Journal of Yarmouk Volume (22) Issue (1) May (2024)

ISSN 2075-2954 (Print)
Journal of Yarmouk available online at
https://www.iasj.net/iasj/journal/239/issues
مجلة اليرموك تصدرها كلية اليرموك الجامعة

Blockchain based Cryptography Hash Algorithm for trust in Cloud Storage Environments

Israa Nazeeh Mohammed [1]
[1]Department of Computer Science, College of Basic Education, University of Diyala, Diyala, Iraq
:* Corresponding author: Author Email
israamohammed@uodiyala.edu.iq

Abstract

Cloud environments have emerged as a powerful technology to meet infrastructure and data service requirements cheaply, with little effort, and with a high level of scalability; as a result, it has been heavily used in many areas of the information technology sector. Blockchain technology is here to stay and is becoming the next big thing, much like the Internet, thanks to its practical applications in supply chains, identity management, smart contracts, cryptocurrency, and speedier cross-border payments. Trust and security issues have prevented it from succeeding despite efforts to produce digital currency. However, the blockchain users govern its operations; therefore, it does not require a central authority to maintain proof gathered from user signatures and data using the Cryptographic Hash Algorithm. Blockchain will maintain evidence collected from data and user signatures based on the encrypted hash algorithm. The investigator identifies operations, gathers evidence, and creates reports based on the examination of storage evidence. The computational load versus the quantity of users, the overall rate of change regarding the quantity of users, and the duration of the hash computation regarding the quantity of users. The resulting graph is plotted for response, hash calculation, and encryption times. The experimental Proposed System Examination of storage revealed that the suggested approach performed better regarding response time and the overall change in cloud storage security characteristics.

Keywords: Blockchain, Cloud Environments, Security Blockchain Solution, SHA-256 Cryptographic hash algorithm.

1. Introduction

A field from computation has seen significant transformations over the last few decades, moving from distributed to service-oriented architecture and from stand-alone programs to client-server architecture. These changes were intended to increase the software's usability and boost the effectiveness of business process execution[1]. Networking computing is next step is cloud computing, an evolving type of IT delivery. With less expensive and complicated IT, it can provide hardware and software as on-demand resources and services via the internet [2]. Because of this, a large number of businesses, including Amazon, IBM, Google, Oracle, Microsoft, Sales Force, and HP, are racing to offer cloud solutions in different forms. Cloud service providers (CSPs) receive service requests from cloud consumers. The third parties that offer their clients cloud storage services are known as CSPs[3]. Attribute Authority (AA) and Third-Party Auditor (TPA) are two more third-party service providers that are meant to offer cloud security features [4]. We are aware that the two most important factors for businesses and institutions using the cloud are security and trust. There are numerous explanations, some of which include [5].The data of cloud customers is highly vulnerable to loss, leaking, or attack, and they are left with no way out of this untenable scenario. Cloud users need to be aware of who they are exchanging data with or dealing with. Transparency is also crucial; cloud customers should know who is accessing their data and how it is being used within the cloud. The newest term in the IT industry, cloud computing, has been discussed a lot in conferences, workshops, and even periodicals [6]. However, defining cloud computing is still a difficult task; there is still disagreement over its exact meaning. There are about a dozen definitions of cloud computing in academics, each with its own unique viewpoint [7]. However, the following characteristics of cloud computing is common among

them [8] a computer platform called cloud computing makes resource sharing possible for scalable infrastructures, middleware, and platforms and apps for application development. Cloud computing platforms are made possible by new computer technologies including virtualization, high-power business servers, high bandwidth, and service-oriented architecture. The three primary categories into which cloud services can be separated are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).Users can store and process all of their data on the web with cloud computing, but security is unquestionably one of the biggest issues [9]. But a more basic barrier keeping businesses from adopting the platform used by cloud computing is inherently less secure than traditional network infrastructure [10]. To earn clients' trust that their data is secure, cloud computing solutions must include security into every facet of their design [11]. When outsourcing and purchasing services from the cloud, cloud customers can increase trust and ensure data security by utilizing blockchain an innovative and developing technology. Blockchain security can offer more protection than centralized database security [12]. Blockchain uses a cryptographic hash function to the previous block to continuously monitor the list of linked and secured documents [13].Blockchain is a cutting-edge, emerging technology that cloud users can use to boost trust and guarantee data security while outsourcing and buying services from the cloudBlockchain security can offer greater security than centralized database security. Blockchain keeps an eye on the list of linked and secure documents continuously by using a cryptographic hash function from the preceding block [14].Moreover, in a situation when data disclosure is mandated, the openness of the blockchain can allow for data transparency. These benefits allow it to be used in a range of settings, including the financial sector and the Internet of Things (IoT) environment, and its uses are anticipated to grow[15]. Because cloud computing is efficient and readily available, it has been implemented in numerous IT systems. Furthermore, the fundamental security features have been explored in relation to cloud security and privacy issues.

2. Literature Review

Numerous earlier studies have demonstrated the applicability of blockchain technology for secure EHR sharing as well as other uses in healthcare systems. Numerous healthcare facilities are participating in different blockchain-based works Secinaro et al. [16] discussed how blockchain is used and its advantages for the accounting, auditing, and business management industries. Siyal et al. [17] presented the Healthcare Data Gateway (HDG) framework, one of the well-known instances of employing a private blockchain for tracking individual clinical data. Li et al. [18] suggested distributed ecosystem and cross-enterprise employing edge computing and blockchain to safely share manufacturing knowledge and services. Griggs et al. [19] created an Thorium-based blockchain application enabling the safe use of sensors to monitor patients who live far away. Chen et al. [20] suggested a cloud application running on blockchain that would store and exchange patient health data. Patients can share and control their health records under this framework without the involvement of an intermediary. Wang et al. [21] suggested a blockchain-based artificial intelligence system that aids in medical decision-making for patients and allows physicians to assess the course of treatment as a whole. Jiang et al. [22] suggested BloCHIE, which is built on an off-chain technique, to protect privacy and authenticity when exchanging personal healthcare data and electronic medical records. Pandey and Litoriya [23] suggested a framework to protect patient privacy and security during the electronic transmission of medical information based on attribute-based signature and MA-ABS. Abid et al. [24] suggested a distributed framework based on blockchain that would allow for the safe storage of patient records and medications on cloud servers to provide secure patient examination facilities. Zhang et al. [25] suggested utilizing signature private key sharing technique to realize data and backups for cloud data storage, as well as a safe and effective data storage and sharing scheme for blockchain-based mobile-edge computing [26]. As far as we know, blockchain technology is directly related to the computer-generated virtual objects that everyone uses. However, there are still a number of documented security issues with blockchain trust in cloud storage environments.

3. Blockchain Security of Cloud Storage

Blockchain technology offers transparency, immutability, and confidence in your data and transactions, which has the potential to completely transform cloud security. Cloud security may be greatly improved by utilizing it for tasks like decentralized identity management, immutable audit trails, and data integrity assurance [27]. With cloud computing, you can store your information in one central place. Using blockchain technology, you can store data in multiple locations around the world, with each node storing a copy of it. Unlike the peer-to-peer blockchain design, cloud computing relies heavily on the presence of multiple intermediary companies [28]. Blockchain technology improves cloud computing Blockchain technology improves cloud computing in several ways. It

improves data security by making data stored in the cloud resistant to tampering. It also increases transparency and auditability as all transactions are recorded and traceable. If consumers' private information leaks out of the cloud computing infrastructure, there may be financial and psychological consequences at stake[29]. Our primary focus is on data security in the cloud computing environment, including integrity and privacy during transmission and storage [30]. When integrated with the environment of cloud computing, blockchain technology increased to the right service degree can ensure safety. An encrypted electronic wallet is installed in order to use Blockchain technology. If the e-wallet is not properly erased, the user information may be abused. The user information can be extracted using the remaining user data. One of the biggest challenges is the occurrence of double transactions in the Blockchain and forging the Bitcoin record. To deal with such security concerns, an e-wallet that is trustworthy and safe is needed. Typically, e-wallets installed on PCs are utilized, but as mobile devices gain popularity daily, it is imperative to more closely examine the security of e-wallets on mobile devices. As a result, a transaction doesn't finish until its security is guaranteed by accuracy and integrity based on the time stamp generated in a mobile device[31].In the event that the attackers compromise or hack the security, a safe and dependable e-wallet restoration must be implemented. The security of user transaction data maintained in the e-wallet as well as the settings necessary for managing and using the e-wallet must be guaranteed. When the e-wallet is not in use, it must offer a means of securely and successfully erasing any leftover user data and it must then dispose of the remaining data.Data storage is one of the most popular cloud services. With little to no investment, end users to cloud servers and benefit from nearly limitless hardware and software resources as well as widespread access can outsource any amount of data [32]. In fact, during the past several years, a number of well-known cloud service providers—including Google Drive 8, Apple iCloud, Dropbox 16, Amazon S315, Microsoft SkyDrive 14, and Dropbox 16—have begun to offer these services. The following two crucial aspects of the cloud present obstacles to the advancement of data security methods[33].

4. SHA-256 Cryptographic Hash Algorithm It is claimed that security issues in the cloud environment can be solved by blockchain technology. Any transaction data is stored and is difficult to remove due to the consensus mechanism of blockchain technology. Otherwise, it becomes difficult for an intruder to interfere with transaction data.In this Figure 2; the blockchain technology-related SHA-256 cryptographic hash algorithm is depicted. To provide secure access, this technique produces two hashes, and is primarily used to verify the integrity of data and messages during the transaction and session time, identify the data and then verify the password. Blockchain architecture, or blockchain technology, is a linked list that is created using a combination of blocks and hash pointers. [34]. Every block has a distinct hash value in addition to data.

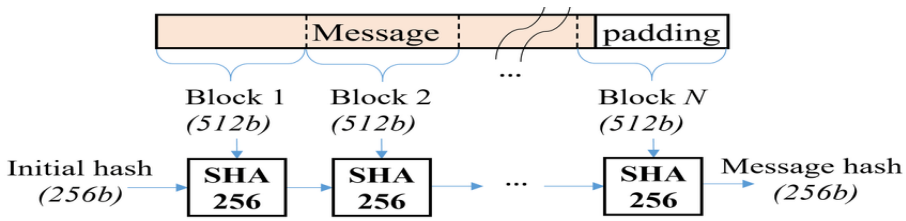

Fig. 1 SHA-256 cryptographic hash algorithm

SHA-256 is widely used in different parts of the Bitcoin network with enhanced security and privacy based on encryption and decryption. Data mining uses SHA-256 as a powerful algorithm to prove the function. The SHA-256 cryptographic hash algorithm, which is connected to blockchain technology, as shown in Figure 1. It is mostly utilized for session time, data identification, password verification, and data and message integrity verification during transactions. It creates hashes for safe access. Blockchain architecture, which is a linked list constructed using blocks and hash pointers, is known as blockchain technology. Every block, with the exception of the first block, which includes no previous hashing, contains information and a unique hash value from the preceding block [35].The activities carried out by an authorized investigator include identifying, gathering, analyzing, and producing reports using the Logical Graph of Evidence (LGoE). A technique operates on the fundamental tenet that distant blocks have a comparable hash value and that a smaller change made in the input block has a complex effect on the output string. The 256 bit block in the input is hashed using the following formula:(256) = Σ 256 $(x)(x\ mod\ y)$ $(x-i)$ (1)Where p(x) denotes parole with mean y and Ha(256) is the hash function of the 256 bit block. The input block is originally divided into fragments using 1025 bits in this algorithm. The rounding constants and the 64-bit hash value are produced. This algorithm consists of 82 repetitions in which the message array is divided into 80 64-bit words.

The 16th bit to the 80th bit is when the iterating loop is planned to begin. In the section that follows, the hash algorithm's performance analysis and outcomes are covered.

5. Proposed System

The purpose of gathering and proving evidence in cloud storage, this study represents and develops Blockchain architecture, as shown in Figure 2. Before utilizing Hash Algorithm to encrypt data, the user must first register with a trusted authority and obtain the key. The user will then use their password, user ID, and a random number to authenticate them. After verification, files encrypted can be uploaded by the user to the cloud. The block includes a time stamp value, a list of transactions along with the data's hash value from the preceding block. The smart contract allows tracking of any changes made to these data. A report is generated and sent to the user if any access has been made. Ultimately, the investigator can obtain the evidence from the Blockchain and the controller, as well as the different adjustments made to that evidence. The results of the experimental evaluation show that the suggested strategy performed better in terms of response time and overall change rate. As a result, our suggested approach has addressed every major drawback of the current systems. Through an authorized server, the user first registers with the cloud service provider. Next, the replacement procedure was used to secure the user's identity. The secure hashing technique protects user data within the cloud network. To safeguard the data, the hash value is tracked to identify any changes that could compromise its security.

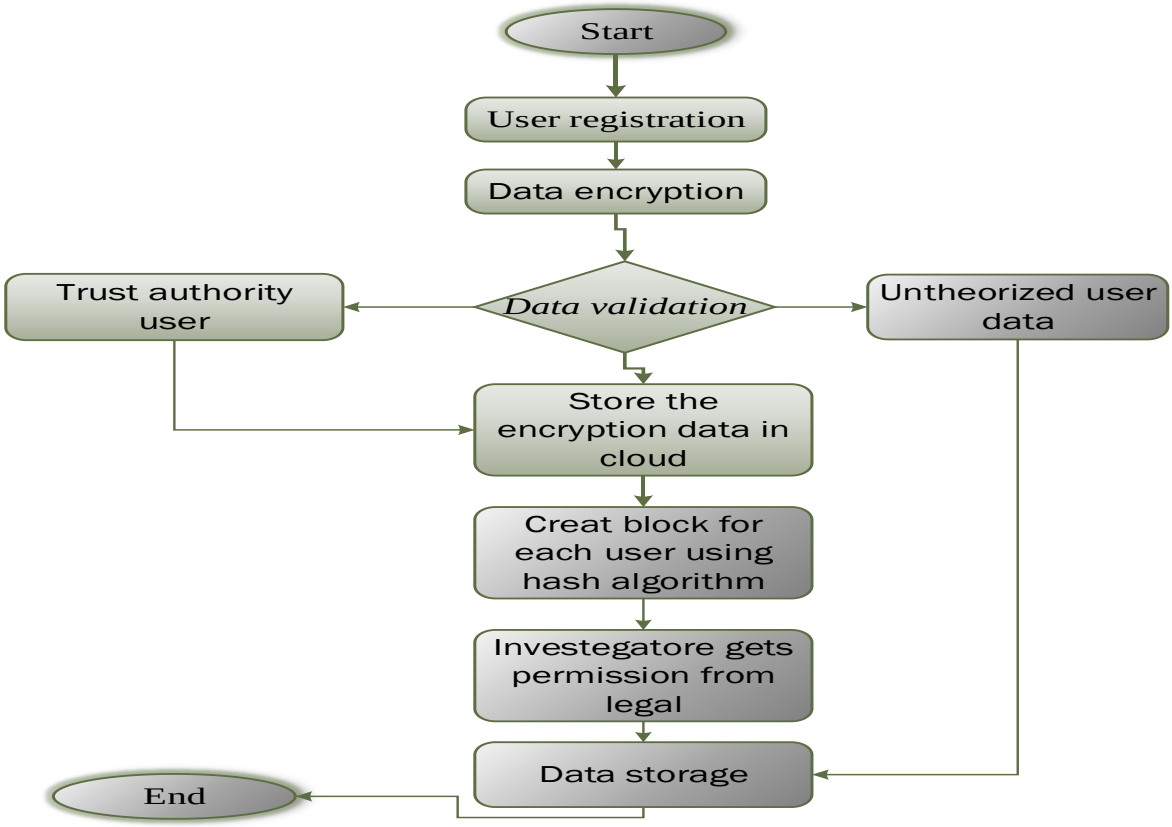

Fig .2 Methodology Blockchain Efficiency for Trust in Cloud Storage Using Cryptography Hash Algorithm

6. Results and Discussion The framework for cloud computing is renowned for producing no harm since it was introduced to the market. The security and authentication of the user and their data are improved by current methods and technological advancements. Thus, the maintenance of user authentication and data secrecy are additional advantages of the cutting-edge cloud computing servers. The hash algorithm-based cloud encryption offers a mutual and planned architecture encounter model that is vulnerable to security vulnerabilities. The suggested paradigm provides more effective protection against dictionary attacks and rainbow attacks thanks to the hash replacement technique. These attacks aim to intercept data transmissions, fabricate a phony browser, and pilfer user passwords. Utilizing a protocol analyzer, end user activity is examined while the cloud network is operational. The cloud server administrator notifies users when they are at risk of attack. Increased security is made possible by the hash cipher approach, which uses double encryption and double key. Because the method is not computationally complex and takes less time to encrypt and decrypt, it is a time-consuming approach with a fast processing speed. Compared to other substitution approaches, less storage space is needed

because the encrypted cipher's data size is the same as the original messages. This technique's key exchange procedure is easier to use and doesn't provide any difficult problems. The cloud server uses the hash algorithm 256 encryption to safeguard the information. This concept uses a string of hash values to hash user data. Variance in these numbers indicates to the user that user data has been altered or lost. This model's Hash 256 method significantly adds to the issue of fake browsers by identifying and thwarting attacks at an early stage. The results of the experimental research showed that the suggested system performed better in terms of accuracy, response time, throughput growth, and total security parameter modification, as shown in Figure 3.

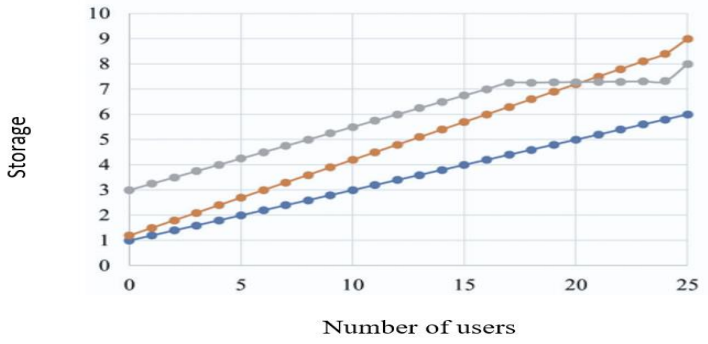

Fig .3 Examination of storage

7. Conclusion

As part of our work, we developed an architecture for cloud storage environments using blockchain technology, which is used for evidence gathering and provenance maintenance. Perfect data encryption and data storage are part of the recommended solution. It was easier for us to generate the SHA-256 hash, which raised our system's security level. This paper has examined the general structure of blockchain. Additionally, the security requirements for blockchain features and cloud computing have been looked at. As our study has demonstrated, blockchain technology holds promise as a useful and practical means of guaranteeing security in cloud computing settings. SHA-256 hashing is crucial for data security and integrity in cloud computing environments. Customers can more easily create SHA-256 hashes by utilizing cloud cryptography services, which improves their capacity to confirm data accuracy and set up safe digital procedures. By following best practices and being aware of the services provided by specific cloud service providers, it is feasible to guarantee that SHA-256 is effective in preserving the dependability and integrity of data kept in the cloud.

References

[1] A. Gupta, S. T. Siddiqui, S. Alam, and M. Shuaib, “Cloud Computing Security using Blockchain,” JETIR June 2019, Vol. 6, Issue 6, no. June, 2019.

[2] A. El Mhouti, A. Bahbah, M. Fahim, Y. El Borji, and A. Soufi, “International Journal of Computing and Digital Systems Improving Weather Forecasting Using Meteorological Big Data Scraped From Web Sources: a Cloud-Based Approach,” Int. J. Comput. Digit. Syst., vol. 2, no. 20, pp. 1–11, 2023, [Online]. Available: http://journals.uob.edu.bh.

[3] H. A. A. Mohammed, I. Nazeeh, W. C. Alisawi, and Q. K. Kadhim, “Anomaly Detection in Human Disease : A Hybrid Approach Using GWO-SVM for Gene Selection,” Rev. d ’ Intell. Artif., vol. 37, no. 4, pp. 913–919, 2023.

[4] Qusay Kanaan Kadhim, R. Yusof, H. S. Mahdi, S. S. Ali Al-Shami, and S. R. Selamat, “A Review Study on Cloud Computing Issues,” in Journal of Physics: Conference Series, Jun. 2018, vol. 1018, no. 1, doi: 10.1088/1742-6596/1018/1/012006.

[5] W. Meng and Q. Wang, “When Intrusion Detection Meets Blockchain Technology : A Review,” IEEE Access, no. March, 2018, doi: 10.1109/ACCESS.2018.2799854.

[6] Y. Du, Y. Li, J. Chen, Y. Hao, and J. Liu, “Edge computing-based digital management system of game events in the era of Internet of Things,” J. Cloud Comput., vol. 12, no. 1, pp. 3–13, 2023, doi: 10.1186/s13677-023-00419-5.

[7] S. Srivastava et al., “Scope of Cloud Computing in Business: A Compendious and Methodical Analysis of Trends in Publications and Patents,” Vision, vol. 27, no. 4, pp. 510–525, 2023, doi: 10.1177/09722629211015600.

[8] B. J. Khadhim, Q. K. Kadhim, W. M. Khudhair, and M. H. Ghaidan, “Virtualization in Mobile Cloud Computing for Augmented Reality Challenges,” Proc. 2021 2nd Inf. Technol. to Enhanc. E-Learning other Appl.

Conf. IT-ELA 2021, no. June 2022, pp. 113–118, 2021, doi: 10.1109/IT-ELA52201.2021.9773680.
[9] S. T. Ahmed and S. M. Kadhem, "Applying the MCMSI for Online Educational Systems Using the Two-Factor Authentication," Int. J. Interact. Mob. Technol., vol. 15, no. 13, pp. 162–171, 2021, doi: 10.3991/ijim.v15i13.23227.
[10] H. A., Q. Kanaan, and H. Sadeq, "Evaluation of Routing Protocols on Ad Hoc Network Modelling from Medical Data using OpNet Simulation," Diyala J. Pure Sci., vol. 13, no. 2, pp. 33–47, Apr. 2017, doi: 10.24237/djps.1302.204C.
[11] G. Li and H. Sato, "A privacy-preserving and fully decentralized storage and sharing system on blockchain," Proc. - Int. Comput. Softw. Appl. Conf., vol. 2, pp. 694–699, 2019, doi: 10.1109/COMPSAC.2019.10289.
[12] Q. K. Kadhim, B. M. Al-Nedawe, and E. M. Hameed, "Encryption and Decryption of Images using GGH Algorithm: Proposed," IOP Conf. Ser. Mater. Sci. Eng., vol. 1090, no. 1, pp. 1–7, Mar. 2021, doi: 10.1088/1757-899X/1090/1/012063.
[13] G. Verma and S. Kanrar, "Secure document sharing model based on blockchain technology and attribute-based encryption," Multimed. Tools Appl., vol. 15, no. July, pp. 1–18, 2023, doi: 10.1007/s11042-023-16186-z.
[14] I. Nazeeh, T. Hussain Hadi, Z. Qahtan Mohammed, S. Taha Ahmed, and Q. Kanaan Kadhim, "Optimizing blockchain technology using a data sharing model," Indones. J. Electr. Eng. Comput. Sci., vol. 29, no. 1, p. 431, 2023, doi: 10.11591/ijeecs.v29.i1.pp431-440.
[15] S. T. Ahmed and S. M. Kadhem, "Early Alzheimer's disease detection using different techniques based on microarray data: A review," Int. J. Online Biomed. Eng., vol. 18, no. 04, pp. 106–126, Mar. 2022, doi: 10.3991/ijoe.v18i04.27133.
[16] S. Secinaro and F. D. Mas, "Blockchain in the accounting , auditing and accountability fields : a bibliometric and coding analysis," Accounting, Audit. Account. J., vol. 35, no. 9, pp. 168–203, 2022, doi: 10.1108/AAAJ-10-2020-4987.
[17] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain Application in Healthcare Systems: A Review," Systems, vol. 11, no. 1, pp. 1–44, 2023, doi: 10.3390/systems11010038.
[18] S. Khezr, A. Yassine, and R. Benlamri, "applied sciences Blockchain Technology in Healthcare : A Comprehensive Review and Directions for Future Research," MDPI, pp. 1–28, 2019, doi: 10.3390/app9091736.
[19] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, and E. A. Howson, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Healthcare Blockchain System Using Smart Contracts for Secure," MDPI, no. June, 2018, doi: 10.1007/s10916-018-0982-x.
[20] G. Chen, B. Xu, M. Lu, and N. Chen, "Exploring blockchain technology and its potential applications for education," Smart Learn. Environ., pp. 1–10, 2018, doi: 10.1186/s40561-017-0050-x.
[21] Y. Wang, J. H. Han, and P. Beynon-davies, "Understanding blockchain technology for future supply chains : a systematic literature review and research agenda Supply Chain Management : An International Journal Article information :," Supply Chain Manag. An Int. J., no. April 2019, 2018, doi: 10.1108/SCM-03-2018-0148.
[22] A. Alsarhan, I. T. Almalkawi, and Y. Kilani, "A New Covid-19 Tracing Approach using Machine Learning and Drones Enabled Wireless Network," Int. J. Interact. Mob. Technol., vol. 15, no. 22, pp. 111–126, 2021, doi: 10.3991/IJIM.V15I22.22623.
[23] P. Pandey and R. Litoriya, "Implementing healthcare services on a large scale : Challenges and reme dies base d on blockchain technology," Heal. Policy Technol., vol. 9, no. 1, pp. 69–78, 2020, doi: 10.1016/j.hlpt.2020.01.004.
[24] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization," Proc. - IEEE INFOCOM, vol. 2018-April, pp. 792–800, 2018, doi: 10.1109/INFOCOM.2018.8485890.
[25] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, Blockchain-based trust management in cloud computing systems : a taxonomy , review and future directions. Journal of Cloud Computing, 2021.
[26] T. H. Hadi, J. Kadum, Q. K. Kadhim, and S. T. Ahmed, "An Enhanced Cloud Storage Auditing Approach Using Boneh-Lynn- Shacham ' s Signature and Automatic Blocker Protocol," Ingénierie des Systèmes d'Information, vol. 29, no. 1, pp. 261–268, 2024, doi: https://doi.org/10.18280/isi.290126 Received:
[27] V. S. Badari Narayan, A. K. Bhagat, C. Chethan, B. S. Alfurhood, A. P. Singh, and T. R. Mahesh, "Blockchain Based De-Duplication Analysis of Cloud Data with Data Integrity using Policy Based Encryption

Technique in Cloud Storage," Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 3s, pp. 161–164, 2023.
[28] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," Symmetry (Basel)., vol. 9, no. 8, pp. 1–13, 2017, doi: 10.3390/sym9080164.
[29] Q. K. Kadhim, R. Yusof, and S. R. Selamat, "The Cloud Computing Control in the Government Services," Jour Adv Res. Dyn. Control Syst., vol. 10, no. 04, pp. 1136–1147, 2018.
[30] S. Taha Ahmed and S. Malallah Kadhem, "Using Machine Learning via Deep Learning Algorithms to Diagnose the Lung Disease Based on Chest Imaging: A Survey," Int. J. Interact. Mob. Technol., vol. 15, no. 16, p. 95, 2021, doi: 10.3991/ijim.v15i16.24191.
[31] R. Awadallah, A. Samsudin, J. E. S. E. N. Teh, and M. Almazrooie, "An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3077123.
[32] Q. Kanaan, H. S. Mahdi, and H. K. Ail, "Storage Architecture for Network Security in Cloud Computing," Diyala J. Pure Sci., vol. 14, no. 1, pp. 1–17, 2018.
[33] C. H. V. N. U. B. Murthy and M. L. Shri, "Blockchain Based Cloud Computing : Architecture and Research Challenges," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3036812.
[34] A. Kuznetsov, I. Oleshko, V. Tymchenko, K. Lisitsky, M. Rodinko, and A. Kolhatin, "Performance analysis of cryptographic hash functions suitable for use in blockchain," Int. J. Comput. Netw. Inf. Secur., vol. 13, no. 2, pp. 1–15, 2021, doi: 10.5815/IJCNIS.2021.02.01.
[35] A. Ramachandran, P. Ramadevi, A. Alkhayyat, and Y. K. Yousif, "Blockchain and Data Integrity Authentication Technique for Secure Cloud Environment," Intell. Autom. Soft Comput., 2023, doi: 10.32604/iasc.2023.032942.