Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

A Comprehensive Study of Traditional and Deep-learning Schemes for Privacy and Data Security in the Cloud

Mohammed fawzi Sheet[1] Melad Jader saeed[2]

mohammed.20csp63@student.uomosul.edu.iq[1], Meladjader@uomosul.edu.iq

Article information

Article history:
Received : 8/5/2022
Accepted : 30/6/2022
Available online :

Abstract

After the availability of Internet infrastructure all over the world, and connectivity is no longer an obstacle over the Internet, cloud computing has emerged as a practical and ideal solution. A huge revolution has taken place in the field of cloud computing, where it is now an industry. However, it faces great difficulties in ensuring data confidentiality and privacy. People hesitate to use it due to the risk of innumerable attacks and security breaches. This article has covered a several directions relayed to cloud computing ideas. This research would focus on traditional and deep-learning based schemes to secure user's data in the cloud. This study concluded some points about the capabilities of the traditional and deep learning-based scheme. The comparison showed that both of them increased the levels of security and privacy of the cloud. The study conclude that the Deep learning-based method had been implanted to secure clouds' data in combination with other technique performed better than others.

Keywords:
Cloud computing, deep learning, Biometric, Privacy in cloud computing

Correspondence:
Author :mohammed Fawzy sheet
Email:
mohammed.20csp63@student.uomosul.edu.iq

1. INTRODUCTION (HEADING 1)

Cloud computing is defined as a technology that relies on transforming programs from products to a websites' services. It is characterized by solving problems of program maintenance and development for variety of businesses. It turned information technology programs from products to services by transferring computer processing, storage, and data to the so-called cloud, which is a server device accessed via the Internet. It is characterized by eliminating challenges of program maintenance and development for enterprises. As a result, the beneficiaries' efforts are solely focused on using these services. Thus, cloud computing is defined as a technique that relies on shifting the computer's processing and storage space to the so-called cloud, which is a server device that can be accessed via the Internet. From items to services, information is available. [1]

Cloud computing have many types included in terms of prevalence, the National Institute of Standards and Technology (NIST) has identified four cloud computing models:

A- Public cloud computing
B- Private cloud computing
C- Community cloud computing
D- Hybrid cloud [2]

We can classify the types of services provided by cloud computing as:

A- "Infrastructure as a Service (IaaS)"
B- "Platform as a Service (PaaS)"
C- "Software as a Service (SaaS)"
D- Cloud Computing "Data as a Service (DaaS)"
E- "HARDWARE AS A SERVICE (HaaS)" [3]

Table 1: Different Layers in Cloud Computing

Layer	SaaS	PaaS	IaaS	DaaS	Haas
Application	✓				
Software		✓			
Infrastructure			✓	✓	✓

The cloud computing has the following important issues [4][5][6][7]:

1. Cyber security and security risks: Despite the benefit of multiple data entry points in cloud computing, it faces a significant challenge of security threats pertaining to this data. So, it is preferable to store data of each client in a private server under your own. So, you do not have to worry about data leakage if it is stored on other servers. You may also secure your cloud using "multi-factor authentication" to safeguard it from any attack or security breach.
2. Data migration is difficult: The stage of data migration from conventional to cloud computing is one of the most challenging and time-consuming issues for users. It necessitates a change in management approach.
3. Ability to comply to operational guidelines: As this challenge is currently regarded as one of the most significant, companies are concerned about the future growth of their business and their suitability with cloud computing. As well as the existence of gaps in operational processes and traditional information technology infrastructure. Thus, the nature of the companies' work can be hampered if they do not have the infrastructure.

2. The Related works

Several surveys and comparative studies had been presented to evaluate performance of the recently proposed methods. Those studies relied on the security issues that might be implemented for unauthorized access or data deletion. In this section related works would be discussed to reshape the current study.

(Basu et. Al, 2018), the authors had presented a review of the security schemes that enhanced the security issues of the cloud. the listed comparisons among them according to data confidentiality and virtualization confidentiality of the proposed security of the cloud [i] (Kumar, 2019) had presented a review of the recently proposed solutions that might prevent the unauthorized access to users' data in the cloud. In fact, the reviewed papers focused on the traditional encryption strategies with no pure comparative among them [8]. (Al-Sit, et al., 2019) had presented a review study to evaluate the security issues of several cloud computing systems. the focused on the encryption system that implemented in those cloud systems. Several attacks had been discussed that may prevent unauthorized person to access the users' data. All of these systems do not implement deep learning methods [9]. (Xu, et al. 2019) had presented a review study that dealt with some of cloud computing security issues in deep learning-based clouds. They are attacks, countermeasures and their opportunities [10]. (Balani & Varol, 2020) had presented a survey for the challenges and threats that faced both users and providers of clouds. They listed some of the most important security issues in cloud computing. No comparison among the proposed security schemes at all [11]. (Abdulateef et al., 2020) presented a survey in which machine learning algorithm had been implemented to enhance cloud security. The authors present advantages and dis advantages of each listed paper but no comparison had been presented [12]. (Tariq, et al., 2020) had proposed some important countermeasures to evaluate the risk and challenges of the deep learning-based models that may be vulnerable for several attacks in cloud computing [13]. (Tahirkheli et al., 2021) had presented a survey that dealt with the security of clouds according to several issues. The study listed nine deferent clouds and presented the comparative criteria among them. Only one announce about Deep learning algorithm to prevent malware activities [14]. (Mohammed & Taha, 2021) presented a proximate comprehensive study about homomorphic encryption to enhance the security and privacy of the cloud computing. No deep learning had been listed among the study papers [15]. (Andi, et al., 2021) had presented a review of the implemented methods and systems that are implemented in cloud computing security. They had listed the common clouds and the security methods, they are (blockchain, Deep Learning and Cryptography. Limited information had been reviewed for the deep learning papers with limited criteria [16].

3. The method:

This paper focused on securing the cloud using deep learning schemes. It is one of the very successful methods, especially since the methods of attack are always evolving and changing. It is needed to neural networks that are constantly evolving with every penetration attempt and every attempt to steal data that is stored in the cloud. The researcher also did not ignore the security of the cloud in different ways such as encryption, where the reader has the possibility to compare between the methods and take advantage of the methods that are more successful.

3.1 Works related to deep learning field

In [17], the authors proposed a new deep learning model that based on CNN and RNN to detect intruders in cloud computing security. Their model was trained and tested by NSL-KDD dataset. Using deep learning model allowed to detect unapproved traffic and prevent access to the cloud. The result showed 99.86% accuracy for 5-classes.

In [18], the researchers presented a method to prevent risk in the cloud to quantify level of risk based on fine-grained model in co-residency. A large-scale dataset had

been built and implemented. Data had been collected via Microsoft Azure Platform. The method proposed some features to describe the patterns of normal subscribers (tenants) behavior. The Tenants are clustered into multiple categories by using DBSCAN algorithm and MinPts algorithm. Then, Deep Neural Network (DNN) is implemented to detect high-risk group according to quantification of risk component and control normal behavior pattern among the Tenants. The results showed the robustness of the proposed model specially with new data. Its accuracy was between (94-98%) and F-score were (0.99, 0.773 and 0.609) for Normal, Periodically Active and Extremely Active respectively.

In [19], the authors implemented the Distributed Deep Learning DDL to enhance the security of the fog-cloud computing with preserving privacy. The proposed scheme based on a trusted authority that provides parameters and public keys. Then, users' authentication would be performed and local gradient uploaded the out put of CNN would be distributed on users. It is similar to other works and it is promising scheme.

In [20], a modified Distributed Deep Learning (DDL) had been implemented in fog-cloud computing environments. The authors proposed Secure and Privacy-Preserving deep learning (SPDDL) fog-cloud computing. The SPDDL had been implemented Trusted Authority (TA) to provide private and public keys for the encryption algorithm. The results showed that the proposed method granted the privacy of users' information and a perform a secured authentication by adding more complexity to the key generation in comparing with other DDL algorithms.

In [21], the authors had improved the authentication process in the cloud computing by implementing Iris as biometric authentication. The pro

posed authentication is based on to neural network model, CNN for features' extraction and MLP for iris feature matching. The authentication was performed in the cloud. The results sowed that the proposed models preformed good according to the time.

In [22], Authors presented a new framework to secure health-care systems that include huge private information about users. MSCryptoNet is proposed to secure the information via implementing the Convolutional Neural Network (CNN) in Key generation. The CNN improved the encryption system of the framework that aims to implement classifier in deferent encryption scheme and minimize the computational and communication cost. The results showed that the proposed frame work had high performance and CNN may be used in another encryption scheme.

In [23], the authors presented a Long Short-Term Memory (LSTM) based system to monitor the network traffic. This would allow to notice and detect the abnormal network traffic. In fact, it is a promising idea that enhance the security of the cloud via extracting features from the network traffic.

In [24], the authors proposed four deep learning models to detect the DDoS attack on the cloud. CNN, LSTM MLP and CCN+LSTM are implemented and compared with machine learning algorithms. The proposed models had less level of performance than the machine learning algorithms except the CNN+LSTM that had high performance level. This model may enhance the cloud security against DDoS attack.

In[25], the authors proposed Intrusion Detection Systems (IDS) in cloud computing security to detect some types of attacks. In which, the IDS can get information about other suspected attack from other IDSs then made a decision using the aggregation algorithm. This matter increased execution time. Therefore. Denoising Autoencoder (DA) is used to build block to construct a deep neural network. The results showed that the system had 95% of accuracy.

In [26], the authors presented a detection method for anomaly traffic in the cloud that based on combination of two deep learning models: CNN and Gray Wolf Optimizer GWO. Those models detect abnormal traffic in a cloud datacenter. The result showed that the proposed method had improve the accuracy of anomaly detection that reach to 8% in compared with other metods.

In [27], the authors proposed a Privacy-Preserving Deep Learning Model (PDLM) to add multiple keys to the encryption system in the cloud. The initial optimization of data had been done by Stochastic Gradient Descent (SGD) to normalize the users' data. The PDLM determine extract the perfect Tylor Series that implemented to calculate the accuracy and weight. Both private and public key for each user would be produced based on fit series that discovered by PDLM. The results showed that PDLM is effective and efficient.

In [ii], the authors proposed a deep learning model that implemented to evaluate the security parameters of a multi-party cloud system. This model encrypted the databases of the users locally then preform the CNN to extract the security features of the hole databases. In fact, it is mater of evaluation not an enhancement.

In [iii], the authors presented a scheme based on Privacy-Preserving Machine Learning to generate multiple keys for each user of the cloud. Firstly, users' data had been optimized by SGD. the optimized data used in keys

generation by Privacy-Preserving Machine Learning. Users' data had been encrypted by two encryption systems. they are "Multi-Key Fully Homomorphic Encryption (MK-FHE)" and "the double decryption mechanism with Fully Homomorphic Encryption" (FHE). The results showed that both proposed schemes are efficient but the second scheme needed interaction among the users.

3.2.Work relate to cloud Security field:

Many researchers had developed and presented their proposed schemes that based on developed and recently proposed encryption algorithms. These algorithms did not implement neither Deep learning nor machine learning methods. The following are some of these studies.

In [iv], the author proposed a complex encryption system based on both symmetric and asymmetric encryption systems. A Blowfish block cipher as a symmetric encryption had been used in combination with ECC as asymmetric encryption. The blowfish encrypt the data then, ECC would encrypt the key of Blowfish. This proposal is suppose to increase the security of the user data.

While In[v], the author proposed an effective approach based on homomorphic encryption that implemented in banking application. The approach relies on encoding the bank's data then, it may be transmitted securely to the cloud. This approach may be used with confidential data.

In [vi], the authors presented a scheme based on two concepts. Firstly, the user verification would be performed by depending fingerprint to authenticate user. Secondly, encryption process which is based on One-Time-Password (as secret key) that had been exchanged between the cloud server and user by which AES block cipher used this secret key to encrypt/decrypt the user's data. The results showed that implementing biometric is a good solution for cloud security.

For the security of cloud computing, in this research, a hybrid verification technique is made which is based on biometric and encryption systems. In order to achieve strong and secure technique, this work uses fingerprint as biometric technique and advanced encryption standard as a trustworthy encryption system. The primary goal of this paper is to avert information access from cloud information stockpiling focuses by unapproved clients. This new data security system can provide efficient authentication of cloud computing.

Data is a collection of information that is combined into one and has a very important meaning. In the study, the object to be secured is the password data , the encryption method Advanced Encryption Standard (AES) with a key length of 256 bits, before the data is encrypted with method of AES, the first password will be encrypted using MD5 , and the second one will be encrypted again using the AES256 method. Based on trial data conducted through two sites about the complexity of passwords, it can be concluded that the original data (before encryption) no 1 to 5 increased to 32 bytes after being encrypted by the MD5 method, and its size increased again to 88 bytes after being encrypted by the AES256 method. Data can be obtained by value original data AES256 is 9, 96 times larger than its original size, would be but the value of the complexity of her also increased in line with the increase in the number of characters or the byte size of the data password above, thereby increasing the level of difficulty by the party that will hack the login data in the cloud.

In [vii], the authors proposed a combination of encryption system to encrypt passwords during authentication. Their proposal based on encrypting password by MD5 encryption then re-encrypted by AES. The store password of the cloud is encrypted using AES too. This scheme can protect password of the user and added more complexity.

In [viii], The authors proposed a backend application to provide immediate solution to prevent unauthorized access to the cloud. Footprint Notifications, Logging Encryption and activities of the authenticated users had been used to authenticate the user access. It is similar to behavior detection but it used events of the cloud to authenticate user.

In[ix], the authors proposed an enhancement for cloud security. Two steps had been performed. Firstly, the users' data would be encrypted by AES with it private key, then the AES key would be encrypted by Elliptic Curve Cryptography (ECC). Secondly, the encrypted key would be hide in a user image by HLSB algorithm of steganography. The implementation of the second encryption secured the AES key which is embedded in an image. This prevents eavesdroppers to get the private key.

In [x], the authors enhanced scheme that implemented Fingerprint as biometric to the identification phase of the scheme. Basically, the proposed scheme is called B^2EIS-RG. It consists of two phases. Firstly, a key generation had been performed by DIV to determine the multi keywords among the huge data of the users in a cloud. The key generation depended on the extracted keywords. Then, Paillier cryptosystem had been implemented to encrypt users' data. In the identification phase, the fingerprint features had been extracted and converted to vectors. These vectors had been encrypted during the Identifying process. The results showed that depending on vectorized biometric features reduced the required space to save biometric images and granted authenticated access to the user' data.

In [xi], the authors proposed a security scheme to protect the medical records in a public server that are connected to several medical institutes. The idea of their proposal based on additional cloud security scheme that allows access for the authenticated institutes. The user data had been encrypted by Shamir's Secret Share (SSS). The proposed scheme allows whole institute to share medical data via Virtual private Network VPN. The results showed that the security scheme preform better than other schemes.

In [xii], the authors enhanced the security of cloud computing by allow Third Party Auditor (TPA) which can

check the integrity of users' data. Data check would be performed in the cloud on behalf of the users. In this scheme, when a user tried to check the integrity of his stored data, he would send a request to the check from TPA. The TPA requested the signature of the user data from the cloud server. The server built a signature for the user data. A hash code is implemented to match both of TPA and server signatures to preform data check. The results showed that the TPA checked the user's data without knowing any details about it.

In [xiii], the authors presented a complicated secured scheme that consisted of three phases. Firstly, the enrolment phase in which the user's data and fingerprint had been encrypted by RSA key of the server then sent to a third-party server. The third part server decrypted data by RSA. The key and fingerprint template had been encrypted by AES and stored in the cloud. In Authentication Phase, user provided his user-name, password and fingerprint. they all would be encrypted by RSA then send to the third-party server. The user authentication data decrypted from the cloud by AES to be compared with the provided data. If they matched, the scheme granted access. If not, access would be denied. In the Data protection phase, the key and fingerprint would be encrypted by 3DES then the user's data would be encrypted by Blowfish. After saucerful authentication, the third party would decrypt the key and the fingerprint template by 3DES then the key would be decrypted by Blowfish. The results showed that the complexity of proposed design granted high security for the cloud users.

In [xiv], the authors proposed a security model based on AES encryption system to encrypt the transmitted data. The proposed model had been implemented in the Heroku, as a cloud platform of (PaaS) type. The author concluded that the AES encryption needed more time to perform encryption and decryption processes.

In [xv], the authors presented fully data encryption in the cloud. The idea based on encryption of the data before user sends it to the cloud. The implemented encryption system was AES as a robust encryption. The proposed scheme provided cloud security and user privacy. It also reduced the noise of encryption in the cloud.

Both of the deep learning based and the traditional schemes had been illustrated in table1 and 2. The common countermeasures had been discussed for each presented work in each category.

The deep learning-based scheme had some countermeasures that can be listed as a promising idea for further enhancement of security of the cloud computing. They consist of strategy, Deep learning techniques, other requirements, goals and achievements as shown in table 1.

Table 1. The Deep learning-based papers countermeasure.

No.	strategy	Deep learning techniques	other requirements	goals	Achievements
18	Anomaly traffic	CNN RNN	-	Detect abnormal network traffic by CNN and RNN to extract traffic features and prevent the anomaly traffic	The scheme had 99.86% of accuracy
19	Abnormal behavior	DNN	DBSCAN MinPts	Prevent abnormal activities	The scheme had 94 - 98% of accuracy
20	Preservin g privacy	DLL CNN	Parameter and public key providing	Provides trusted Authority	Secure fog cloud
21	Preservin g privacy	SPDDL	Public key providing	Provides trusted Authority	Secure fog cloud
22	Biometric Uthenticat ion	CNN MLP	Iris biometric	More secured authentication	preformed good according to the time
23	Preservin g privacy	CNN classifier	Key generation	Maintain privacy of health care cloud	preformed good with high privacy
24	Anomaly traffic	LSTM	network traffic's feature	Detect abnormal network traffic by LSTM	preformed good
25	Anomaly traffic	CNN LSTM MLP CCN+LST M	Machine learning methods network traffic's feature	enhance the cloud security against DDoS attack	The machine learning performed better than deep learning but the combination of CCN+LSTM is performed better than all.
26	Anomaly traffic	Denoising Autoencoder	aggregation	Build Intrusion Detection Systems for the cloud computing	The scheme has 95% of accuracy
27	Anomaly traffic	CNN + Gray Wolf	-	detect abnormal traffic in a cloud datacenter	More accuracy reaches to 8%.

		Optimizer			
28	Preservin g privacy	PDLM	Tylor Series Private and public key	add multiple keys to the encryption system in the cloud	PDLM is effective and efficient
29	Preservin g privacy	CNN	the security features of the hole databases	Enhance privacy of the cloud based on whole data	Evaluate the performance for the features.
30	Preservin g privacy	CNN SGD	MK-FHE DFHE	Secured Users' data	More interaction of users is needed

The illustrated papers above are mostly delt with preserving privacy of users' data and anomaly traffic in the cloud computing. Just one paper delt with biometric authentication and on paper delt with user's behavior. Most of the papers implement CNN with other deep learning algorithms. The combination had performed better than CNN based scheme alone. Deferent encryption system had been used to encrypt user's data. The listed achievements may enhance the privacy and security and trusted authentication process.

The traditional schemes are illustrated in table 2. Another two countermeasures had been used. The main method and the auxiliary methods instead of the Deep learning method and other requirements.

Table 2. The Traditional paper based countermeasure.

No.	strategy	main method	auxiliary methods	goals	Achievements
31	Encryption	Blowfish ECC	-	Dual encryption to secure data in th cloud	Increase the complexity of the key that used to encrypt the data
32	Encryption	Paillier	key homomorphic	Secure the banking application	Performed good to be implemented in confidential data
33	Biometric authentication	fingerprint	AES MD5 One-Time-Password	Secure the cloud authentication	Implementing finger print biometric in cloud authentication
34	Encryption	AES MD5	Password	Password encryption	added more complexity
35	Abnormal behavior	Backend application	Cloud event	Prevent unauthorized access	Add robust authentication
36	Encryption	AES ECC	HLSB	Secure data and hide keys	Secured the primary key
37	Biometric authentication	fingerprint	Paillier	Enhance the authentication	Improve authentication Huge image number
38	Encryption	Shamir's Secret Share (SSS)	VPN	Secure health care cloud	Added more security to the health care cloud
39	Signature authentication	Hash code	Third Party Auditor	Secure cloud	No additional information were required
40	Biometric authentication	fingerprint	RSA AES Blowfish 3DES	Secure fingerprint and encryption key	Secured the finger print and encrypted data.
41	Encryption	AES	-	Secure data in the cloud	Data had been secured but more time is required
42	Encryption	AES	Whole data of the cloud	Secure whole data in the cloud	Reduced the noise and increase privacy

The authors proposed encryption scheme in most of the papers, while some other proposed biometric authentication. Signature authentication and abnormal behavior had been proposed one paper for each. Double encryption schemes had a good implementation as well as whole data encryption but they require more time. Biometric authentication is a good solution based on extracted string.
Both schemes are implemented in deferent fields and businesses because of their high performance.

5. CONCLUSION

Cloud computing has emerged as a practical and optimal solution following the availability of Internet infrastructure in various parts of the world, and the issue of communication does not constitute an impediment to touching the cloud, specially, in light of the massive increase in smartphone issuance, which always carry with it the characteristics of Internet connection and the ability to deal with a wide range of data and files over the network, particularly multimedia, and one of the most significant challenges confronting the cloud computing system are security and privacy, where there is concern about confidentiality violations. Both of traditional and deep learning- based schemes had the capability to increase the levels of data security and privacy. It is obvious that biometric based schemes had met the deep-learning schemes in their capabilities. Behavior strategies can offer more security to the cloud to prevent unauthorized access. While the privacy issue had great interest in the cloud's data privacy. Deep learning-based method had been implanted to secure clouds' data in combination with other technique performed better than others.

Reference

[1] Borangiu, T., Trentesaux, D., Thomas, A., Leitão, P., & Barata, J. (2019). Digital transformation of manufacturing through cloud services and resource virtualization. Computers in Industry, 108, 150–162.

[2] P. Bhuvaneshwari "Cloud Computing Types and Associated Challenges" IJIRT | Volume 2 Issue 7 | ISSN: 2349-6002 IJIRT 150539 International Journal of Innovative Research In Technology 15. © December 2015.

[3] Ahmad, S., Mehfuz, S., & Beg, J. (2020, December). Securely work from home with CASB policies under COVID-19 pandemic: a short review. In 2020 9th International conference system modeling and advancement in research trends (SMART) (pp. 109-114). IEEE.

[4] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing.

[5] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal, 1(2), 1-7.

[6] Balaji, K. (2021). Load balancing in cloud computing: issues and challenges. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(2), 3077-3084.

[7] Thabit, F., Alhomdy, S. A. H., Alahdal, A., & Jagtap, S. B. (2020). Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques. Journal of Information and Computational Science, 12(10).

[8] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE.

[9] Kumar, G. (2019). A review on data protection of cloud computing security, benefits, risks and suggestions. PDF). United International Journal for Research & Technology, 1(2), 26.

[10] Al-Sit, W. T., Al-Jubouri, Q., & Al-Zoubi, H. (2019). Cloud Security based on the Homomorphic Encryption. International Journal of Advanced Computer Science and Applications, 10(8).

[11] Xu, G., Li, H., Ren, H., Yang, K., & Deng, R. H. (2019). Data security issues in deep learning: attacks, countermeasures, and opportunities. IEEE Communications Magazine, 57(11), 116-122.

[12] Balani, Z., & Varol, H. (2020). Cloud Computing Security Challenges and Threats. 2020 8th International Symposium on Digital Forensics and Security (ISDFS).

[13] Abdulateef, A. A., Mohammed, A. H., & Abdulateef, I. A. (2020, October). Cloud Computing Security For Algorithms. In 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-5). IEEE.

[14] Tariq, M. I., Memon, N. A., Ahmed, S., Tayyaba, S., Mushtaq, M. T., Mian, N. A., ... & Ashraf, M. W. (2020). A review of deep learning security and privacy defensive techniques. Mobile Information Systems, 2020.

[15] Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R.,& Kim, K. I. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. Electronics, 10(15), 1811.

[16] Mohammed, S. J., & Taha, D. B. (2021). From cloud computing security towards homomorphic encryption: A comprehensive review. TELKOMNIKA (Telecomm unication Computing Electronics and Control), 19(4), 1152-1161.

[17] Andi, H. K. (2021). Estimating the Role of Blockchain, Deep Learning and Cryptography algorithms in Cloud Security. Journal of Trends in Computer Science and Smart Technology, 3(4), 305-313.

[18] Hizal, S., ÇAVUŞOĞLU, Ü., & AKGÜN, D. (2021, June). A New Deep Learning Based Intrusion Detection System for Cloud Security. In 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-4). IEEE.

[19] Jin Han, Wanyu Zang, Meng Yu and Ravi Sandhu "Quantify Co-Residency Risks in the Cloud through Deep Learning" 1545-5971 (c) IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission 2020.

[20] Li, Y., Li, H., Xu, G., Xiang, T., Huang, X., & Lu, R. (2020). Toward secure and privacy-preserving distributed deep learning in fog-cloud computing. IEEE Internet of Things Journal, 7(12), 11460-11472.

[21] Y. Li, H. Li, G. Xu, T. Xiang, X. Huang, R. Lu, "Secure and Privacy-Preserving Distributed Deep Learning in Fog-Cloud Computing " 10.1109/JIOT. 3012480, IEEE Internet of Things Journal 1 Towards 2020.

[22] Sudhakar, T., & Gavrilova, M. (2020). Cancelable biometrics using deep learning as a cloud service. IEEE Access, 8, 112932-112943.

[23] Owusu-Agyemang Kwabena, Zhen Qin, Tianming Zhuang, and Zhiguang Qin, "MSCryptoNet: Multi-Scheme Privacy-Preserving Deep Learning in Cloud Computing"2169-3536 VOLUME 7, IEEE, 2019.

[24] Lin, P., Ye, K., & Xu, C. Z. (2019, June). Dynamic network anomaly detection system by using deep learning techniques. In International conference on cloud computing (pp. 161-176). Springer, Cham.

[25] Roopak, M., Yun Tian, G., & Chambers, J. (2019). Deep Learning Models for Cyber Security in IoT Networks. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC).

[26] Abusitta, A., Bellaiche, M., Dagenais, M., & Halabi, T. (2019). A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Future Generation Computer Systems.

[27] Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2019). A hybrid deep learning-based model for anomaly

detection in cloud datacenter networks. IEEE Transactions on Network and Service Management, 16(3), 924-935.
[28] Xindi Ma, Jianfeng Ma, Hui Li, Qi Jiang and Sheng Gao "PDLM: Privacy-Preserving Deep Learning Model on Cloud with Multiple Keys" IEEE, June 15,2018.
[29] Ma, X., Zhang, F., Chen, X., & Shen, J. (2018). Privacy preserving multi-party computation delegation for deep learning in cloud computing. Information Sciences, 459, 103-116.
[30] P. LI, J. Li. Z. huang, T. Li, Ch. Gao, S. Ming, K. Chen Multi-key privacy-preserving deep learning in cloud computing. Future Generation Computer Systems, 2017.
[31] Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, 12(6).
[32] Altaee, M. M. S. (2021) Developing A cloud-based banking application using Paillier Homomorphic encryption. MSc thesis, Computer sciences, University of Mosul.
[33] Hossain, M. A., & Al Hasan, M. A. "Improving cloud data security through hybrid verification technique based on biometrics and encryption system". International Journal of Computers and Applications, 1–10. 2020.
[34] Khakim, L., Mukhlisin, M., & Suharjono, A. (2020). Security system design for cloud computing by using the combination of AES256 and MD5 algorithm. In IOP Conference Series: Materials Science and Engineering (Vol. 732, No. 1, p. 012044). IOP Publishing.
[35] Olowu, M., Yinka-Banjo, C., Misra, S., & Florez, H. (2019, November). A secured private-cloud computing system. In International Conference on Applied Informatics (pp. 373-384). Springer, Cham.
[36] Hosam, O., & Ahmad, M. H. (2019). Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. Int. J. Comput. Sci. Eng., 19(2), 153-161.
[37] Sudharani , Sakthivel N. , and Subasree S. "Biometric-based Bucket Encrypting Index Structure with Random Generator" International Journal of Advanced Trends in Computer Science and Engineering Volume 8, No.2, March - April 2019.
[38] Marwan, M., AlShahwan, F., Sifou, F., Kartit, A., & Ouahmane, H. (2019). Improving the Security of Cloud-based Medical Image Storage. Engineering Letters, 27(1).
[39] Bincy J., and Thejaswi A.. "Privacy-Preserving External Auditing for Data Storage Security in Cloud". IJRET: International Journal of Research in Engineering and Technology, Volume: 03 Issue: 04 | Apr-2018.
[40] ArunPrakash, R., T. Jayasankar, and K. VinothKumar. "Biometric encoding and biometric authentication (BEBA) protocol for secure cloud in m-commerce environment." Appl. Math. Inf. Sci 12.1 (2018): 255-263.
[41] Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018, April). Data security in cloud computing using AES under HEROKU cloud. In 2018 27th wireless and optical communication conference (WOCC) (pp. 1-5). IEEE.
[42] Alkady, Y., Farouk, F., & Rizk, R. (2018). Fully Homomorphic Encryption with AES in Cloud Computing Security. Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2018, 370–382.

دراسة شاملة لمخططات التعلم التقليدية والعميقة للخصوصية وأمن البيانات في السحابة

محمد فوزي شيت[1] و ميلاد جادر سعيد[2]
جامعة الموصل - العراق
mohammed.20csp63@student.uomosul.edu.iq[1],
Meladjader@uomosul.edu.iq[2]

تاريخ الاستلام:8/5/2022 **تاريخ القبول:30/6/2022**

الملخص

ظهرت الحوسبة السحابية كحل عملي ومثالي بعد توفر البنية التحتية للإنترنت في جميع أنحاء العالم، كما لم يعد الاتصال عقبة على الإنترنت. فقد حدثت ثورة هائلة في مجال الحوسبة السحابية، إذ أصبحت الآن صناعة رائجة. ومع ذلك، فإنه يواجه صعوبات كبيرة في ضمان سرية البيانات وخصوصيتها. وعليه يتردد الناس في استخدامه بسبب مخاطر الهجمات والخروقات الأمنية التي لا حصر لها. لقد غطت هذه الدراسة عدة توجهات تم عرضها لأفكار الحوسبة السحابية. سيركز هذا البحث على المخططات التقليدية والقائمة على التعلم العميق لتأمين بيانات المستخدم في السحابة. خلصت هذه الدراسة إلى بعض النقاط حول قدرات النظم التقليدية والنظم القائمة على التعلم العميق. تشير المقارنة أن استخدام كلا النوعين من النظم يؤدي إلى زيادة مستويات الأمان والخصوصية على السحابة. واستنتجت الدراسة أن نماذج الاعمال المعتمدة على التعلم العميق مع التقنيات الأخرى حققت أداء افضل من الطرق الأخرى.

الكلمات المفتاحية: الحوسبة السحابية ، التعلم العميق ، المقاييس الحيوية ، الخصوصية في الحوسبة السحابية