Al-Qadisiyah Journal of Pure Science

Volume 27 | Number 1 Article 21

4-7-2022

A Comparative Study Of Combining Deep Learning And Homomorphic Encryption Techniques

Emad M. Alsaedi
Computer Sciences Department, University of Technology, Baghdad,Iraq,
cs.19.71@grad.uotechnology.edu.iq

Alaa Kadhim Farhan
Computer Sciences Department, University of Technology, Baghdad, 10066, Iraq,
alaa.k.farhan@uotechnology.edu.iq

Recommended Citation

Alsaedi, Emad M. and Farhan, Alaa Kadhim (2022) "A Comparative Study Of Combining Deep Learning And Homomorphic Encryption Techniques," *Al-Qadisiyah Journal of Pure Science*: Vol. 27: No. 1, Article 21.
DOI: 10.29350/qjps.2022.27.1.1452
Available at: https://qjps.researchcommons.org/home/vol27/iss1/21

Al-Qadisiyah Journal of Pure Science
ISSN(Printed): 1997-2490 ISSN(Online): 2411-3514
DOI: /10.29350/jops.
http://qu.edu.iq/journalsc/index.php/JOPS

A comparative study of combining deep learning and homomorphic encryption techniques

Authors Names
a.Emad M. Alsaedi
b.Alaa kadhim Farhan

Article History
Received on: 26/9/2021
Revised on: 25/12/2021
Accepted on: 20/1/2022
Keywords:
CNN
Deep Learning
Homomorphic encryption
Privacy preserving
DOI:https://doi.org/10.29350/jobs. 2022.27. 1.1452

ABSTRACT

Deep learning simulation necessitates considerable internal computational resources and fast training for large amounts of data. The cloud has been delivering software to help with this transition in recent years, posing additional security risks to data breaches. Modern encryption schemes maintain personal secrecy and are the best method for protecting data stored on a server and data sent from an unauthorized third party. However, when data must be stored or analyzed, decryption is needed, and homomorphic encryption was the first symptom of data security issues found with Strong Encryption. It enables an untrustworthy cloud resource to process encrypted data without revealing sensitive information. This paper looks at the fundamental principles of homomorphic encryption, their forms, and integrating them with deep learning. Researchers are particularly interested in privacy-preserving Homomorphic encryption schemes for neural networks. Finally, present options, open problems, threats, prospects, and new research paths are identified across networks.

1. Introduction

Deep learning (DL) is one of the most commonly used ways of analyzing personal data and is at the forefront of many digital services and applications. Deep learning has been such a competitive and computationally efficient paradigm that it is now a part of daily life. However, it is hard to imagine our lives without these services., there is an increasing need for privacy-preserving machine learning(9). There are several approaches to balancing confidentiality with computing performance to ensure privacy for deep learning inference. Data security is an essential requirement in our time. As a result of the rapid development of unsecured computer networks, personal data should be protected from unauthorized persons.

Modern block ciphers consist of rounds of permutation and substitution processes, thereby strongly exhibiting Shannon's confusion and diffusion properties. The two extensively deliberated

[a1]Computer Sciences Department, University of Technology, Baghdad, Iraq: Email:cs.19.71@grad.uotechnology.edu.iq

[b] Computer Sciences Department, University of Technology, Baghdad, 10066, Iraq, Email:Alaa.K.Farhan@uotechnology.edu.iq

architectures used to build the block ciphers are the famous Fiestal network, and the other is Substitution-Permutation (S-P)(1). In November 2009, AES algorithm exposure was attacked eight rounds type attack (distinguish attack). However, the modern algorithm worked on a principle of confusion and diffusion. Confusion worked substitution to generate S-BOX, e.g., AES and diffusion worked permutation to generate initial permutation, e.g., DES, because principle confusion used AES algorithm has resistance against this type of attack(10). In 1978, RSA was suggested by Ron, Rivest, Adi, Shamir, and Leonard Adleman. It is among the finest known public critical cryptosystems for key interchange, digital signature, or information cryptography.

RSA uses not fixed size cryptography block, and the size of the key is not fixed. RSA asymmetric encryption algorithm depends on number theory. It is a block cipher system(6). Lightweight security cryptography contains more than one proposals algorithm like PRESENT(a lightweight block cipher with a block size of 64 bits and a key size of 80 or 128 bits), CLEFIA (Its name is derived from the French word clef, meaning "key"), KATAN(A Family of Small and Efficient Hardware-Oriented Block Ciphers), HEIGHT(high security and lightweight), SIMON-SPECK, Fantomas, KLEIN (family of block ciphers)and many other algorithms. Lightweight security goals to gain sufficient security levels with an optimum resource use(18). one of the other technology that protects data and maintains operations such as addition and multiplication on the ciphertext is homomorphic encryption. The encrypted data can compute arbitrary or group functions without decoding them beforehand. However, only the very last result needs to be decrypted.

Regarding privacy, this is very interesting(27). Many homomorphic encryption systems exist. Each one has its own set of advantages and disadvantages. For example, with partial homomorphic encryption(PHE), one can't add and multiply simultaneously for security reasons. Somewhat Homomorphic (SHE) Encryption technique can add and multiply the underlying message while keeping the encrypted data; however, the number of these operations is restricted because of the increasing noise. It's possible to employ any function using fully homomorphic encryption (FHE)(2). A homomorphic approach can evaluate the linear functions that makeup CNNs.

On the other hand, CNN has layers like the activation layer that rely on nonlinear functions like ReLU and Sigmoid. There is no homomorphic method to apply these functions. Hence addition and multiplication are the only representations available(17). Many attempts have been made to employ deep convolutional neural networks (CNNs) to gain insights from encrypted data because they are the machine learning method of choice for many applications. However, when reporting high-level

implementations, researchers typically neglect to look at the trade-offs involved in implementing CNN primitive operators like convolution, nonlinear activation, and pooling in the FHE framework(11). This research focuses on homomorphic encryption (HE), which allows for deep learning while maintaining privacy for the learner. The several types of homomorphic encryption and how they work with CNN's deep learning method are described.

2. Related work

In this paragraph, some articles will be reviewed that have used the original architecture of deep learning technology and Homomorphic encryption.

- HE algorithms used
- How to implement in deep learning
- Time
- Accuracy
- Noise

A realistic alternative to stable matrix computation is to outsource it. The demonstration of E2DM, modern architecture for safe data evaluation using convolutional neural networks, demonstrated its usefulness (CNN). Compared to CryptoNets, our tests show that E2DM achieves smaller encrypted messages and lower latency. Compared to CryptoNets, our tests show that E2DM achieves smaller encrypted messages and lower latency. Various computing applications, such as genetic testing and machine learning, will benefit from our stable matrix computation primitive. Furthermore, our E2DM system can investigate financial model evaluation in particular(9).

BAYHENN, the author's realistic approach for safe DNN inference, is presented. It is capable of safeguarding both client and server privacy simultaneously. Symmetric coding and Bayesian neural networks are the fundamental components of their solution. The essential data of the customer is protected using symmetric encryption, and the DNN weights in the Cloud server are protected using Bayesian neural networks. We're using MNIST and a real-world clinical dataset to test our solution's efficacy. The delay of both tasks is steadily reduced thanks to our technology. Moreover, their approach outperforms GAZELLE in end-to-end latency by around 5(25).

There are now two types of CareNets: the compact and resource-efficient CNN and the symmetric induction CNN. A new compact packing scheme underpins our strategy, which integrates CNN account flow into HE coding scripts, compressing the input, weight, and activation data. As a result, it is possible to implement the CareNets on retinal pictures utilizing GPU-accelerated FHE libraries for CNN inference. As a result, careNets achieve a 32.78-fold acceleration, a 45-fold gain in memory efficiency, and a 5851-fold decrease in sent message size, according to our findings. Moreover, to stay within 3 percent of the CNN unencoded baselines in terms of accuracy(3).

A deep neural network dependent on Level-HE is proposed for rapid and reliable inferences about the encoded data. The Torus Cipher Scheme (LTFHE) allows us to do ReLU activations and maximal clusters quickly and easily because it's symmetrical and straightforward to double-binary code. Our inferences by cost substitution LTFHE complications with low-cost LTFHE shifts also use logarithmic quantization. To reduce backlogs, use a mixed bit width accumulator, which is recommended since activations, maximal clusters, transitions, and accumulations in LTFHE. ReLU has a tiny multiplier depth. Somewhat Homomorphic may create considerably more complex network designs with more convolutional and activation layers. As demonstrated by our experiments, SHE is superior to LHECNNs before MNIST and CIFAR-10 in inference accuracy while also reducing inference latency by up to 94.23 percent(11).

Develop a systematic approach to generating activation employment for CNNs conducive to higher learning. Using commonly used functions like linear correction units (ReLU) and xenomorphs, researchers first determined the quality of an excellent activation function that leads to the best performance. After that, they examined the various polynomial approximation methods to determine which one provides the best results for polynomial activation. A novel weighted polynomial approximation method was also proposed to evenly distribute the batch adjustment layer's output. Different datasets such as MNIST, FMNIST, and CIFAR-10 were used to demonstrate their proposed efficacy.(14).

The introduction of a DNN model of privacy preservation known as differential multiple-schema privacy (MSDP) based on secure multi-party compute (SMC) fusion, and differential privacy makes it very practical given that current proposals cannot make all shapes completely homogeneous. Efficiently the MSDP introduces a secure multi-party alternative to ReLU to keep connection and computation costs minimum. With the help of experimental validation on four of the most widely used

human activity recognition datasets, MSDP shows superior performance with excellent generalization performance and is safe compared to current ultra-modern models without violating privacy. (15).

They are looking to take advantage of recent data-based control developments, such as deep reinforcement learning, whose high computational demands typically require outsourcing to an external server. In comparison, Fully homogeneous coding (FHE) with reinforcement learning architecture (RL) offers higher stability from partially symmetric coding (PHE) and lower computational costs (LHE). Therefore, researchers first show that the effect of coding noise on the model (VI) based tabular value frequency convergence may be analytically limited when using stable applications of the TD (0), SARSA (0), and Z learning algorithms. Then, to demonstrate numerically how little coding noise impacts these methods by using the Cheon-Kim-Kim-Song coding scheme (CKKS) diagram.(21).

3. **Background Theory**

3.1 Neural Network

The neurons in a NN are organized into layers based on how they are activated. Weighted paths connect neurons in one layer with neurons in the next. As well as an output layer made up of the network's output values contains two input layers: one for input data and another for the network's output data. Hidden layers are referred to as "hidden" since they are not visible outside. Neural networks frequently employ a variety of layer types. Neuronal networks can achieve their full potential while still being scaleable because of the "fusing" of different essential elements(28).

3.2. Deep Learning Model

Deep learning aims to extract complex features from high-dimensional data and utilize it to build a model that links inputs to outputs (such as classes). Deep learning architectures are usually constructed as multi-layered networks so that more abstract features are computed as nonlinear functions of lower-level features. Layered neural networks are the most common form of deep learning architecture(23). A CNN differs from a standard deep neural network in that it emphasizes convolution and layer pooling rather than having all layers connected. A convolutional layer performs a dot product between the layer's input and kernel filter. A sliding window method is employed to encompass the entire input. The variables of the kernels are modified in advance to extract helpful information from the input material(22). By decreasing the amount of information in a small area to just one value,

pooling layers help lower the spatial dimension of data. The model is unaffected by scaling and shifting transformations because it takes advantage of local networking by combining those layers. More layers mean a more extensive network's receptive field, which allows it to catch more complex patterns, such as curves, irregular forms, and even objects. The interaction pattern between layers has been an essential consideration in the design of neural network designs in recent years: When performing classification and regression tasks, fully connected neural networks (FCNNs) are typically employed because there will be a global interaction between the input. These neural networks (CNNs) are trained on data that has a spatial constraint.

3.2.1. Activation Layer:

The activation layer is a nonlinear feature that applies a mathematical procedure to the output of the convolution layer. Because these tasks are not linear, the difficulty increases significantly when assessing Homomorphic Encrypted (HE) data. As a result, designers must develop a substitute element that only requires multiplication and addition (5).

3.2.2. Pooling Layer:

This sample layer's purpose is to minimize the data size. Pooling can be classified into several types, such as maximum and average pooling, mean pooling, and so on. One would not use the max-pooling option in HE. Still, average pooling is a solution used in HE because average pooling determines the number of values using two operations allowed in HE(8).

3.2.3. Fully Connected Layer:

It is described as a “Fully Connected Layer” since each neuron is connected to the neuron in the previous layer. There is only a dot product operation in

this layer, consisting of multiplication and addition functions. As a result, it can be employed over encrypted data (5).

3.2.4. Dropout Layer:

This was done to avoid overfitting. Researchers often get excellent classification results for using a machine learning model, suggesting bias in the training set(26).

4. Homomorphic Encryption

The original purpose of cryptography was to provide a secure means of conversation by encrypting and sending a message that the other party could only decode. (4). By presenting the concept of computing over encrypted data in 1978 as a "privacy transformation," Rivest, Adleman, and Dertouzos sparked interest in homomorphic encryption research(13). In its broadest definition, homomorphic encryption refers to a technique for performing calculations on a message while keeping it secure. It's encrypted by adding random noise to the message. The amount of noise in an encrypted message grows when performing addition or multiplication. In addition, the rise is more pronounced compared to multiplication. Decryption relies on noise removal once rounding errors have been calculated. When an operation (addition or multiplication) is performed on the encrypted data, the standard encryption algorithm, on the other hand, does not maintain the relationship. The secret keys and ciphertexts are not accessible to the machine. Because it only uses openly available data, there is no risk of a data leak. The HE principle describes a mapping between messages and ciphertext space functions. It is no difference in the main operation, such as addition and homomorphic multiplication functions are applied to ciphertexts or unencrypted data (after decryption)(12).

In an additively HE, the operation generates the ciphertext $C_+ \rightarrow C_1 \oplus C_2$, which can be decrypted to $M_1 + M_2$.

The ciphertext $C_\times \rightarrow C_1 \otimes C_2$ is generated decrypted to $M_1.M_2$ in a multiplicatively HE.

Without understanding M_1 and M_2, both HEs obtain ciphertexts C+ and $C_\times$. Conventional encryption cannot compute $M_1 + M_2$ and M_1 when users sacrifice their confidentiality. M_2 without first decrypting c_1 and c_2. The HE is classified based on a list of unique basic mathematical operations performed on encrypted data. The number of operations in the list directly impacts HE's productivity and flexibility. A higher-number HE scheme is more versatile but less effective. A scheme with a lower number, on the other hand, is less versatile but more effective.HE method is divided into three types; Fully Homomorphic (FHE), Somewhat Homomorphic (SHE), and Partially Homomorphic (PHE) encryptions are defined, along with their limitations and scopes(24).

4.1. Partially homomorphic encryption

Using a schema like this, you can test any circuit that uses two gate types (addition or multiplication). There are no restrictions on the circle's diameter or depth. For applications that only

add or multiply encrypted data, this is an ideal type to choose. The number of standard multipliers is unbounded in the RSA cipher system, making it a PHE. Unfortunately, there is no guarantee of security in the PHE coding process. One route in the security solution is the worst instance of "noisy" difficulties. If there's some error in the encoded message, it's called noise. Therefore, it creates an uncertain relationship between the encoded message and the outside world.(19).

4.2. Somewhat Homomorphic Encryption

SHE supports a predetermined number of different homomorphic operations, thus limiting the number of operations performed. Since each operation adds to the underlying noise, a correct evaluation requires only a finite number of acts. As noise exceeds a certain threshold, message decryption fails. The BGN scheme Dan Boneh, Eu-Jin Goh, and Kobbi Nissim was the first to allow both additions and multiplications with constant-size ciphertexts. The subgroup decision problem is used to calculate BGN hardness. The SHE can evaluate circles made of addition and multiplication gates, but with depth restrictions (such as five circles at most deep). What we call homogeneous plane coding is a subset of SHE. It can evaluate circuits with variable depth, but depth must be set before coding, so you should set your scheme parameters depending on the circuits you aim to evaluate. SHE is useful in evaluating low-grade polynomials up to a certain level; however, we sometimes need to evaluate arbitrary depth circuits [26]. As shown in Fig.1.

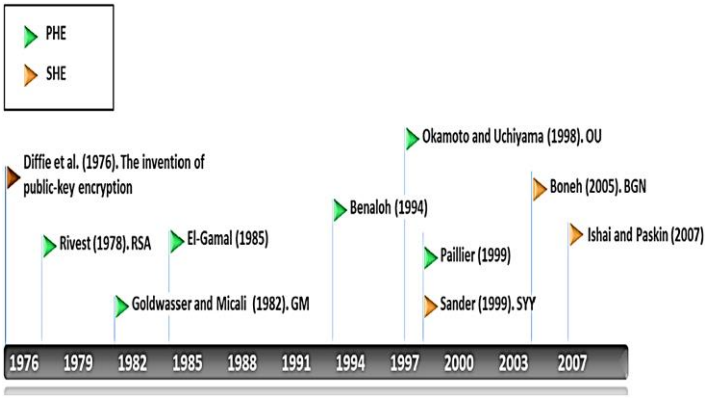

Fig. (1) Partially and Somewhat Homomorphic encryption timeline(16)

4.3. Fully Homomorphic Encryption

FHE method can evaluate circuits consisting of addition and multiplication gate, but unlike SHE, FHE has unlimited circuit depth, making it suitable for deep learning applications. Although several FHE charts have been proposed over the past decade, they have been challenging to use in practice. FHE is now being built over the SHE. Thanks to Craig Gentry, who explained in his paper

how we could build FHE from SHE using what called bootstrapping. The general idea behind FHE is that the f function can be efficiently expressed as a circuit that processes symmetrically encoded data, for example, software, mathematical operations, etc. FHE is considered a promising post-quantum tool. Existing public-key cryptography depends on the robustness of solving problems such as factoring or discrete algorithms. These widely studied problems are believed to be difficult to solve as shown in Fig2. (19).

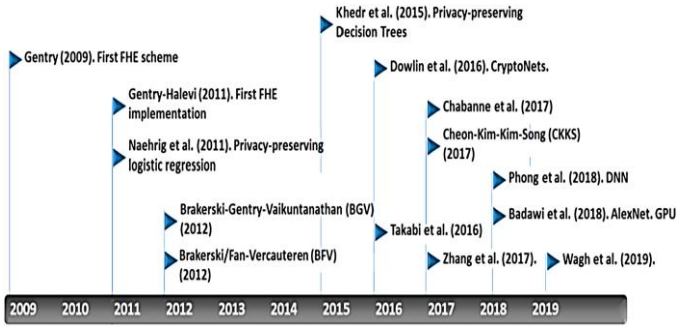

Fig. (2) Fully Homomorphic encryption timeline(16).

5. Deep Learning in Homomorphic encryption

In recent years, deep learning-based analysis has yielded outstanding outcomes in various sectors. However, there are a limited number of easy operations on rational numbers in deep learning models. Hence their mathematical formulation is complex. Many of the most recent deep learning-based outcomes were derived using deep neural networks models that only utilized a few types of operations (e.g., multiplication, addition, division, subtraction, exponential, and logarithm). The homomorphic encryption characteristic allows neural network models to include operations on ciphertext data in their functionality. Higher learning and in-depth learning are the centers of Fig.3 . Data is encrypted before processing using a secret key for training purposes only. Therefore, only the deep learning-based algorithm will be available only for the encrypted data (ciphertext). At the same time, the raw data (plaintext) is kept separate from the processing machine and hidden on the data provider's side.(7).Finally, the network may be trained immediately on ciphertext data because of the homomorphic characteristic behind the encryption method, straight support for floating-point mathematics, and all network operations written to assure application on ciphertext data. Decryption is impossible without the secret key. Hence the model generates encrypted predictions. After the training

phase, the encrypted version of a model would predict new encrypted instances (inference step) using input samples encrypted with the same key as during the training phase. The cryptographic scheme makes use of symmetric keys. As a result, both plaintext encryption and ciphertext data decoding utilize a secret key(17)(22).

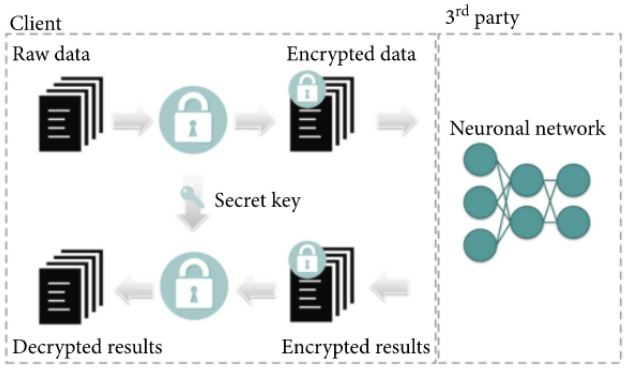

Fig. (3) Homomorphic encryption-based deep learning(22)

6. Homomorphic encryption in CNN

Homomorphic encryption-based privacy-preserving learning architectures suffer from computational overload, decreased precision, and inefficient training. Create a homomorphic privacy-preserving learning architecture using a convolutional neural network and homomorphic encryption (HCNN). Just the CNN architecture is encoded, not encrypted. The approximation problem must be solved to turn a simple CNN into a privacy-preserving CNN. If the CNN in the input comprises non-polynomial functions, the approximated CNN is retrained using only polynomial functions(20).

7. HCNN Challenge

Homomorphic encryption (HE) allows for the direct computation of encrypted data. This is perfect for dealing with DL's problems in terms of data protection. Homomorphic CNNs are CNNs that run on encrypted data (HCNNs). While FHE has a lot of potentials, there are a few obstacles that prevent standard techniques for traditional CNNs from being easily translated to HCNNs(17).

7.1 Plaintext Space

The first issue is deciding which plaintext space to use for HCNN computation. A neural network's weights and inputs are usually decimals expressed in floating-point. Unfortunately, most

FHE libraries cannot explicitly encode and process these, necessitating special care. We pack the same pixel of multiple images in a single ciphertext for simplicity and to enable inference on large datasets, as shown in Fig. (4). For batch inference scenarios, this packing is practical (where the client has many images to classify). The client might, for example, be a hospital that wants to run a disease detector on a variety of photographs from various patients. It's worth noting that the BFV scheme can be applied so that a ciphertext can have a fixed number of slots for storing several plaintext messages, allowing ciphertexts to be thought of as vectors. It's worth noting that CryptoNets is a kind of network. Was the first to suggest this packing scheme(17).

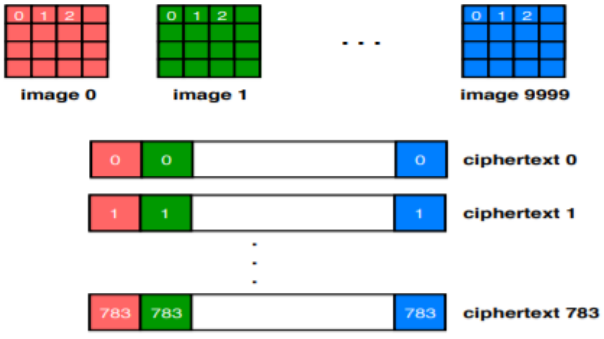

Fig. (4) a single ciphertext with multiple images(17)

7.2. Layers of Neural Networks

In most FHE schemes, computation is limited to ciphertext addition and multiplication operations. As a consequence, FHE schemes make it simple to compute polynomial functions. Like all FHE schemes, encryption introduces a small amount of noise into the data, and each operation on ciphertexts adds to that noise. Decryption is possible if the noise does not reach a certain threshold. The decrypted findings are practically meaningless otherwise(17).

8. Homomorphic Evaluation of Deep Learning

There is a heavy emphasis on the utility of higher education schemes for information processing in NN. The NN-HE model is a natural progression from NN models. The approach entails adding HE to the network input and uniformly scattering the signals across the network. Although preserving secrecy, the training and inference phases are critical to the NN operation. The model's dimensions are determined ahead of time in the inference step, so the number of apriorary operations can be calculated. From HE's viewpoint, the grid is a flat circle with layers referring to the planes. The encryption scheme made it possible. Implement a coding scheme with a fixed noise budget and no

preamble or re-encoding. In other words, since the amount of noise that the encoded text supports is known and the polynomial functions have a constant limit over the encoded data, the HE planar plot is adequate for the inference point. On the other hand, deep learning necessitates a well-planned FHE scale due to the network's many hidden layers. As a result, boot or other re-encoding operations must regulate a significant amount of noise (7).

9. Summary of Deep Learning in HE

In this paragraph, the methods used are briefly illustrated, and see the most comprehensive for deep learning in HE as shown in table (1) below.

Table (1) Summarized DLHE

Author	Years	Methodology	Outcomes
Jiang, Xiaoqian, et al.	2019	E2DM	E2DM achieves smaller encrypted messages and less latency. Compared to CryptoNets.
Xie, Peichen, Bingzhe et al.	2019	BAYHENN	In terms of end-to-end latency, our system outperforms GAZELLE by around 5 seconds.
Chao, Jin, et al.	2019	-GPU-accelerated ---FHE library -CNN inference	CareNets achieve more than 32.78 × acceleration, 45 × improvement in memory efficiency, and a 5851 × reduction in message size transmitted While maintaining the accuracy within 3% of the CNN unencoded baselines
Lou, Qian, and Lei Jiang	2019	LTFHE ReLU LHECNNs CIFAR SHE MNIST	When compared to LHECNNs previous to MNIST and CIFAR, SHE achieves state-of-the-art inference accuracy and cuts inference latency by 76.21% to 94.23 %
Obla, Srinath, et	2020	HCNN	Improved classification accuracy can be obtained by first optimizing the network's output

al.			with Softplus.
Owusu-Agyemeng, Kwabena, et al.	2021	-multiple-schema privacy (MSDP) -secure multi-party compute (SMC)	To keep connectivity and computing costs to a low, MSDP introduces a stable multi-party alternative to ReLU. MSDP outperforms current ultra-modern models in terms of efficiency and generalization, and it has been shown to be reliable.
Jihoon Suh et al.	2021	-RL -LHE -FHE -PHE -CKKS	To fully comprehend the ability of advanced RL over HE, more detailed numerical studies are needed. The interaction of computational overhead, delay, precision, and security levels must be investigated both theoretically and experimentally.
Jiang, Xiaoqian, et al.	2019	E2DM	E2DM achieves smaller encrypted messages and less latency. Compared to CryptoNets.
Xie, Peichen, Bingzhe et al.	2019	BAYHENN	In terms of end-to-end latency, our system outperforms GAZELLE by around 5 seconds.
Chao, Jin, et al.	2019	-GPU-accelerated ---FHE library -CNN inference	CareNets achieve more than 32.78 × acceleration, 45 × improvement in memory efficiency, and a 5851 × reduction in message size transmitted While maintaining the accuracy within 3% of the CNN unencoded baselines
Lou, Qian, and Lei Jiang	2019	LTFHE ReLU LHECNNs CIFAR	When compared to LHECNNs previous to MNIST and CIFAR, SHE achieves state-of-the-art inference accuracy and cuts inference latency by 76.21% to 94.23 %

		SHE MNIST	
Obla, Srinath, et al.	2020	HCNN	Improved classification accuracy can be obtained by first optimizing the network's output with Softplus.
Owusu-Agyemeng, Kwabena, et al.	2021	-multiple-schema privacy (MSDP) -secure multi-party compute (SMC)	To keep connectivity and computing costs to a low, MSDP introduces a stable multi-party alternative to ReLU. MSDP outperforms current ultra-modern models in terms of efficiency and generalization, and it has been shown to be reliable.
Nayna Jain et a.	2021	-CKKS -FHE -HElib library	- a secure way to comput it is possible to implement encrypted inference in a reasonable time by investing in the right CNN design and parameter choices.
Jihoon Suh et al.	2021	-RL -LHE -FHE -PHE -CKKS	To fully comprehend the ability of advanced RL over HE, more detailed numerical studies are needed. The interaction of computational overhead, delay, precision, and security levels must be investigated both theoretically and experimentally.

5.Conclusion

In this paper, we study recent developments in HE cryptosystems, concentrating primarily on the intersection of cryptography and neural networks, reviewing the state-of-the-art and state-of-practice; and explain basic concepts such as totally homomorphic encryption, slightly homomorphic encryption, partly homomorphic encryption, and homomorphic in deep learning, such as HCNN. The main aim is

to demonstrate how non-trustworthy individuals can process encrypted data without revealing sensitive information. We focus on privacy-preserving neural networks and their applications in particular.

Author Contributions: All authors contributed equally in writing this article. All authors read and approved the final manuscript. A.K and E.M. proposed this idea, A.K suggested the general outline of the paper. Then E.M carried out each part, and discussed it with A.K to suggest improvements.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1]. Alhudhaif A, Ahmad M, Alkhayyat A, Tsafack N, Farhan AK, Ahmed R. 2021. Block Cipher Nonlinear Confusion Components Based on New 5-D Hyperchaotic System. *IEEE Access*. 9:87686–96

[2]. Boulemtafes A, Derhab A, Challal Y, Boulemtafes A, Derhab A, et al. 2020. A review of privacy-preserving techniques for deep learning To cite this version : HAL Id : hal-02921443 A Review of Privacy-Preserving Techniques for Deep Learning

[3]. Chao J, Badawi A Al, Unnikrishnan B, Lin J, Mun CF, et al. 2019. CaRENets: Compact and Resource-Efficient CNN for Homomorphic Inference on Encrypted Medical Images

[4]. Fan J, Vercauteren F. 2012. Somewhat Practical Fully Homomorphic Encryption. *Proc. 15th Int. Conf. Pract. Theory Public Key Cryptogr.*, pp. 1–16

[5]. Hao M, Li H, Luo X, Xu G, Yang H, Liu S. 2020. Efficient and Privacy-Enhanced Federated Learning for Industrial Artificial Intelligence. *Proc. IEEE*. 16(10):6532–42

[6]. Hasan N, Farhan A. 2019. Security Improve in ZigBee Protocol Based on RSA Public Algorithm in WSN. *Eng. Technol. J.* 37(3B):67–73

[7]. Huang K, Liu X, Fu S, Guo D, Xu M. 2021. A Lightweight Privacy-Preserving CNN Feature Extraction Framework for Mobile Sensing. *IEEE Trans. Dependable Secur. Comput.* 18(3):1441–55

[8]. Ieee SM, Ieee F, Sze V, Chen Y-H, Yang T-J, Emer JS. 2017. MIT tutorial. *Proc. IEEE*. 105(12):2295–2329

[9]. Jiang X, Lauter K, Kim M, Song Y. 2018. Secure outsourced matrix computation and

application to neural networks. *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1209–22

[10]. Kadhim AF, Kamal ZA. 2018. Generating dynamic S-BOX based on Particle Swarm Optimization and Chaos Theory for AES. *Iraqi J. Sci.* 59(3):1733–45

[11]. Lou Q, Jiang L. 2019. SHE: A fast and accurate deep neural network for encrypted data. *Adv. Neural Inf. Process. Syst.* 32(NeurIPS):1–9

[12]. Lyu L, He X, Law YW, Palaniswami M. 2017. Privacy-preserving collaborative deep learning with application to human activity recognition. *Int. Conf. Inf. Knowl. Manag. Proc.* Part F1318(November):1219–28

[13]. Macq B, Jj Q. 2021. Cryptography for Trusted Artificial Intelligence in Medicine. , pp. 207–10

[14]. Obla S, Gong X, Aloufi A, Hu P, Takabi D. 2020. Effective Activation Functions for Homomorphic Evaluation of Deep Neural Networks. *IEEE Access*. 8:153098–112

[15]. Owusu-Agyemeng K, Qin Z, Xiong H, Liu Y, Zhuang T, Qin Z. 2021. MSDP: multi-scheme privacy-preserving deep learning via differential privacy. *Pers. Ubiquitous Comput.*

[16]. Pulido-Gaytan B, Tchernykh A, Cortés-Mendoza JM, Babenko M, Radchenko G, et al. 2021. Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities. *Peer-to-Peer Netw. Appl.* 14(3):1666–91

[17]. QaisarAhmadAlBadawi A, Chao J, Lin J, Mun CF, Jie SJ, et al. 2020. Towards the AlexNet Moment for Homomorphic Encryption: HCNN, the First Homomorphic CNN on Encrypted Data with GPUs. *IEEE Trans. Emerg. Top. Comput.*

[18]. Rokan Naif J, H. Abdul-majeed G, K. Farhan A. 2019. Internet of Things Security using New Chaotic System and Lightweight AES. *J. Al-Qadisiyah Comput. Sci. Math.* 11(2):45–52

[19]. Sathya SS, Vepakomma P, Raskar R, Ramachandra R, Bhattacharya S. 2018. A Review of Homomorphic Encryption Libraries for Secure Computation. , pp. 1–12

[20]. Sirichotedumrong W, Kiya H. 2021. A GAN-based image transformation scheme for privacy-preserving deep neural networks. *Eur. Signal Process. Conf.* 2021-Janua(c):745–49

[21]. Suh J, Tanaka T. 2021. Encrypted Value Iteration and Temporal Difference Learning over Leveled Homomorphic Encryption. *Proc. Am. Control Conf.* 2021-May:2555–61

[22]. Vizitiu A, Niă CI, Puiu A, Suciu C, Itu LM. 2020. Applying Deep Neural Networks over Homomorphic Encrypted Medical Data. *Comput. Math. Methods Med.* 2020:

[23]. Wei L. 2020. A Brief Introduction to Deep Learning. *C++ Template Metaprogramming Pract.*, pp. 69–82

[24]. Will MA, Ko RKL. 2015. *A guide to homomorphic encryption*. Elsevier Inc. 101 pp.

[25]. Xie P, Wu B, Sun G. 2019. Bayhenn: Combining Bayesian deep learning and homomorphic encryption for secure DNN inference. *IJCAI Int. Jt. Conf. Artif. Intell.* 2019-Augus:4831–37

[26]. Zaid Khalaf Hussien BND. 2020. Anomaly Detection Approach Based on Deep Neural Network and Dropout. *Baghdad Sci. J.* 17:701–9

[27]. Zhang D, Chen X, Wang D, Shi J. 2018. A survey on collaborative deep learning and privacy-preserving. *IEEE 3rd Int. Conf. Data Sci. Cybersp.*, pp. 652–58

[28]. Zhang T, Zeng Y, Xu B. 2016. HCNN: A neural network model for combining local and global features towards human-like classification. *Int. J. Pattern Recognit. Artif. Intell.* 30(1):