Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

Estimating the Role of Blockchain, Deep Learning and Cryptography algorithms in Cloud Security

Hari Krishnan Andi

Centre for Postgraduate Studies, Asia Metropolitan University, Malaysia

E-mail: hari.andi@amu.edu.my

Abstract

Cloud network has become very popular in recent days due to its accessibility merits. The data stored in the cloud environment are accessible by the clients from any location. A reliable shielding approach will protect the data stored in the cloud from the hackers and malwares. Blockchain is one of the recent technologies implemented to the cloud network for storing the location of the saved data in an encrypted ledger format. This saves the stored data location without exploring it to the hacker's algorithm. Hence the hacking algorithm fails by not knowing the location to be targeted. Deep learning is an advanced technique developed to act like that of the human neurological analysis on several problems. Implementation of deep learning algorithm to the cloud security module identifies the movement of malware and spywares in the cloud storage. Similarly the cryptography is an old technique structured to hide the information with a cover data or cover image. It allows the hacking algorithm to extract only the useless data. This paper reviews the recent advancements in the cloud security with blockchain, deep learning and cryptographic models.

Keyword: IoT, BAAS, Shared Cloud, Cloud Data Processing, Secure Data

1. Introduction

The data which are stored in remote place are represented as cloud storage. The cloud storage systems are even utilized to do manipulation and algorithmic operation in its own place. For that a remote server is connected to the cloud storage. Based upon the utilization of space from the cloud environment a nominal amount will be collected from the user. The storage space in cloud environment are usually very large and that to be segregated into different piece for different user. In general, the cloud storage systems are categorized into three types as public, private and hybrid cloud.

DOI: https://doi.org/10.36548/jtcsst.2021.4.006
Received: 28.03.2022, received in revised form: 25.04.2022, accepted: 10.05.2022, published: 19.05.2022

1.1 Private Cloud

The private cloud is a system that gives a dedicated storage space for each user and that can't be accessed by the other users. The private cloud systems are employed in the application that requires a customized secure process and computing. The user also has a choice to install or upgrade their hardware and software modules in the private cloud system and the visibility of the data to the user is very high in this system. The data that are computed from the cloud system have very larger speed of operation and it reduces the computation burden to the local storage system. Hence the performances of the private cloud systems are predictable. Similarly the cost requirement for maintaining such system is also limited and predicted as the system is not going to expand at any requirement.

1.2 Public Cloud

Public clouds are the storage space open to all public for accessing the available space for their workstation. Public clouds acts like a shared platform, that allows the same storage system for all the users. The public clouds are operated by corporates, universities and government organizations by collecting a nominal fee from the user based on their usage. Google cloud, Microsoft Azure are one of the major examples of the public cloud systems.

1.3 Hybrid Cloud

Hybrid cloud is a combination of both public and private cloud for ensuring a smooth computation process. In general, the data that can be operated without care will be processed in the public cloud and the data that needs more attention will be processed in the private cloud. By applying the hybrid cloud to the system, the corporates can save their expenses on managing the data. Also it provides more security than the public cloud system and more operating efficiency than the private cloud system.

1.4 Community Cloud

Community cloud is the system that allows several organizations to share their work place on the same cloud environment. In general the community cloud systems are utilized by the government organizations or the corporates that have more than one company for the operations. The community cloud systems are more flexible and easy to share information among their own concerns. It also reduces the cost by avoiding a separate cloud system for each company. However, the community cloud systems are costly than the public cloud

systems. Table 1 explores the merits and demerits of each cloud system based on their operating nature.

Table 1. Performance analysis of various cloud systems

Cloud System	Merits	Demerits
Public Cloud	• Low cost • Open to all locations • Scalability • Easy to setup	• Poor security • Performance related to internet • Not customizable
Private Cloud	• Secure • High privacy • Better performance	• High cost • Restricted operation • Minimum scalability
Hybrid Cloud	• Secure and flexible • Cost effective • Risk management	• Networking issues • Poor service reliability • Questionable compatibility
Community Cloud	• Cost effective • Data Sharing • Secured infrastructure	• Slow data adoption • Fixed storage space • Not suitable for all

2. Related Work

2.1 Blockchain

The cloud system that are managed and operated by a third-party security system using blockchain technology is represented as BaaS (Blockchain as a Service). BaaS acts like a hosting service of a cloud system that secures the data from its back end. The architectural view of BaaS is shown in Figure 1. Here the information available in the cloud system are incorporated to the users through a blockchain system, that stores the information of data access by the users in an encrypted digital form. This ensures the accessibility of the data by other users connected to the same cloud systems. BaaS systems are very suitable for public and community based cloud systems that allows the users to use only their required data. Though the BaaS based cloud architectures are costly in nature and that needs trained people for monitoring and operational control.

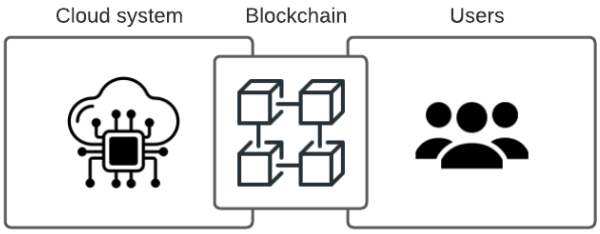

Figure 1. Architecture of a BaaS

2.2 Deep Learning Algorithms

Deep learning algorithms are implemented to the cloud system for detecting the movement of vulnerabilities inside the cloud system. The deep learning algorithms are working based on the human neurological manner and that requires huge amount of data for its training process. The recent year deep learning algorithms are very efficient in detecting the vulnerabilities as they are trained with large quantity of different form of vulnerable data. The deep learning algorithms are also employed in the cloud system for categorizing the data into the allocated storage plot. In some cases the deep learning approaches are designed to segregate and identify the users based on their activity for improving the performances of the cloud operations.

2.3 Cloud Cryptography

Cloud cryptography is a system of encryption that safes the data from the attacks through cryptographic technology. The cryptography technologies are very efficient in addressing the issues related to hacking, breaching and malware activity. However, it is not possible to directly encrypt the data of the cloud server from a remote place. Therefore an in-built coding algorithm is placed over the cloud system for encryption. Symmetric key, asymmetric key and hashing are the three major algorithms employed for cloud encryption designs.

The symmetric key algorithm employs a same key for its operation and encryption and decryption process, where it uses a two way key model for verification and approval when it requires. The blowfish, advanced encryption standard and data encryption standard are the examples symmetric key algorithms. Asymmetric key algorithm uses separate keys for encryption and decryption. Hence the decryption key acts like a private key for the users to decode their data at the time of retrieval. Rivest Shamir Adleman Algorithm (RSA) and Elliptic Curve Cryptography (ECC) are the examples of asymmetric keys that improves the

security nature of the cloud system. Table 2 represents the attainments of various technologies in cloud security systems.

Table 2. Cloud security model and its attainments

First Author & Citation	Methodology	Technique	Application	Achievements
Li [1]	Blockchain	Merkle Hash Tree using the hashtags	Public auditing	Addresses 51% of malicious attacks
Wang [2]	Blockchain	Smart contract technique	Fair payment	Reduces the operational time
Wang [3]	Blockchain	Ciphertext-policy attribute-based encryption	Access control	1000ms runtime for 20 attributes
Ren [4]	Blockchain	Identity-based proxy aggregate signature	Smart homes	Performance improved by 20% over the regular blockchain models
Zhang [5]	Blockchain	multi-cloud storage data auditing scheme	Data auditing	Improves arbitration and restricts malicious activity with lesser computational time
Agarwal [6]	Deep learning	Feature selection-whale optimization algorithm-deep neural network	DDOS attack detection	95.35% of accuracy
Yaseen [7]	Deep learning	Hyper-parameter Tuning	Cloud video analytics	97% accuracy and 96% precision
Yan [8]	Deep learning	Retrieval and storage-based indexing framework	Healthcare data processing	0.066 seconds of mean retrieval time

Mohiyuddin [9]	Deep learning	Neuro fuzzy with SVM	Medical IoT data	29000 data observed per second
Lie [10]	Deep learning	Combination of cloud, caching and distributed file systems	Obstetric Imaging Diagnostic	Completes 4501cache records in 337ms
Chinnasamy [11]	Cryptography	Hybrid model using ECC and Blowfish	Data security	Encryption time = 1.523S/ data Decryption time = 1.287S/data
Sumathi [12]	Cryptography	Modified random Fibonacci	Attribute protection	8.83MB space required for key generation and requires 3.2ms for 7 key generation
Saeed [13]	Cryptography	Combination of AES, ECC and RSA	3 layer security model	Average encryption time = 186.8ms Average decryption time = 114.8ms
Adee [14]	Cryptography	RSA and AES with identity-based encryption algorithms alongside Least Significant Bit steganography	4 step data security	1.3seconds for message encryption and 7.3seconds for cover image process
Sandhia [15]	Cryptography	Multi-Authority Ciphertext Policy Attribute Based Encryption with Elliptic Curve Cryptography	Secure data sharing	Encryption time = 200ms for 10 attributes Decryption time = 210ms for 10 attributes

3. Discussion

Cloud security is a combination of data security and infrastructure security. Blockchain and cryptographic algorithms are directly related to the data security and in certain cases it has been found that such technologies are implemented to infrastructure security also. Infrastructure security is a process of safe guarding the hardware and software systems available in the cloud environment. Deep learning algorithms are found very efficient in handling the malicious nodes and malwares while attacking the data and the cloud infrastructures. A combination of deep learning algorithm with blockchain or cryptography algorithm will improve the combined security issues of the cloud infrastructure.

4. Conclusion

Cloud data sharing has become very popular in recent days as it allows the users to utilize a greater number of storage spaces than the regular storage system. However, security has become questionable for cloud systems as more users access the data from a same cloud system. To avoid this, certain organizations employ private cloud environments. Even such private cloud environments are open to vulnerability attack from the hackers. Hence certain hybrid and multi layered security algorithms are developed to address such issues. This paper analyzes the architectural difference among different cloud models and explores the techniques designed based on blockchain, deep learning and cryptography methodologies on addressing the cloud security issues.

References

[1] Li, Jiaxing, Jigang Wu, Guiyuan Jiang, and Thambipillai Srikanthan. "Blockchain-based public auditing for big data in cloud storage." Information Processing & Management 57, no. 6 (2020): 102382.

[2] Wang, Hao, Hong Qin, Minghao Zhao, Xiaochao Wei, Hua Shen, and Willy Susilo. "Blockchain-based fair payment smart contract for public cloud storage auditing." Information Sciences 519 (2020): 348-362.

[3] Wang, Shangping, Xu Wang, and Yaling Zhang. "A secure cloud storage framework with access control based on blockchain." IEEE access 7 (2019): 112713-112725.

[4] Ren, Yongjun, Yan Leng, Jian Qi, Pradip Kumar Sharma, Jin Wang, Zafer Almakhadmeh, and Amr Tolba. "Multiple cloud storage mechanism based on

blockchain in smart homes." Future Generation Computer Systems 115 (2021): 304-313.

[5] Zhang, Cheng, Yang Xu, Yupeng Hu, J. Wu, Ju Ren, and Yaoxue Zhang. "A blockchain-based multi-cloud storage data auditing scheme to locate faults." IEEE Transactions on Cloud Computing (2021).

[6] Agarwal, Ankit, Manju Khari, and Rajiv Singh. "Detection of DDOS attack using deep learning model in cloud storage application." Wireless Personal Communications (2021): 1-21.

[7] Yaseen, Muhammad Usman, Ashiq Anjum, Omer Rana, and Nikolaos Antonopoulos. "Deep learning hyper-parameter optimization for video analytics in clouds." IEEE Transactions on Systems, Man, and Cybernetics: Systems 49, no. 1 (2018): 253-264.

[8] Yan, Shengguang, Lijuan He, Jaebok Seo, and Minmin Lin. "Concurrent healthcare data processing and storage framework using deep-learning in distributed cloud computing environment." IEEE Transactions on Industrial Informatics 17, no. 4 (2020): 2794-2801.

[9] Mohiyuddin, Aqsa, Abdul Rehman Javed, Chinmay Chakraborty, Muhammad Rizwan, Maryam Shabbir, and Jamel Nebhen. "Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system." International Journal of Fuzzy Systems 24, no. 2 (2022): 1203-1215.

[10] Lie, Weiwei, Bin Jiang, and Wenjing Zhao. "Obstetric imaging diagnostic platform based on cloud computing technology under the background of smart medical big data and deep learning." IEEE Access 8 (2020): 78265-78278.

[11] Chinnasamy, P., S. Padmavathi, R. Swathy, and S. Rakesh. "Efficient data security using hybrid cryptography on cloud computing." In Inventive Communication and Computational Technologies, pp. 537-547. Springer, Singapore, 2021.

[12] Sumathi, M., and S. Sangeetha. "A group-key-based sensitive attribute protection in cloud storage using modified random Fibonacci cryptography." Complex & Intelligent Systems 7, no. 4 (2021): 1733-1747.

[13] Saeed, Zinah Raad. "Improved cloud storage security of using three layers cryptography algorithms." International Journal of Computer Science and Information Security (IJCSIS) 16, no. 10 (2018).

[14] Adee, Rose, and Haralambos Mouratidis. "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography." Sensors 22, no. 3 (2022): 1109.

[15] Sandhia, G. K., and SV Kasmir Raja. "Secure sharing of data in cloud using MA-CPABE with elliptic curve cryptography." Journal of Ambient Intelligence and Humanized Computing (2021): 1-10.

Author's biography

Hari Krishnan Andi is presently working as the director, Centre for Postgraduate Studies, Asia Metropolitan University, Malaysia. His major area of research includes emotional intelligence, data mining, soft skills, business management, psychological development, and mentoring techniques.