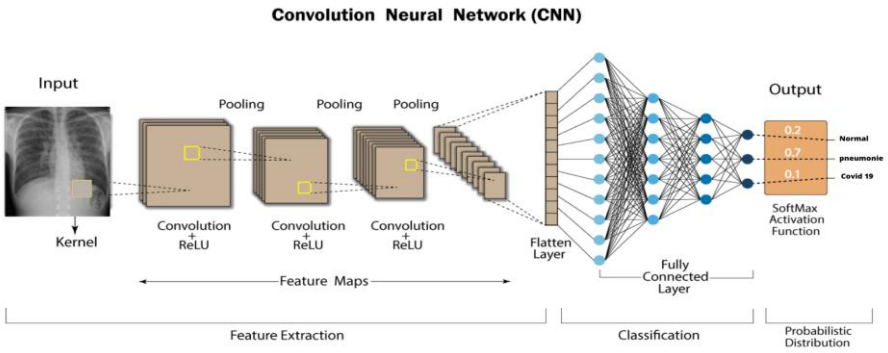


Fig. 1: Convolution Neural Network (CNN)

Neural Network Activation Layer

Deep learning neural networks include several layers, which makes the back propagation algorithm challenging to use. Calculating the parameter. For this reason, the sigmoid function has been substituted with the corrected linear function. Although this method is not differentiable in 0, this is not a serious issue because there is typically no chance that an entry will equal 0. The activation functions are explained in Figure (2) [10]. It determined by this whether the data triggered at zero or one. The activation layer is a nonlinear feature that uses a mathematical procedure to apply the output of the convolution layer. When utilized to measure homomorphic encrypted (HE) data, these nonlinear tasks become far more challenging. Therefore, we will need to devise. An alternative element that just requires addition and multiplication [5].

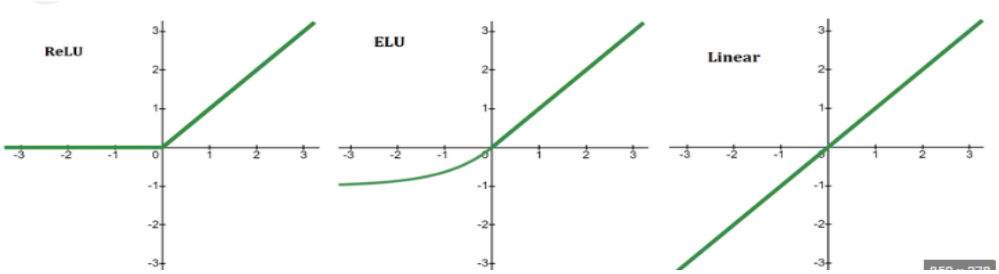


Fig. 2: Neural Network Activation Function

Layer of Pooling

It is a sampling layer whose objective is to retain the smallest possible amount of data. There are many different types of pooling, such as mean pooling, maximum and average pooling, and others. Since we won't be using, HE's max-pooling feature in this instance, we won't verify the encrypted data's overall value. We will employ the 'average pooling' solution for 'HE.' Since the average in pooling establishes the value amount, there is only one more step that needs to be carried out on the data encrypted with 'HE' [11]. In Figure (3), the principle pooling layer is displayed.

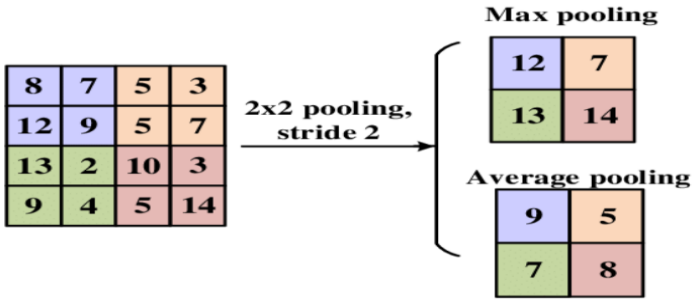


Fig. 3: Pooling Layer of Polling

Layer of Fully Connected

The Fully-Connected layers are concerned with feed forward neural networks. The last tiers of the network are called the Fully Connected Layers. The input to the fully connected layer is the flattened output from the last

pooling or convolutional layer, which is fed into the layer after it has been fully linked [4]. This layer is known as the Fully coupled Layer because every neuron in it is coupled to every other neuron in the layer above. There is only one dot product function in this layer, which consists of addition and multiplication operations. It can therefore use it to decode HE data [12], as seen in Figure (4):

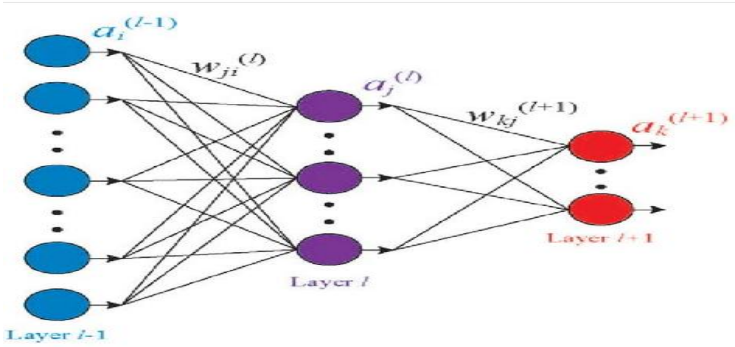


Fig. 4: Layer of Fully Connected

Layer of Dropout

In order to reduce overfitting, the Dropout layer randomly sets the input units to 0 at a rate frequency at each step of the training process. It's important to remember that, as shown in Figure (5), the Dropout layer only operates when the training parameter is set to true, indicating that no data are dropped during inference. when utilizing a model. It is a layer designed to address the over-fitting issue. For several types of data, our machine learning model frequently produces flawless classification results during training, which suggests bias in the training set [13].

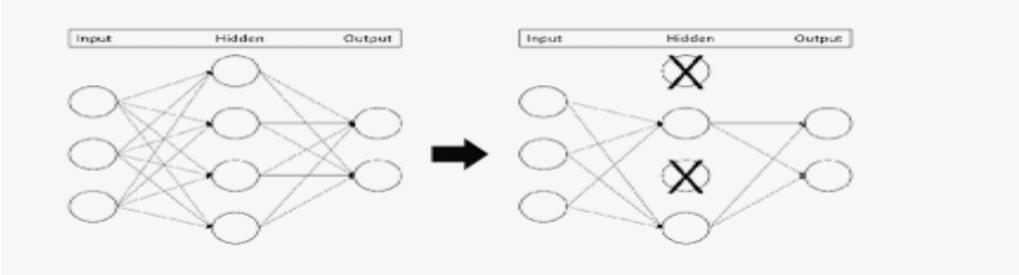


Fig. 5: Dropout Layer

HE: Homomorphic Encryption

Through the use of homomorphic encryption, mathematical operations on data can now be carried out on cipher text rather than the original data. An encrypted form of the input data is known as the cipher text (sometimes termed plain text). After being operated on, it is decrypted to produce the required output. Various instruments are utilized to safeguard privacy. Homomorphic encryption and differential privacy strategies rank highest and are typically associated with polynomial approximation [14]. A mapping function from a domain set input element to an algebraic set range output element is known as a homomorphism. HE encryption uses a unique kind of calculation on cipher tests to provide encrypted results. Standard encryption approaches prevent operations on encrypted data by limiting the cloud service provider. Because of this, users of cloud services don't have to worry about the security or privacy of their data. This necessitates the creation of an algorithm, as suggested by Rivest, Adleman, and Dortouzous in 1978, that can execute computations on encrypted data. The name "Privacy Homomorphism" was given to this idea. Based on the number of iterations and computational operations carried out, HE can be divided into three categories [15]. With partially homomorphic encryption (PHE), there is just one encrypted data process possible: addition or multiplication.

More procedures are provided by somewhat homomorphic encryption (SWHE), 38 addition and multiplication, but only a few operations. With Fully Homomorphic Encryption (FHE), several addition and multiplication operations are possible without limiting the functions. Can describe the kind of HF shown in Figure (6).

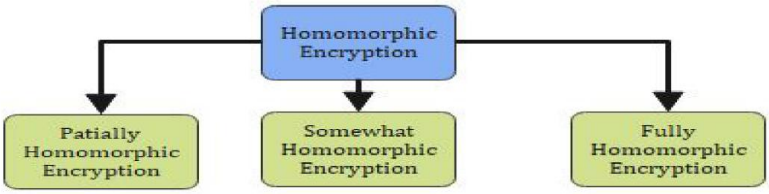


Fig. 6: Types of Homomorphic Cryptography

Thus, the HE is the encryption algorithm E over an operation "∘" & as illustrated in equation (1) and figure (7), where M stands for the messages' space: $(m1) \circ (m2) = (m1 \circ m2), \forall\, m1, m2 \in M$

This approach has four stages for the encryption in HE [16].

Key Generation (Key_Gen): Security parameters are generated at this step.

A pair of secret and public keys are generated in an asymmetric type, as opposed to a single key in an asymmetric type.

The encryption algorithm (Enc): uses the encryption key to encrypt the plaintext input message, m ϵ M. $c = (m)$, where c ∈ C, C is the cypher text space, generates the cipher text.

Decryption Algorithm (Dec): Using the decryption key $((c) = m)$, the original message is recovered at this step by decrypting cipher text c.

The Assessment Algorithm (Eval): In this phase, the cipher texts $(c1, c2)$ are evaluated, i.e., $\{(c1, c2)\} = Eval\ \{(m1, m2)\}$, without disclosing the messages $(m1, m2)$, i.e. $\{(c1, c2)\} = (m1, m2)$.

Secure Multi-Party Computation: (SMPC)

HE is an element of secure multiparty computing (MPC / SMPC), a cryptographic technique for disseminating a computation across multiple parties while making sure that no participant has access to another's data. By employing safe multiparty computation protocols, information scientists and analysts can quietly, discreetly, and compliantly compute on various datasets without ever moving or exposing them. This is a novel perspective that highlights the interconnectedness of the participants. Partitioning data is possible, and only a small portion of each actor's data with other actors, enabling computations and interaction without requiring the original data to be recreated. It can therefore be combined until all participants have finished it and are notified of the production's outcomes. Unlike HE, parties in a protected MPC measure a function on their inputs jointly using a protocol as opposed to a single entity. Throughout the procedure, the parties' secrets must remain undiscovered. The parties in a secure MPC have high communication costs but low calculation costs. Servers have low transmission costs and high processing costs in comparison to MPC. For use in training, it is far too general [17].

Distinctive Privacy

One technique used in higher education is differential privacy, which enables researchers and database analysts to draw conclusions from databases holding individuals' personal data without revealing that knowledge about specific individuals. Decision trees, support vector machines, logistic regressions with differential privacy, and other machine learning techniques have all been the subject of multiple investigations; deals in instances were reached without disclosing any data. The input data, mimic learning, and differential private model parameters make up the three parts of this algorithm [18].

Correlated Assignments

As a consequence of deep learning's ongoing advancements in a variety of domains, such as natural language processing, vision, recommendation systems, and so on, Deep Neural Networks (DNNs) have been used in production systems. The main causes of these developments are the abundance of large datasets and powerful computers. We compare in several ways in this study, including cooperation, non-collaboration, and multi-parties [19]:

Cooperation

The three issues brought up by previous FHE-based systems like CryptoNets are addressed by the researchers' new privacy-preserving learning architecture, CryptoNets. Globally Encrypted, Locally Unencrypted Deep Neural

Network (GELUNet) is the moniker given to it. The intrinsic technique divides each neuron into linear and nonlinear parts, which are then performed separately on non-colluding participants.

For linear computations, the homomorphic cryptosystem Paillier is employed. It is far more efficient than CryptoNets' FHE and provides sufficient security confidence to keep data encrypted globally. Thus, the first issue has been settled. Without the original method of dividing the two components, it would be challenging to utilize Paillier because it does not support nonlinear polynomials. In order to maintain the current accuracy, the cryptographic incomputable signals are handled in a locally unencrypted but privacy protected manner, which solves issues two and three. Using the random masking technique, privacy components were added to back propagation algorithms for a loss-free model with low computing and communication costs [20]. The first secure key architecture for scaling DL-based analysis of data collected by dispersed clients, called Deep Secure, is described in this paper. Using state-of-the-art architectures on sensitive data is made possible by deep secure, all without compromising security for precision. We provide a sincere but inquisitive opponent model that is in line with the literature for a generic instance where both DL parameters and input data must always be kept secret. Unlike earlier work based on homomorphic encryption, Deep Secure suggests utilizing Yao's Garbled Circuit (GC) protocol to secure DL execution. That is, this new study is based on homomorphic encryption. [5], neither privacy nor utility is compromised by the techniques we use. Our architecture is the best choice for arriving data servers from clients with the least amount of delay when the sample size is less than 2600 samples obtained by each dispersed client. Offer a collection of low-overhead preprocessing techniques that further cut down on the GC overall runtime in the context of deep learning. [21].

Lack of Cooperation

This study suggests two approaches for putting a multikey learning system into practice. Both methods make it possible for numerous data owners with different datasets to safely learn neural network architecture in the cloud. Data owners employ multi-key fully homomorphic encryption (MK-FHE) and a hybrid framework that combines totally homomorphic encryption (FHE) with the dual decryption technique Bresson, Catalano, and Point cheval scheme (BCP) before uploading sensitive data to a cloud server [18]. RG - RP is a privacy-preserving technique that employs randomization and perturbation in two stages. The Repeated Gompertz (RG) nonlinear perturbation is used to decrease the Maximum Posteriori (MAP) estimate derived from training data. Second, high-dimensional data is transformed into low-dimensional data using a row orthogonal projection matrix. Independent Component Analysis (ICA) is used to achieve these goals of maintaining precision, reducing gearbox energy consumption, and boosting assault resistance. Based on the transformed data from the participants, the cloud creates a deep learning model. The evaluation findings show that the recommended LSTM in CNN model along with the RGRP privacy strategy gives you an outstanding balance of privacy and precision. The LSTM-CNN performs better than other comparable models in terms of efficiency, both with and without confidentiality; however, the privacy version of the LSTM-CNN performs slightly worse [22]. This study provided a novel lightweight framework for privacy-preserving CNN extraction features in the setting of mobile sensing. Applying the encryption technique based on secret sharing and moving computationally intensive operations to edge servers may allow them to significantly reduce the load on mobile sensors and end users. Furthermore, Is not necessary communication between the server and the end user. Consequently, they have created a collection of crypto building blocks that do not require the processing power of approaches such as homomorphic cryptography or broken circuits. Unlike previous homomorphic encryption-based systems, the CNN attributes privacy protection and extraction approach does not involve any computations for favored known CNN layers. Thus, hypotheses can be tested through empirical trials [23].

Many parties

In this work, the data training problem was solved using the Edge Computing paradigm. issue by minimizing or completely removing the transfer of user data to the cloud and moving processing to the location where the data actually stored at the user's discretion. By doing this, worries about the data breach and manipulation may be allayed since the data isn't being collected at scale in the first place.

There are fewer reasons for attacks because to obtain data for millions of customers, the criminal needs to obtain access to millions of devices rather than just one cloud service. This concept was put into practice in this paper by: (i) creating a personal machine learning approach where the majority of data stays on controlled devices; (ii) applying this technique to two learning tasks and obtaining the results, i.e., supervised (accelerometer traces activity recognition) and unsupervised (text documents modeling topic); and (iii) They examine the robustness of our approach against antagonistic attacks, as well as the viability of implementing such approaches on a realis: a model of Raspberry Pi 3 [24].

Each server has a neural network component that is divided by the system administrator and includes weights and biases matrices. In order to get a result, a client splits their data into two secret postings, which are sent to dual several non-complicit servers. The activation function layers are anticipated to be continuous, small-degree polynomials due to the symmetric coding. The model runs continually on servers, producing forecasts that are encrypted and that the client decodes to get the final prediction. Theoretical research conducted by the authors indicates that the answer specifically satisfies the model and the data. According to the authors' investigation, their method was more efficient than the competitors in terms of connections and computing complexity. They provide a brand-new image processing method built on the foundation of generative adversarial systems (GAS). By applying images to DNN without requiring visual input, the suggested technique strengthens its defenses against Crypto-Text Only Attacks (COAs), especially those that rely on DNN. This study demonstrates that the suggested transformation technique may maintain visual data on.

Both regular photographs and optically protected images are directly applied to DNN for secrecy-preserving image classification. Dealing with encryption keys is not necessary because the proposed technique uses GANs. They examined the effectiveness of the suggested method for determining the accuracy robust to COAs in the Image Classification Experiment [25]. Coaches exchange models in server-assisted collaborative PP model learning. the assumption being that weights are more resilient to data leaking than gradients. In the server-assisted network topology (SNT), the principal server trainer recovers the most current weights and finishes local training. Subsequently, the weights are uploaded to the vector server and encoded using a common key among the coaches. Once all coaches have completed the process, the top weight bearers are distributed to other coaches. The FNT version employs the identical methodology, with the exception that coaches distribute the weights directly to one another either in a preset order or at random. The writers have theoretically demonstrated a secure degree of privacy and performance assurance based on concepts.

Despite the fact that it is believed to be challenging to reverse the input, the authors believe the findings are effective based on calculation and effectiveness as stated in [26]. Following an analytical trial of the face identification task in white square settings, the method produced good numerical and visual results utilizing road distance. There is, nevertheless, a trade-off between the offered subtlety and detail. [27] suggested FedOpt, a cutting-edge tactic to enhance privacy protection and communication in Florida in order to facilitate effective communication, a new compression technique was developed in conjunction with the Scattered Compression Method (SCA) and combined with an additional algorithm to.

To stop FedOpt data leaks, implement symmetric encryption with differential privacy. To accommodate the educational goal, the proposed FedOpt enhances order privacy and communication effectiveness. Empirical evidence suggests that FedOpt performs better than the most recent FL approaches, particularly when examining the three different evaluations [28]. An extra degree of security against malevolent attach on the original data is offered by the suggested training to divide the distributor class using DNN scalable activation functions. Our proposed methodology presents considerable difficulties in retrieving primary data, even when attackers capture metadata and manipulate underlying weights, according to preliminary testing. There was also discussion of the trade-offs between precision and data privacy.

The hospital can attain the ideal balance between specificity and precision by adjusting the time pause settings in response to observations. We will continue to examine suitable time intervals and develop the idea by focusing on tasks like segmentation and object detection, as demonstrated. To increase precision, [29] proposes chaining differential privacy with LRP at these level parameters. To ascertain if a neuron's value is high or low, one uses the LRP. Next, the associated privacy budget is utilized to pump Neurons subjected to Laplace noise according to their significance group. The more money allocated to privacy; the more noise is generated. In addition, the loss function altered the objective value at every batch, guaranteeing data security at every point of access and producing a dependable paradigm for privacy protection. The Laplace mechanism is used to approximate and disrupt the loss function polynomially, and the Maclaurin series is utilized. The analysis of the solution's outcomes revealed that even with a significant quantity of noise, the accuracy attained was elevated. [30]. Selecting architectures from the ground up is necessary to guarantee differentiated privacy.

Since individual training points must have the ability to affect model alterations, the gold standard of differential privacy guarantees must be as strictly defined as practical. Reduce the Privacy Preserving sensitivity of deep learning by being the first to realize that the activation function has been chosen. Analytically and empirically, the tempered sigmoid, a general family of bounded activation functions, consistently outperformed unbounded activation functions such as ReLU. We achieved new state-of-the-art accuracy on MNIST, Fashion-MNIST, and CIFAR10 using this method without altering the foundation of the learning process or performing differential

privacy. In differentially private input data, a Semi-Generative Adversarial Privacy-Preserving Network (PPSGAN) is proposed that selectively boosts noise to each image's class-independent landscapes so that the processed image can maintain its original class mark. According to our research on synthetic datasets anonymized using a variety of techniques, PPSGAN performs more usefully than other conventional techniques including blurring, noise-adding, filtering, and GAN generation [31]. It was suggested to use the technique for different private learning of DGM parameters. For the purpose of enhancing the usefulness of inference queries over the DGM, our method adds and optimizes noise that is unique to the characteristics of the private input dataset and the DGM graph structure.

We have never heard of a budget allocation for data-dependent privacy before. Method for DGMs. Our approach necessitates a privacy expenditure approximately three times lower to get the same or greater advantage when compared to the standard data-independent strategy on several criteria [32].

Deep Learning (PPDL) Mechanisms and Results for Privacy-preserving Comparison

This paragraph provides a quick description of the techniques used. Tables 1 through 3 illustrate the most thorough and open privacy preservation for deep learning, depending on the technique employed.

Table 1: PPDL Methods Summarized According to 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: PPDL Approaches Summarized According to 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.	• For both local users and the cloud server, FedOpt can mitigate security threats and honest-the-users.

		• Privacy difference	• 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: PPDL Approaches based on Differentially Private Model Levels Summarized

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.

Concluding Remarks

Deep learning has advanced in several application contexts over the past few years. Certain information security specialists claim that deep learning poses privacy threats. A number of privacy protection strategies, including differential privacy and homogeneous cryptography, are assessed in addition to the risks being looked at. The study assesses the effectiveness of the remedies as of right now and contrasts various defense systems. The optimal trade-off between accuracy and privacy was found to be achieved by combining the RG+RP privacy technique with the LSTMCN model. The authors of this work demonstrate in Tables 1 through 3 how a sharing model can provide a specific level of privacy and success guarantees within a set of theories. They think that regardless of the model weight, information can still be leaked from the input data. Differential anonymity, leaking, and anonymous transmission have all been suggested as potential remedies in this situation. Inaccurate Supplementation Techniques Compared to VL, the model is more able to generalize with disruption, and there is enough data to detect images. The Extracted CNN privacy features using random division did not require rounding. demonstrated that the technique maintains precision while being compatible with all CNN architectures. If the buyer is dishonest and makes sincere but peculiar demands, like in this case, the strategy is safe. The accuracy of the solution was almost as good as the non-coding option on FHE encryption using MNIST and other pertinent datasets and MORE schemas. In spite of this, the MORE cipher variation has received criticism due to security vulnerabilities. Thus, HE and deep learning together are an interesting combo since they enable completely anonymous data inference. They may also be used for training purposes to significantly enhance privacy in client-server environments such as ours. We've modified encrypted deep learning for a completely new use case; we presume that the approach in authors' tables 1, 2, and 3 trades off accuracy and time.

References

van der Hoog, S. (2017). Deep learning in (and of) agent-based models: A prospectus. *Journal of Basrah Researches (Sciences), 48*(1), 1-19.

Sadiq, A.T., & Abdullah, S.M. (2012). Hybrid intelligent technique for text categorization. *In IEEE International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 238-245.

Bolibar, J., Rabatel, A., Gouttevin, I., Galiez, C., Condom, T., & Sauquet, E. (2020). Deep learning applied to glacier evolution modelling. *The Cryosphere*, *14*(2), 565-584.

Chen, M., Hao, Y., Hwang, K., Wang, L., & Wang, L. (2017). Disease prediction by machine learning over big data from healthcare communities. *IEEE Access*, *5*, 8869-8879.

Zhang, D., Chen, X., Wang, D., & Shi, J. (2018). A survey on collaborative deep learning and privacy-preserving. *In IEEE Third International Conference on Data Science in Cyberspace (DSC)*, 652-658.

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. *In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 1310-1321.

Hao, M., Li, H., Luo, X., Xu, G., Yang, H., & Liu, S. (2019). Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE Transactions on Industrial Informatics*, *16*(10), 6532-6542.

Sze, V., Chen, Y.H., Yang, T.J., & Emer, J.S. (2017). Efficient processing of deep neural networks: A tutorial and survey. *Proceedings of the IEEE*, *105*(12), 2295-2329.

Osawaru, E.R., & AH, R.A. (2014). A highlight of security challenges in big data. *Int J Inform Syst Eng*, *2*(1), 2289-2265.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press. http://www.deeplearningbook.org.

Forsyth, D.A., Mundy, J.L., di Gesu, V., & Cipolla, R. (Eds.). (2003). *Shape, contour and grouping in computer vision*, 1681, 319–345.Springer.

Valueva, M.V., Nagornov, N.N., Lyakhov, P.A., Valuev, G.V., & Chervyakov, N.I. (2020). Application of the residue number system to reduce hardware costs of the convolutional neural network implementation. *Mathematics and computers in simulation*, *177*, 232-243.

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 1310-1321.

Ioffe, S., & Szegedy, C. (2015). Batch normalization: Accelerating deep network training by reducing internal covariate shift. *In International conference on machine learning*, 448-456.

Hesamifard, E., Takabi, H., & Ghasemi, M. (2016, December). Cryptodl: towards deep learning over encrypted data. *In Annual Computer Security Applications Conference (ACSAC 2016), Los Angeles, California, USA* (Vol. 11, pp. 1-2).

Liu, W., Pan, F., Wang, X.A., Cao, Y., & Tang, D. (2019). Privacy-preserving all convolutional net based on homomorphic encryption. *In Advances in Network-Based Information Systems: The 21st International Conference on Network-Based Information Systems (NBiS-2018)*, 752-762. Springer International Publishing.

Senosi, A., & Sibiya, G. (2017). Classification and evaluation of privacy preserving data mining: a review. *IEEE AFRICON*, 849-855.

Vizitiu, A., Niţă, C.I., Puiu, A., Suciu, C., & Itu, L.M. (2020). Applying deep neural networks over homomorphic encrypted medical data. *Computational and mathematical methods in medicine*, *2020*.

Ma, X., Chen, X., & Zhang, X. (2019). Non-interactive privacy-preserving neural network prediction. *Information Sciences*, *481*, 507-519.

Chaudhuri, K., Monteleoni, C., & Sarwate, A.D. (2011). Differentially private empirical risk minimization. *Journal of Machine Learning Research*, *12*(3), 1069–1109.

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

Li, P., Li, J., Huang, Z., Li, T., Gao, C.Z., Yiu, S.M., & Chen, K. (2017). Multi-key privacy-preserving deep learning in cloud computing. *Future Generation Computer Systems*, *74*, 76-85.

Lyu, L., He, X., Law, Y.W., & Palaniswami, M. (2017). Privacy-preserving collaborative deep learning with application to human activity recognition. *In Proceedings of the ACM on Conference on Information and Knowledge Management*, 1219-1228.

Phuong, T.T. (2019). Privacy-preserving deep learning via weight transmission. *IEEE Transactions on Information Forensics and Security*, *14*(11), 3003-3015.

Zerka, F., Urovi, V., Bottari, F., Leijenaar, R. T. H., Walsh, S., Gabrani-Juma, H., Gueuning, M., Vaidyanathan, A., Vos, W., Occhipinti, M., Woodruff, H. C., Dumontier, M., & Lambin, P. (2021). Privacy preserving distributed learning classifiers – Sequential learning with small sets of data. *Computers in Biology and Medicine, 136,* 104716. https://doi.org/10.1016/j.compbiomed.2021.104716

Fu, Y., Wang, H., Xu, K., Mi, H., & Wang, Y. (2019). Mixup based privacy preserving mixed collaboration learning. *In IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 275-2755.

Asad, M., Moustafa, A., & Ito, T. (2020). FedOpt: Towards communication efficiency and privacy preservation in federated learning. *Applied Sciences*, *10*(8), 1-17.

Huang, K., Liu, X., Fu, S., Guo, D., & Xu, M. (2019). A lightweight privacy-preserving CNN feature extraction framework for mobile sensing. *IEEE Transactions on Dependable and Secure Computing*, *18*(3), 1441-1455.

Durrant, A., Markovic, M., Matthews, D., May, D., Leontidis, G., & Enright, J. (2021). How might technology rise to the challenge of data sharing in agri-food? *Global Food Security*, *28*, 1-30.

Vizitiu, A., Niţă, C.I., Puiu, A., Suciu, C., & Itu, L.M. (2019). Towards privacy-preserving deep learning based medical imaging applications. *In IEEE international symposium on medical measurements and applications (MeMeA)*, 1-6.

Sirichotedumrong, W., & Kiya, H. (2021). A gan-based image transformation scheme for privacy-preserving deep neural networks. *In IEEE 28th European Signal Processing Conference (EUSIPCO)*, 745-749.

Yu, C.H., Chou, C.N., & Chang, E. (2019). Distributed layer-partitioned training for privacy-preserved deep learning. *In IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, 343-346.