•**Review**•

Privacy-preserving deep learning techniques for wearable sensor-based big data applications

Rafik HAMZA*, Minh-Son DAO

Integrated Big Data Research Center | NICT-National Institute of Information and Communications Technology, Tokyo, Japan

* **Corresponding author,** rafik.hamza@nict.go.jp; rafik.hamza@hotmail.com

Received: 27 October 2021 **Revised:** 16 December 2021 **Accepted:** 20 January 2022

Citation: Rafik HAMZA, Minh-Son DAO. Privacy-preserving deep learning techniques for wearable sensor-based big data applications. Virtual Reality & Intelligent Hardware, 2022, 4(3): 210—222
DOI: 10.1016/j.vrih.2022.01.007

Abstract Wearable technologies have the potential to become a valuable influence on human daily life where they may enable observing the world in new ways, including, for example, using augmented reality (AR) applications. Wearable technology uses electronic devices that may be carried as accessories, clothes, or even embedded in the user's body. Although the potential benefits of smart wearables are numerous, their extensive and continual usage creates several privacy concerns and tricky information security challenges. In this paper, we present a comprehensive survey of recent privacy-preserving big data analytics applications based on wearable sensors. We highlight the fundamental features of security and privacy for wearable device applications. Then, we examine the utilization of deep learning algorithms with cryptography and determine their usability for wearable sensors. We also present a case study on privacy-preserving machine learning techniques. Herein, we theoretically and empirically evaluate the privacy-preserving deep learning framework's performance. We explain the implementation details of a case study of a secure prediction service using the convolutional neural network (CNN) model and the Cheon-Kim-Kim-Song (CHKS) homomorphic encryption algorithm. Finally, we explore the obstacles and gaps in the deployment of practical real-world applications. Following a comprehensive overview, we identify the most important obstacles that must be overcome and discuss some interesting future research directions.

Keywords Wearable technology; Augmented reality; Privacy-preserving; Deep learning; Big data; Secure prediction service

1 Introduction

Japan's “Society 5.0” project envisions a human-centered society that combines the economic progress of the use of artificial intelligence and big data applications[1]. Considering Society 5.0, the Japanese government and IT industries are collaborating to implement technological advances remotely through cloud platforms, particularly in AI with big data[1,2]. Figure 1 shows the stages of the evolution of human society from the previous stages toward Society 5.0. The project is mainly to balance economic progress

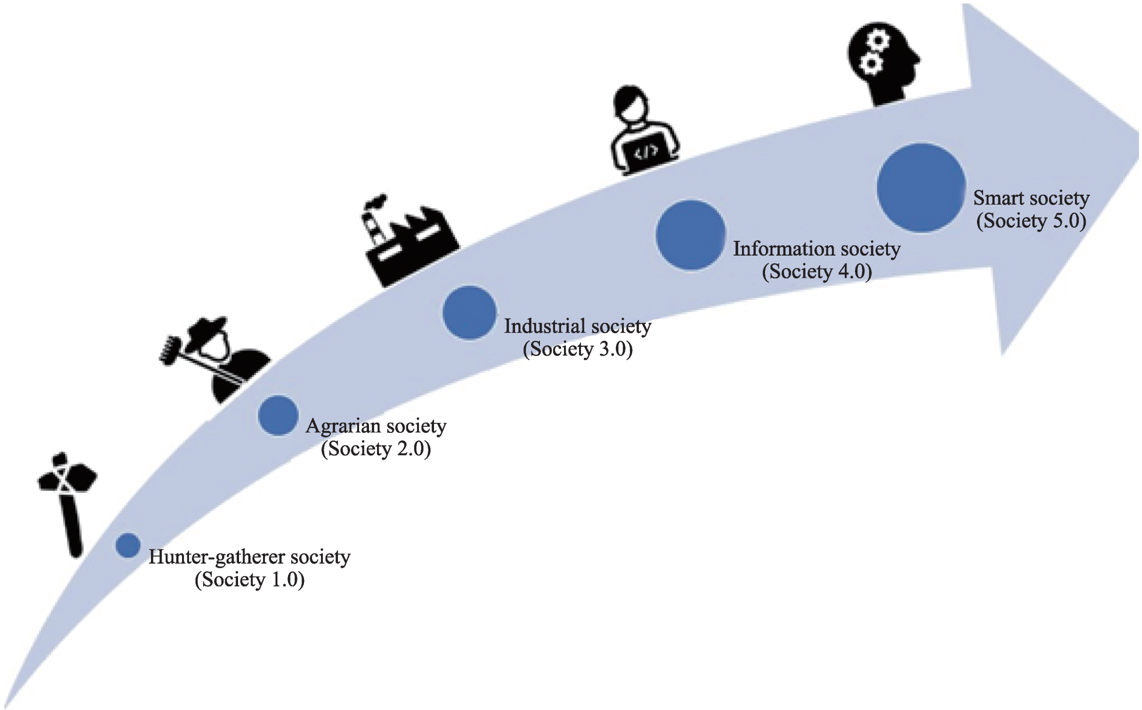

Figure 1 Technology evolution towards "Society 5.0".

and solutions to social issues. Society 5.0 is a promising technology framework in the era of 5G and AI. The incorporation of new and developing technology into all aspects of human life contributes to the production of datasets involving individuals and institutions. These data are aggregated for big data, which can be used for different analytics purposes such as medical, financial decision-making, and online advertisement. Therefore, the capacity to absorb extraordinarily large information, analyze, and interpret it effectively, and draw results and inferences is referred to as "big data analytic"[3].

Over the last few decades, the Internet has had a tremendous impact, globally linking networked equipment such as computers and wearable sensors. Considering the rapid advancement of the Internet, the reach of Internet connectivity has enabled the primary mode of human communication and engagement. Information applications deliver a wide range of information usage to increase the quality of industrial applications and the quality components of the human lifestyle.

A critical challenge for the government and enterprises is ensuring data security and privacy when processing huge datasets. Most IT companies collect, transport, store, and analyze large datasets and face significant privacy issues every day. These issues make the realization of the “Society 5.0” project a challenging issue. The issues of data protection during transmission and at rest have attracted scholarly attention recently[4,5]. Cryptographic-based security mechanisms propose different solutions to safeguard the security of datasets as they transit across networks or are stored in data warehouses, for example, encryption and blockchain technologies[6,7]. However, the unresolved issue is how to preserve the privacy of the collected data effectively and securely while it is being processed.

This paper aims to anticipate how security technology will be useful for the safe processing of the collected data from wearable sensors, particularly in increasing the utility and performance of privacy-preserving machine learning analytics in the era of 5G and beyond. This paper also considers the analytics technology of cross-big data in emerging AI-5G applications. Assume that a user has the entire value of their information assets encrypted using their secret key and that all the information assets should be encrypted and stored on the cloud servers. Herein, without decrypting the user's information assets, statistical analysis can be performed without any need to exchange the user's secret and information attached to their assets. Owing to the confidential nature of some private information assets, only limited authorized users (including data owners) can access and use these information assets. However, these private information assets can contribute to increasing the results of any big data machine learning model. Accordingly, a collaboration between cryptography and machine learning techniques can exploit the efficient and safe use of private information permitted by big data applications[8].

In this study, we present an overview of privacy-preserving machine learning techniques for emerging applications in 5G environments.

We also present a cutting-edge overview of security encryption applications in big data analytics using statistical analysis for emerging applications of AI-5G. We aim to anticipate how security technology will be useful for the safe processing of big data, particularly in increasing the utility and performance of privacy-preserving machine learning for big data analytics. Finally, we highlight some discussions and research opportunities concerning the future of AI-5G security. This survey is designed to provide researchers and practitioners with a clear understanding and basis for comprehending, applying, and expanding the relevant state-of-the-art secure big data analytics.

The rest of the study is organized as follows. Considering Section 3, the security and privacy discussion in VR/AR systems is presented. Regarding Section 4, privacy-preserving machine learning techniques for data analytics are discussed. Finally, we conclude the study with some discussions and challenges of the emerging applications of AI-5G in Section 5.

2 Security and privacy in wearable sensors in the era of 5G and AI

Augmented reality technologies are rapidly developing and becoming commercially available. These innovative mechanisms provide new security and privacy concerns and objections[9,10]. These difficulties can be divided into two categories: extent and application of the system. Overlaps among applications sharing different types of devices and more complicated authentication protocols for wearable sensors provide security and privacy problems with AR technology. Although some problems may be solved by adapting current solutions to smartphones, others require innovative methods for wearable devices. In addition to the conventional description of adjusting real and virtual objects in real time for AR technologies with the developed applications and protocols, we consider the following characteristics in our study.

First, a sophisticated collection of information is always in most of the devices and sensors (e.g., GPS and microphones). Second, most innovative wearable sensors have multiple interactive outputs, such as touchscreens and voice commands. Majority of the device platforms can run several applications simultaneously and can connect wirelessly with other augmented reality devices. This gives companies an alternative approach to deploying collaboration platforms to enhance the performance of virtual reality and augmented reality applications. The joint effort could produce new innovative ideas, especially with on-device AI-enabled technology.

Augmented reality applications may require access to various sensor data to work properly[9], such as video and audio feeds and GPS data. A major issue of AR systems (such as desktop and smartphone operating systems) is to balance the access necessary for functioning with the danger of an application stealing data or misusing that access. For example, a rogue program may leak a user's location or video stream to its backend servers. Moreover, VR/AR systems have the capability to record significantly more personally identifiable information than conventional systems. Thus, VR/AR systems can have a significant influence on user privacy, such as eye-tracking technology, collecting biometric data, recording microphones, capturing images, location-tracking, etc. Regarding this case, a security mechanism is required for VR/AR platforms[9,10].

Chen et al. proposed a mobile edge computing framework for augmented reality applications based on federated learning[11]. They addressed the low-latency object detection and classification problems of AR applications using federated learning and minimized user privacy concerns. However, federated learning techniques have different security concerns[7,9]. Therefore, we conclude that cryptography techniques with machine learning can be more appropriate for VR/AR applications to ensure user privacy.

Augmented reality applications use computer-generated graphics to overlay improvements on the user's perspective of reality using big data and machine learning techniques, especially with virtual reality industrial applications[12]. These applications quickly develop and become more commercially available, especially considering the expansion of wearable device exploitation. Figure 2 shows some examples of wearable devices that can be used for AR and VR applications. Although only smart glasses can be directly observed with augmented reality, most of these applications use different data from other wearable devices, such as smart clothes, to improve the realistic perception of virtual elements[13]. The collected data from wearable devices help further AR applications to enhance the reality for users. However, these developments have resulted in high concerns of privacy and security challenges. For example, regarding health monitoring wearable devices, we can observe some techniques for healthcare monitoring based on the wearable sensors for visual reality and mobile AR[14,15]. There are other security aspects for wearable healthcare sensors. This may cause some problems by manipulating the physical hardware or some problems when the device is measuring data from several sensors and preserving the privacy for predictive analysis (e.g., health care)[15].

Because a small device may be worn on a part of the body, which should be easily accessible, the

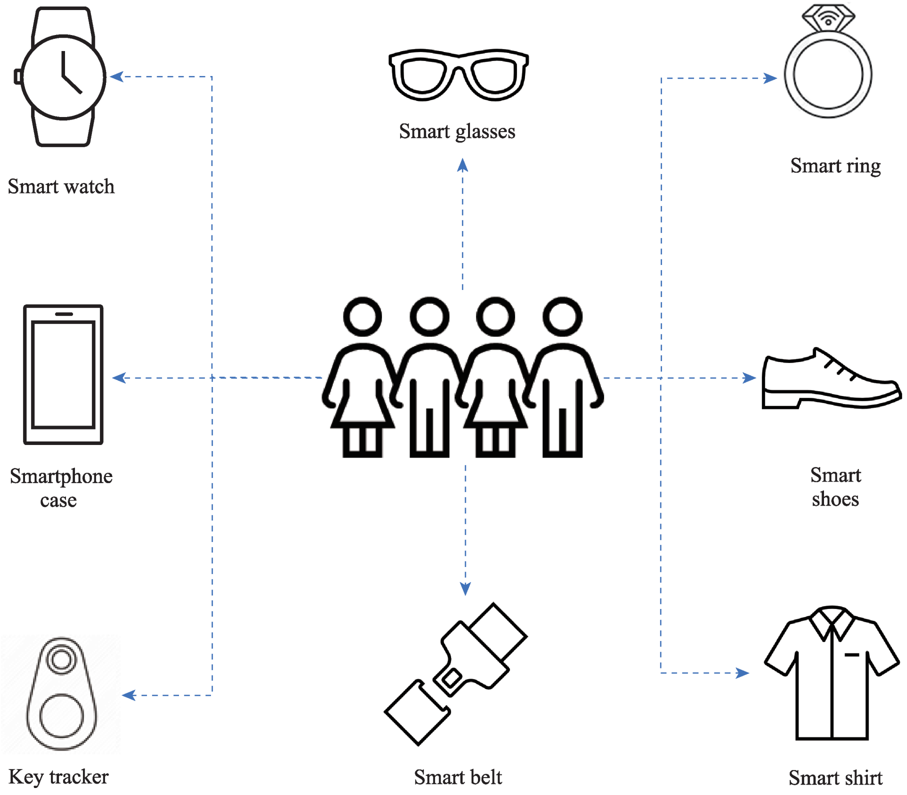

Figure 2 Some popular wearable devices.

possible results for an increase in human performance[16] are limited. This may require a separate large screen or controller. The technology employs a smartphone as an entry point to transport data, and 5G-based cloud computing services contribute to achieving various machine learning tasks and other purposes[11,17]. This has led to various privacy and security challenges for virtual reality learning environment applications[18].

To solve the challenging problems beyond 5G application scenarios, wearable systems need to evaluate the information security measures that expand on the information security aspects needed[9]. Widely known security concerns such as malware and ransomware can have a significant influence on VR/AR systems. Several VR/AR platforms do not use encryption for network connections, which is highly required in conventional media such as instant messaging applications. Furthermore, several platforms also depend on untrustworthy third-party services or connections[9]. Similar to any collaborative system, VR/AR platforms may collect data locally or on the edge server. These data may also need to be protected, possibly indicating the need to employ cryptography techniques. A new approach to preventing privacy issues and security breaches in wearable device projects is privacy-preserving deep learning using cryptography techniques[3,7].

3 Privacy-preserving techniques

Our main goal is to assess state-of-the-art solutions for the statistical analysis of confidential data and minimize the concerns of the user's privacy. These techniques should enable the use of advanced analytic techniques over encrypted private information sets with very large and diverse big datasets. They can also have the capacity to delegate computations to a third party, such as cloud providers, considering the resources. In addition, the competency of data analysts has spurred advancements toward efficient privacy-preserving deep learning for big data analysis. Therefore, several techniques have been developed to assess the usability, level of security, and performance of homomorphic encryption when used in big data applications[19‒21]. Several deep learning algorithms have been examined to determine the usability of homomorphic encryption algorithms to securely handle data. Some examples of these strategies are discussed below.

In this section, we discuss some important relevant state-of-the-art studies on privacy-preserving deep learning for big data analytics. These include different discussions on the privacy-preserving deep learning techniques using homomorphic encryption algorithms. Aono et al. used various homomorphic encryption methods to construct logistic regressions and discovered that this process was scalable across homomorphically encrypted data[22]. Esperanca et al. pointed out that the effective and scalable statistical analysis of the encrypted datasets necessitates particularly adapted computational approaches[23]. This could differ significantly from the state-of-the-art techniques for plaintext settings with no encryption settings. Yonetani et al. employed a homomorphic encryption algorithm for visual learning, which included face identification, and determining locations on private information might be accessed[24].

This section focuses on the deployment of the security of database servers and clients using the homomorphic encryption structure as described in the literature[25‒28] as shown in Figure 3. The computing process of the fully homomorphic encryption algorithm is shown in Figure 3. The fully homomorphic cryptosystem's analytical performance can be implemented as a cloud server on a virtual reality platform.

The problem of privacy-preserving big data has been investigated severally[29‒31]. Various privacy-preserving protocols have also been proposed. Privacy-preserving big data protocols can be classified into two categories: randomization- and secure multiparty computation (SMC)-based approaches. Considering

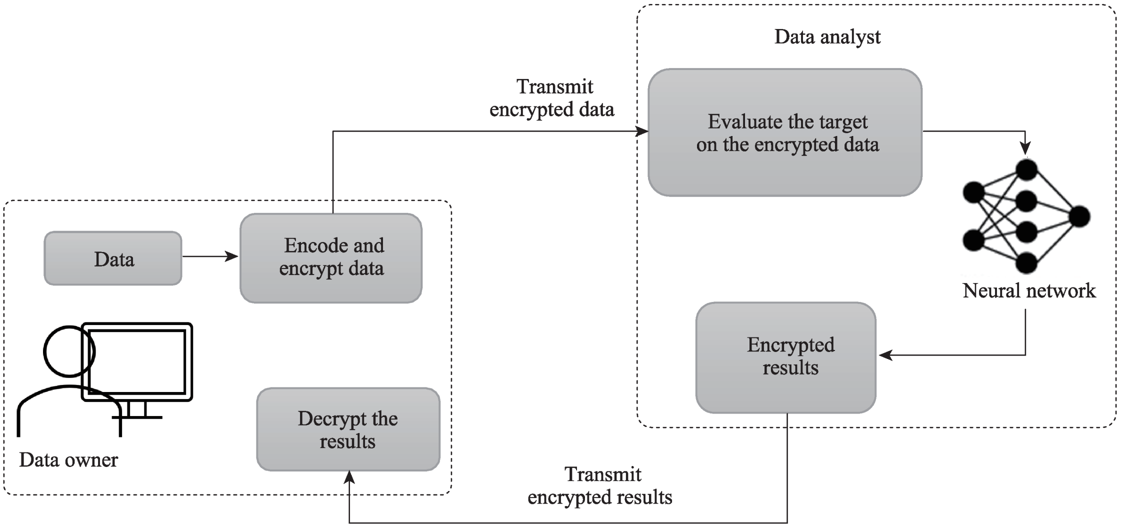

Figure 3 Framework of privacy-preserving deep learning using homomorphic encryption algorithm.

the aim of this study, we will focus on privacy-preserving deep learning techniques[32,33]. Secure multiparty computation-based approaches are often used to develop ways in which participants can collectively compute a function using their information, while maintaining privacy.

We present a practical scenario of using homomorphic encryption for privacy-preserving deep learning algorithms for big data analytics. Figure 3 shows the details of the scenario. We use this scenario to implement our secure prediction prototype in Figure 4 (in the following section). Initially, private prediction is introduced as a service when the data owner outsources a third party for analytics or the prediction of private encrypted data. For example, consider an untrustworthy data analyst with a trained model and perhaps the computational capabilities to perform the analytic tasks.

Two possibilities were investigated between the data owner and the data analyst as shown in Figure 3. Therefore, private prediction as a service is considered as the first phase to make the data owner outsource

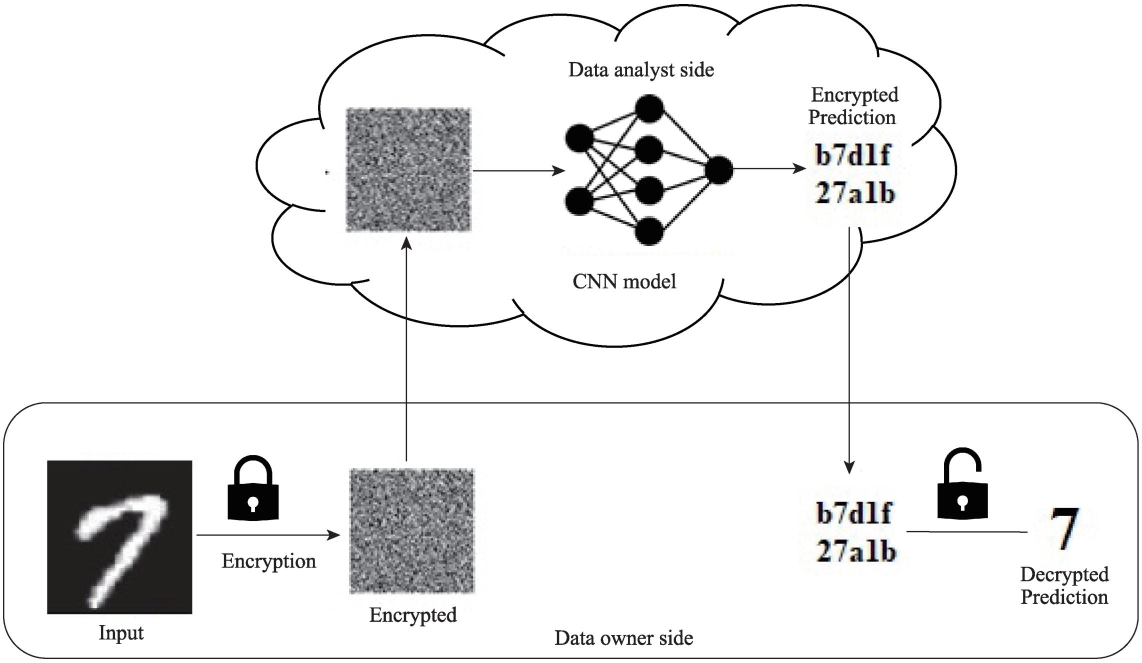

Figure 4 Privacy-preserving deep learning as a secure prediction prototype.

the analysis of his encrypted data (denoted also ciphertext) using a cloud or third party. For example, consider an untrustworthy data analyst with a trained model and perhaps the computational capabilities to perform the prediction challenge. The training service is considered as the second phase, where the owner provides ciphertext to the cloud for training an encrypted ready model w_encr. Thereafter, w_encr is adopted to analyze the new ciphertexts (psi). The model created is set and ready for analytics requests. Considering both situations, the encrypted outcomes are returned to the data owner to be decrypted. Regarding the first situation, the data owner will only be aware of the data and the results. The prediction result is P_(encr(psi)); however, nothing is known from the model w. This is a secret asset for the untrustworthy data analyst.

Note that implementing homomorphic encryption for statistical analysis can maintain metric reliability even when randomization is used. Nevertheless, difficulties similar to those encountered in privacy-preserving machine learning emerge. Data analysts rely on different deep learning algorithms to reach the desired predictions, such as convolutional neural networks[34], recurrent neural networks[35], and linear means classifiers[36]. For example, Li et al. introduced a machine-learning scheme with two homomorphic encryption algorithms to preserve the privacy of user datasets[37]. Although it performs model training using distinct public keys, the computational load is increased by several additional encryption and decryption operations in each iteration.

Bost et al. deployed and trained three different classifiers: naive Bayes, a hyperplane decision, and decision trees over the encrypted data. In addition, recent advances have allowed GPU usage for prediction using deep learning algorithms[38]. Takabi et al. used a GPU to speed up the arithmetic operations of convolutional neural networks (CNNs) on encrypted messages[39]. The authors of PrivFT[40] conducted a study on the CKKS method based on GPU implementation. Later, Jung et al. demonstrated the first GPU implementation for bootstrapping CKKS using the arithmetic of approximate numbers[41]. The authors assert that they have excellent results with a 40.0 speedup compared to the previous eight-thread CPU deployment using the same data under the same experimental environment.

4 Case study of the privacy-preserving handwritten digit classification

In this section, we present a case study of privacy-preserving machine learning adopted from the scenario shown in Figure 3. We employ a security framework with an encryption technique as a secure prediction service (Figure 4). We use the Modified National Institute of Standards and Technology (MNIST) dataset sample, which provides [28×28] gray-scale pictures of decimal numbers zero to nine, with a typical partition of 50000 training photos and 10000 test set images. Although MNIST is considered as a straightforward sample, it retains the industry standard for homomorphic analysis challenges. We also utilized a basic neural network comprising a CNN model with two linear layers.

Considering the implementation of homomorphic encryption, we utilize the CKKS algorithm from the Seal toolkit. Because the homomorphic encryption algorithm constraints on the range of multiplications, we chose the square activation function. The parameters for the CKKS encryption algorithm from the seal tool are poly modulus degree=8192 with 128-bits security. Selecting alternative precision settings and modifying the coefficient modulus of the CKKS algorithm while evaluating the degradation and accuracy cause challenging experimental analysis, especially with control precision of the fractional part from the encryption parameters.

Generally, the model used in this test is a convolutional neural network, which consists of convolutional layers. A two-dimensional (2D) convolution is applied to an input signal composed of several input planes.

Figure 4 shows the proposed solution to secure the prediction prototype via a privacy-preserving deep learning technique. The implemented model consists of a convolution with four kernels. The shape of the kernel is 7×7, and the stride is 3×3. We also used a square activation function, where each input value was processed towards the estimated activation function in this layer. We employed the first linear layers with input and output sizes of 256 and 64, respectively. Thereafter, we apply the square activation function and the second linear layer with input and output sizes of 64 and ten, respectively. Subsequently, we train a plain PyTorch model to classify the MNIST sample and to test its accuracy on the test set. We initiated the encrypted evaluation using the pre-trained prototype. Finally, we run an encrypted evaluation over the entire test set. These operations overall have high complexity and are time-consuming.

Moreover, polynomials of varying degrees can be used to approximate activation functions. Higher degree polynomials provide a more accurate approximation[42]. Note that when used to replace the activation function in a CNN, they result in better trained model performance. However, when operations are performed on encrypted data, a higher-degree polynomial leads to extremely sluggish calculations. Consequently, practically, a solution based on HE schemes should be limited to calculating low-degree polynomials[29]. We must strike a balance between the degree of the polynomial approximation and the model's performance.

The proposed CNN model is trained on input with plaintext and encrypted sets. We aim to demonstrate the network's ability to learn from encrypted data. We further evaluated the CNN model's ability to maintain performance by running and evaluating the results of two scenarios: plaintext and encrypted sets. Figure 5 shows the accuracy results for training the CNN model on a Figure 5a plaintext and Figure 5b Encrypted data.

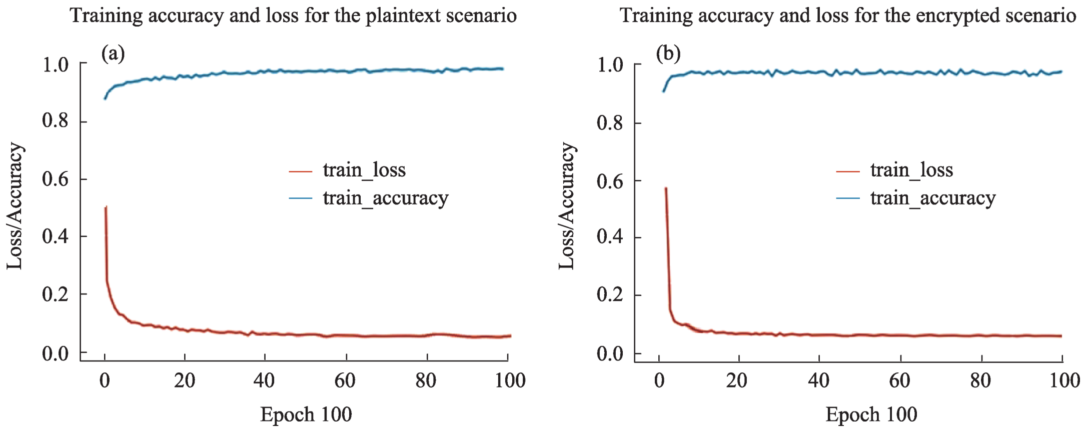

Figure 5 Performance of the suggested CNN model on both the plaintext and encrypted sets: (a) plaintext and (b) encrypted set.

The results of building the classifier with plaintext set obtained 99.78% and 99.75% accuracies on the training and testing datasets, respectively. Figure 5a shows the accuracy findings from training the model with plaintext. The results of building the classifier with encrypted data obtained 99.57% and 99.45% accuracies on the training and testing datasets, respectively. Figure 3b represents the accuracy findings from training the model with the encrypted set generated by the CKKS algorithm. All the pre-trained CNN models performed well considering the classification accuracy.

The accuracy results achieved by training the proposed CNN model with plaintext were approximately 0.5% higher than those of the encrypted data. The results confirm the network's ability to learn from the encrypted data and integrate the security mechanism in the emerging applications of AI-5G. The proposed cryptosystem can be addressed for different VR and AR applications, such as speech emotion recognition[43], neural network image reconstruction[44], and other relevant neural network applications[45–47].

5 Comparison of existing computational approaches

To maintain privacy, computational approaches intend to apply CNNs to encrypted data. They encrypt data using well-known encryption techniques. Considering state-of-the-art privacy-preserving techniques, CryptoNets and CryptoDL alter the NN, making it process encrypted data and is compliant with the encryption mechanism utilized. These changes have an impact on the network's performance, considering the computational complexity. Subsequently, the data owner may face a lag in their prediction results. The computational complexity and prediction latency are increased because all the functions are computed using nested additions and multiplications. The size of encrypted data is inflated sometimes because of the encrypted data processing operations and the selected encryption algorithm. In fact, the size of encrypted data is one to three times larger in magnitude than unencrypted data[48].

Table 1 lists the computational methods using encrypted data, the dataset utilized, the accuracy of the classification model, the class of artificial neural network, along with the number of convolutional layers in the network (depth of the NN), and the homomorphic encryption references used in their works.

Table 1 computational methods comparison

	Dataset	Accuracy	Artificial neural network	Homomorphic encryption
CryptoNN[48]	MNIST	95.49%	CNN 3 NN depth	Functional Encryption[49]
CryptoNets[50]	MNIST	99%	CNN 2 NN depth	YASHE scheme[51]
CryptoDL[51]	MNIST	99.52%	CNN 5 NN depth	HELib[52]

CryptoDL seeks to increase the speed and latency of CryptoNets and to apply a deeper NN to encrypted data; nonetheless, it has limitations. The activation algorithms and approximation techniques used by CryptoNets and CryptoDL differ significantly. Considering CryptoNets, the sigmoid approximation was employed as the activation function, whereas CryptoDL examined the numerous activation functions before settling on the ReLu approximation. Furthermore, CryptoNN uses a different encryption approach than cryptoNets and CryptoDL to conduct NN operations while maintaining their secrecy and security. This privacy is preserved using secure matrix computing based on FE, rather than through customized calculation necessitating the change of NN's functions and structure. Since CryptoNets and CryptoDL enable the categorization of encrypted data using NNs programme builds on unencrypted data, CryptoNN enables both training and testing on encrypted data[52,53]. Figure 6 shows the overview structure of the CryptoNN framework. Although CryptoDL outperformed CryptoNets on the MNIST dataset with a lower computing cost, similar to CryptoNets, it has restrictions considering the number of hidden layers and complexity of the dataset employed.

All of the approaches mentioned in Table 1 have only been attempted on basic datasets like MNIST and CIFAR-10; hence, their scalability is actually unknown for big data industrial applications. Consequently, larger and more accurate big data samples should be employed and examined. Although these approaches were tested using small datasets and small networks, their complexity and latency were clearly visible. This emphasizes the challenge of applying these approaches to cutting-edge CNNs and handling more realistic situations.

6 Discussion and conclusion

In this paper, we present a summary of recent privacy-preserving big data analytics with homomorphic

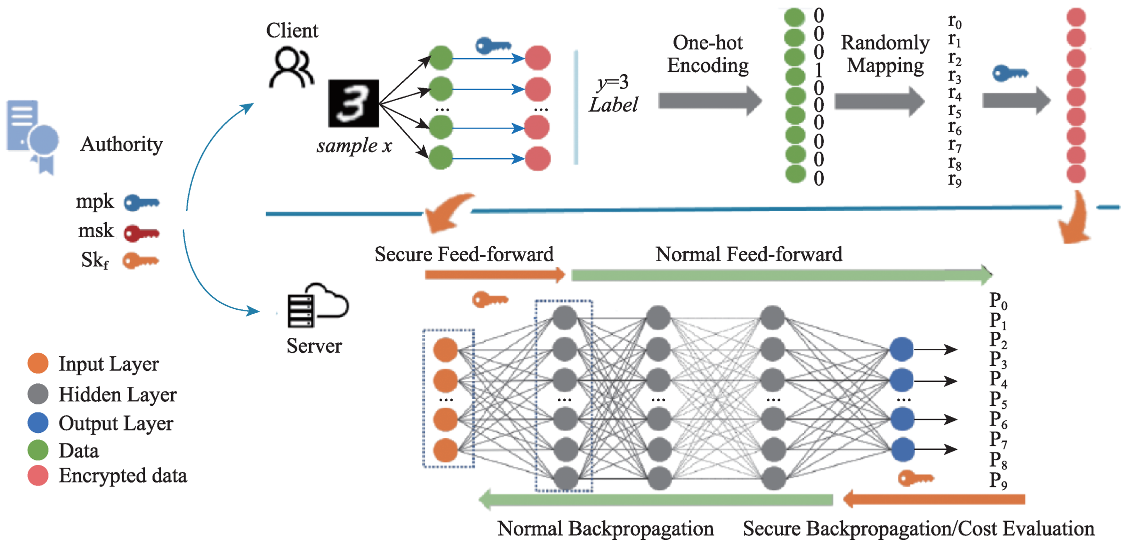

Figure 6 CryptoNN framework adapted from.[47]

encryption algorithms. We have also described a scenario that may be of interest to the analysis techniques between data owners and analysts. Finally, we have explored the obstacles and gaps in the deployment of practical real-world applications. As a result, we believe that a homomorphic encryption algorithm could be a viable approach for industrial applications in the near future, allowing secure and efficient collaboration between data owners and untrustworthy data analysts. Because this is a developing study area, further discoveries will allow the usage of data owners in a production environment, particularly in support of the big data analytical process.

One of the biggest obstacles in this context is the development of fully feasible use cases for multimedia data such as high-resolution images and videos[54]. This is because security techniques are still quite slow due to the insufficient computing power of wearable devices and the highly complex operations of the encryption algorithms. For example, an online application for face recognition can withstand delays of only a few seconds. However, it can provide highly secure applications[55]. On the contrary, offline actions can be considered for cryptography deployments, such as statistics on medical research outcomes, even if they are time-consuming. Nevertheless, the scope of industrial use cases will grow in lockstep with the advancement of both the understanding and efficiency capacity of cryptography and security algorithms. This essentially transformative solution will become increasingly widespread for applications designed to protect the privacy and security of wearable data.

Declaration of competing interest

We declare that we have no conflict of interest.

References

1 Onday O. Japan's society 5.0: Going beyond industry 4.0. Business and Economics Journal, 2019, 10(2):1−6
DOI: 10.4172/2151-6219.1000389

2 Hamza R, Zettsu K. Investigation on privacy-preserving techniques for personal data. ICDAR'21: Proceedings of the 2021 Workshop on Intelligent Cross-Data Analysis and Retrieval. 2021, 62−66
DOI:10.1145/3463944.3469267

3 Gahi Y, Guennoun M, Mouftah H T. Big Data Analytics: security and privacy challenges. In: 2016 IEEE Symposium on Computers and Communication. Messina, Italy, IEEE, 2016, 952−957
DOI:10.1109/iscc.2016.7543859

4 Hamza R, Hassan A, Huang T, Ke L S, Yan H Y. An efficient cryptosystem for video surveillance in the Internet of Things environment. Complexity, 2019, 1625678
DOI:10.1155/2019/1625678

5 Jia B, Zhang X S, Liu J W, Zhang Y, Huang K, Liang Y Q. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Transactions on Industrial Informatics, 5960, PP(99): 1
DOI:10.1109/tii.2021.3085960

6 Patil A S, Hamza R, Hassan A, Jiang N, Yan H Y, Li J. Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. Computers & Security, 2020, 97: 101958
DOI:10.1016/j.cose.2020.101958

7 Rafique A, van Landuyt D, Heydari Beni E, Lagaisse B, Joosen W. CryptDICE: Distributed data protection system for secure cloud data storage and computation. Information Systems, 2021, 96: 101671
DOI:10.1016/j.is.2020.101671

8 Dahl M, Mancuso J, Dupis Y, Decoste B, Giraud M, Livingstone I, Patriquin J, Uhma G. Private machine learning in tensorflow using secure computation. 2018

9 Wang M H, Zhu T Q, Zhang T, Zhang J, Yu S, Zhou W L. Security and privacy in 6G networks: new areas and new challenges. Digital Communications and Networks, 2020, 6(3): 281‒291
DOI:10.1016/j.dcan.2020.07.003

10 Lebeck K, Ruth K, Kohno T, Roesner F. Towards security and privacy for multi-user augmented reality: foundations with end users. In: 2018 IEEE Symposium on Security and Privacy. San Francisco, CA, USA, IEEE, 2018, 392‒408
DOI:10.1109/sp.2018.00051

11 Chen D W, Xie L J, Kim B, Wang L, Hong C S, Wang L C, Han Z. Federated learning based mobile edge computing for augmented reality applications. In: 2020 International Conference on Computing, Networking and Communications (ICNC). Big Island, HI, USA, IEEE, 2020,767‒773
DOI:10.1109/icnc47757.2020.9049708

12 Syamimi A, Gong Y W, Liew R. VR industrial applications—A Singapore perspective. Virtual Reality & Intelligent Hardware, 2020, 2(5): 409‒420
DOI:10.1016/j.vrih.2020.06.001

13 Zheng L Y, Liu X, An Z W, Li S F, Zhang R J. A smart assistance system for cable assembly by combining wearable augmented reality with portable visual inspection. Virtual Reality & Intelligent Hardware, 2020, 2(1): 12‒27
DOI:10.1016/j.vrih.2019.12.002

14 González F C J, Villegas O O V, Ramírez D E T, Sánchez V G C, Domínguez H O. Smart multi-level tool for remote patient monitoring based on a wireless sensor network and mobile augmented reality. Sensors (Basel, Switzerland), 2014, 14(9): 17212‒17234
DOI:10.3390/s140917212

15 Li Y, Zheng L, Wang X W. Flexible and wearable healthcare sensors for visual reality health-monitoring. Virtual Reality & Intelligent Hardware, 2019, 1(4): 411‒427
DOI:10.1016/j.vrih.2019.08.001

16 Yin J H, Chng C B, Wong P M, Ho N, Chua M, Chui C K. VR and AR in human performance research—An NUS experience. Virtual Reality & Intelligent Hardware, 2020, 2(5): 381‒393
DOI:10.1016/j.vrih.2020.07.009

17 Kim H, Kwon Y T, Lim H R, Kim J H, Kim Y S, Yeo W H. Recent advances in wearable sensors and integrated functional devices for virtual and augmented reality applications. Advanced Functional Materials, 2021, 31(39): 2005692
DOI:10.1002/adfm.202005692

18 Gulhane A, Vyas A, Mitra R, Oruche R, Hoefer G, Valluripally S, Calyam P, Hoque K A. Security, privacy and safety risk assessment for virtual reality learning environment applications. In: 2019 16th IEEE Annual Consumer Communications & Networking Conference. Las Vegas, NV, USA, IEEE, 2019,1‒9
DOI:10.1109/ccnc.2019.8651847

19 Fun T S, Samsudin A. A survey of homomorphic encryption for outsourced big data computation. KSII Transactions on Internet and Information Systems, 2016, 10(8): 3826‒3851

DOI:10.3837/tiis.2016.08.022

20 Gao W C, Yu W, Liang F, Hatcher W G, Lu C. Privacy-preserving auction for big data trading using homomorphic encryption. IEEE Transactions on Network Science and Engineering, 2020, 7(2): 776‒791
DOI:10.1109/tnse.2018.2846736

21 Wang D, Guo B, Shen Y, Cheng S J, Lin Y H. A faster fully homomorphic encryption scheme in big data. In: 2017 IEEE 2nd International Conference on Big Data Analysis. Beijing, China, IEEE, 2017, 345‒349
DOI:10.1109/icbda.2017.8078836

22 Aono Y, Hayashi T, Phong L T, Wang L H. Privacy-preserving logistic regression with distributed data sources via homomorphic encryption. IEICE Transactions on Information and Systems, 2016, E99.D(8): 2079‒2089
DOI:10.1587/transinf.2015inp0020

23 Esperanca P, Aslett L, Holmes C. Encrypted accelerated least squares regression. Artificial Intelligence and Statistics. 2017

24 Yonetani R, Boddeti V N, Kitani K M, Sato Y. Privacy-preserving visual learning using doubly permuted homomorphic encryption. In: 2017 IEEE International Conference on Computer Vision. Venice, Italy, IEEE, 2017, 2059‒2069
DOI:10.1109/iccv.2017.225

25 Fang H K, Qian Q. Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet, 2021, 13(4): 94
DOI:10.3390/fi13040094

26 Halevi S. Homomorphic encryption. In Tutorials on the Foundations of Cryptography. Springer, Cham, 2017, 219‒276
DOI: 10.1007/978-3-319-57048-8_5

27 Yagoub M A, Laouid A, Kazar O, Bounceur A, Euler R, AlShaikh M. An adaptive and efficient fully homomorphic encryption technique. ICFNDS'18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. 2018, 1‒6
DOI:10.1145/3231053.3231088

28 Yan X Y, Wu Q L, Sun Y M. A homomorphic encryption and privacy protection method based on blockchain and edge computing. Wireless Communications and Mobile Computing, 2020, 8832341
DOI:10.1155/2020/8832341

29 Iezzi M. Practical privacy-preserving data science with homomorphic encryption: an overview. In: 2020 IEEE International Conference on Big Data (Big Data). Atlanta, GA, USA, IEEE, 2020, 3979‒3988
DOI:10.1109/bigdata50022.2020.9377989

30 Pramanik M I, Lau R Y K, Hossain M S, Rahoman M M, Debnath S K, Rashed M G, Uddin M Z. Privacy preserving big data analytics: a critical analysis of state-of-the-art. WIREs Data Mining and Knowledge Discovery, 2021, 11(1): e1387
DOI:10.1002/widm.1387

31 Tran H Y, Hu J K. Privacy-preserving big data analytics a comprehensive survey. Journal of Parallel and Distributed Computing, 2019, 134: 207‒218
DOI:10.1016/j.jpdc.2019.08.007

32 Vijaya K A, Sujith M S, Sai K T, Rajesh G, Yashwanth D J S. Secure Multiparty computation enabled E-Healthcare system with Homomorphic encryption. IOP Conference Series: Materials Science and Engineering, 2020, 981(2): 022079
DOI:10.1088/1757-899x/981/2/022079

33 Li D, Liao X F, Xiang T, Wu J H, Le J Q. Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation. Computers & Security, 2020, 90: 101701
DOI:10.1016/j.cose.2019.101701

34 Hesamifard E, Takabi H, Ghasemi M. Deep neural networks classification over encrypted data. CODASPY'19: Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy. 2019, 97‒108
DOI:10.1145/3292006.3300044

35 Podschwadt R, Takabi D. Classification of encrypted word embeddings using recurrent neural networks. 2020

36 Graepel T, Lauter K, Naehrig M. ML confidential: Machine learning on encrypted data. In International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg. 2012, 1‒21
DOI: 10.1007/978-3-642-37682-5_1

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

DOI:10.1016/j.future.2017.02.006

38 Bost R, Popa R A, Tu S, Goldwasser S. Machine learning classification over encrypted data. In: Proceedings 2015 Network and Distributed System Security Symposium. San Diego, CA, Reston, VA: Internet Society, 2015
DOI:10.14722/ndss.2015.23241

39 Takabi D, Podschwadt R, Druce J, Wu C, Procopio K. Privacy preserving neural network inference on encrypted data with GPUs. 2019

40 Badawi A A, Hoang L, Mun C F, Laine K, Aung K M M. PrivFT: private and fast text classification with homomorphic encryption. IEEE Access, 2020, 8: 226544‒226556
DOI:10.1109/access.2020.3045465

41 Jung W, Kim S, Ahn J H, Cheon J H, Lee Y. Over 100x faster bootstrapping in fully homomorphic encryption through memory-centric optimization with GPUs. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 114‒148
DOI:10.46586/tches.v2021.i4.114-148

42 Hesamifard E, Takabi H, Ghasemi M. Cryptodl: Deep neural networks over encrypted data. 2017

43 Zhao Z P, Bao Z T, Zhang Z X, Cummins N, Sun S H, Wang H S, Tao J H, Schuller B W. Self-attention transfer networks for speech emotion recognition. Virtual Reality & Intelligent Hardware, 2021, 3(1): 43‒54
DOI:10.1016/j.vrih.2020.12.002

44 Li M C, An L, Yu T, Wang Y G, Chen F, Liu Y B. Neural hand reconstruction using a single RGB image. Virtual Reality & Intelligent Hardware, 2020, 2(3): 276‒289
DOI:10.1016/j.vrih.2020.05.001

45 Mishra P, Lehmkuhl R, Srinivasan A, Zheng W, Popa R A. Delphi: A cryptographic inference service for neural networks. In 29th Security Symposium Security. 2020, 2505‒2522

46 Sarmah S S. An efficient IoT-based patient monitoring and heart disease prediction system using deep learning modified neural network. IEEE Access, 2020, 8: 135784‒135797
DOI:10.1109/access.2020.3007561

47 Ge C P, Yin C C, Liu Z, Fang L M, Zhu J C, Ling H D. A privacy preserve big data analysis system for wearable wireless sensor network. Computers & Security, 2020, 96: 101887
DOI:10.1016/j.cose.2020.101887

48 Xu R H, Joshi J B D, Li C. CryptoNN: training neural networks over encrypted data. In: 2019 IEEE 39th International Conference on Distributed Computing Systems. Dallas, TX, USA, IEEE, 2019, 1199‒1209
DOI:10.1109/icdcs.2019.00121

49 Abdalla M, Bourse F, De Caro A, Pointcheval D. Simple Functional Encryption Schemes for Inner Products. Berlin, Heidelberg, Springer Berlin Heidelberg, 2015, 733‒751
DOI: 10.1007/978-3-662-46447-2_33

50 Gilad-Bachrach R, Dowlin N, Laine K, Lauter K, Naehrig M, Wernsing J. CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy. In: Proceedings of the 33rd International Conference on Machine Learning. Proceedings of Machine Learning Research, Edited by Maria Florina B, Kilian Q W. PMLR 2016, 201‒210

51 Bos J W, Lauter K E, Loftus J, Naehrig M. Improved security for a ring-based fully homomorphic encryption scheme. IACR Cryptology EPrint Archive, 2013, 75

52 Halevi S, Shoup V. Algorithms in HElib. Berlin, Heidelberg, Springer Berlin Heidelberg, 2014, 554‒571
DOI: 10.1007/978-3-662-44371-2_31

53 El Saj R, Sedgh Gooya E, Alfalou A, Khalil M. Privacy-preserving deep neural network methods: computational and perceptual methods—an overview. Electronics, 2021, 10(11): 1367
DOI:10.3390/electronics10111367

54 Alkhelaiwi M, Boulila W, Ahmad J, Koubaa A, Driss M. An efficient approach based on privacy-preserving deep learning for satellite image classification. Remote Sensing, 2021, 13(11): 2221
DOI:10.3390/rs13112221

55 Zhang Y S, Xiao X L, Yang L X, Xiang Y, Zhong S. Secure and efficient outsourcing of PCA-based face recognition. IEEE Transactions on Information Forensics and Security, 2020, 15: 1683‒1695
DOI:10.1109/tifs.2019.2947872