Analysis of Secure Data Sharing Techniques Using Blockchain

Neha Mathur[*1], Shweta Sinha[*2], Rajesh Kumar Tyagi[3], Nishtha Jatana[4]

[1,2,3] Amity University, Haryana, India
[4]MSIT, New Delhi, India
Emails: mathurneha89@gmail.com; ssinha@ggn.amity.edu ; rktyagi@ggn.amity.edu ; nishtha.jatana@gmail.com

Abstract
The demand for cloud computing has increased immensely, and its security is becoming challenging. The enormous growth in cloud computing adaptation has been observed, but the information security concerns have not been addressed thoroughly. The security issues related to cloud computing are a concern. The emergence of Blockchain as a key security provider has increased the hope for the availability of a secure cloud computing environment. The data-sharing technique based on the cloud scenario relies on the network's storage and architecture; however, the storage providers are considered trusted third parties for data-sharing and storage purposes. The associated limitations such as security, high operational cost, centralized storage capability, and data availability have become a challenging task, which leads to the development of a trusted data management system for secure data sharing through the Blockchain. This study presents an analysis of secure data-sharing techniques using Blockchain. The related research articles were elicited from several sources such as Springer, IEEE, Elsevier, and other online sources. The primary studies have been categorized into four types: healthcare data sharing, vehicular communication-based data sharing, IoT-based data sharing, and other miscellaneous techniques. The techniques have been analyzed based on various performance metrics. The analysis and findings of this study can pave a way for the future development of safe data-sharing techniques using Blockchain technology.

Keywords: secure data sharing; Blockchain; IoT; healthcare; vehicular communication-based data sharing

1. Introduction

Many companies and individuals utilize cloud computing for data sharing and storage-related applications. The data owners consider availability, scalability, and low cost as the essential features for data storage in the cloud [1]. In addition, recurrent maintenance, software updates, and storage infrastructure maintenance are liberated from the data owners. However, the centralized architecture and the security and privacy concerns of the cloud have become challenging for the users of cloud computing. Besides the limited control, the centralized format of data storage, and the unknown data organization in the Cloud have also become a tedious tasks in cloud computing.

Several traditional methods suffer from the cloud's centralized storage and data availability capability [2]. Besides, secure data sharing is still challenging; hence, the cryptographic methods and the trust-based construction of the framework become the necessary component in cloud computing. Thus, the blockchain-based data-sharing technique emerged due to the decentralized nature and security benefits that attracted several researchers that solve the mutual trust and centralized storage. In Blockchain technology, all transactions are recorded; hence, no information can be altered by the user which provides enhanced security.

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

Blockchain is developed by considering the untrusted environment and tampering of data, and cryptography is therefore deemed essential to ensuring the security and integrity of data sharing [2]. In addition, the smart contract is utilized for transparent, faster, conflict-free, undeniable, and secure transactions automatically without considering the aid of a third party that uses the computer code. However, misinterpretation and misuse may occur, which can be protected through various authentication and access control techniques [3].

1.1 Motivation

The blockchain-based secure data sharing uses the decentralized approach for sharing information between devices. Thus, using secure data sharing can minimize unauthorized data access and information leakage [4]. Several researchers developed a certain data-sharing approach for security based on Blockchain, but challenges such as high-level security and privacy issues still prevail. Hence, this research provides an analysis of the prevalent data-sharing techniques based on Blockchain to identify the obstacles and fulfill them in future work to model an efficient approach. The objectives of this study are:

- To study and analyze the prevalent data-sharing methods based on Blockchain.
- To categorize the existing techniques based on the methods utilized to obtain secure data sharing.
- To analyze the performance metrics used for quantifying the approaches used for data sharing using Blockchain.
- To provide challenges that exist after a thorough review of the existing approaches used for data sharing using blockchain that provides research opportunities for researchers working in the area.

To fulfill the objectives, the prevalent secure data-sharing techniques based on blockchain criteria are analyzed to identify the challenges faced by the system. The prevalent methods are analyzed based on the type of data sharing, such as healthcare, vehicular communication, IoT, and miscellaneous methods. In addition, the performance metrics utilized and the mechanism used by the prevalent methods are analyzed to identify the research gaps in the area.

The remaining paper is organized as follows: Section 2 details the related works, and the results and discussion are presented in Section 3. Section 4 details the research gaps, and the conclusion of this study is presented in section 5.

2. Related Works

The prevalent literature concerning secure data sharing using Blockchain is reviewed in this section.

2.1 Categorization of Techniques

The prevalent related works of secure data sharing in the cloud can be categorized into four different groups: healthcare-based data sharing, vehicular communication-based data sharing, IoT-based data sharing, and other techniques, as depicted in Figure 1.

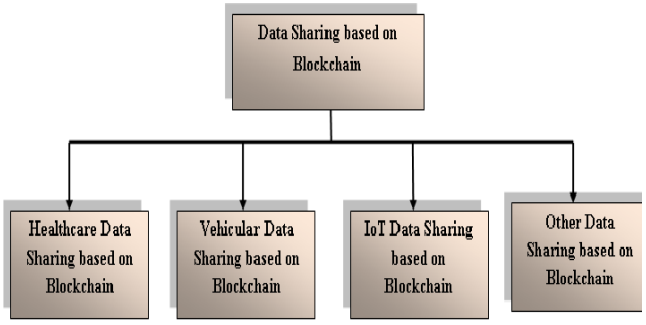

Figure 1: Categories of secure data sharing based on Blockchain

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

2.1.1 Data sharing in healthcare

The extensive data collected from healthcare devices demand the privacy-preserving model, to ensure the secure and safe transaction of delicate information of the patient. Hence, the blockchain is widely used to ensure the secure transaction of medical data. An analysis of some blockchain techniques used for healthcare applications is described in this section.

The healthcare-based secure data sharing using Blockchain is detailed here. Researchers have used the authentication approach for secure data sharing in the medical field in a decentralized network [1]. The researchers in their work have utilized the Burrows Abadi Nidham (BAN) logic-based authentication for data sharing in the integrated cloud and blockchain network. Here, the hashes generated for secure data sharing were stored in the Blockchain with encryption. In addition, the certification authority was utilized for the detection of malicious attacks and efficient data sharing through the public key and decryption process. The consortium blockchain was used in the user and processing layer to update and retrieve medical information. This medical data-sharing approach obtained security, authentication, and cost efficiency and showed a better performance.

Further, for secure data sharing using the blockchain technique, researchers have utilized the remote patient monitoring system [2]. In this, the data concerning the patient is shared in the network, which the patient owns, and the medical institution requests the patient for data access for the real-time patient monitoring framework. For this, the GHOSTDAG blockchain was used to provide secure transactions through alert messages. Besides, authorized users such as insurance companies, family members, and others were included in the data sharing for further processing. The method employed for real-time monitoring was reliable and obtained high throughput for secure transmission.

Researchers have also worked for medical data sharing based on four layers of the architecture using the integrated IoT with blockchain framework [3]. In this arrangement, the patient's information was stored in the physical layer, and the devices such as sensors and other wearable components were placed in the second layer named the device layer. The communication occurs in the third layer, and the real-time processing interfaces such as the Blockchain were placed in the fourth layer. Here, the information of the patient is stored in the Blockchain with appropriate encryption for ensuring the authentication of the information, such as laboratory and test reports. The latency of the medical data-sharing technique is lower, and the energy consumption is also reduced through the developed method.

The combined Blockchain and the digest chain named Medchain were utilized for secure data sharing in the healthcare scenario [4]. Here, the integrity of the information transmitted in the network is obtained through the generation of the digest chain. In addition, secure sharing is obtained through the session-based sharing strategy, in which the cryptography-based scheme was utilized for privacy preservation. The entities such as health providers, patients, and the data requester were considered for the data sharing technique. The immutability of the Blockchain is ensured through the cascaded hashing method. The efficiency and security analysis shows that the process was robust against attacks.

Healthcare data sharing was utilized by authors in their work for secure transactions through the blockchain technique [5]. Authors used revocable attribution-based signatures for electronic medical data sharing in the healthcare system [6]. Here, the sign-in key is generated using the integration of the master key and the update key. The master key refers to the attribute set and user identity, and the update key refers to the revocation of the attribute. Here, the authorized Blockchain is utilized for storage and information access, in which the user updates the information with the signature, and upon request, the data is retrieved through authorization. The efficiency and storage were evaluated to show the best performance of the healthcare system.

Researchers have used secure patient data sharing through the Blockchain [7]. With this data, the cancer prediction was made from the obtained information through combined deep learning and blockchain architecture. In this, the deep learning classifier is trained using the weights, which is performed through the Blockchain to solve the issues regarding computation complexity. The information like the CT image of patients from several hospitals connected to the Blockchain is utilized for training the classifier, in which the weights and hashes are stored in the Blockchain for the minimization of the cost. Besides, preprocessing and optimization were utilized for the removal of noise and to solve the optimization issues. The detection accuracy was computed by the efficiency estimation of the blockchain-based deep learning technique.

Hence from the evaluation, it is demonstrated that blockchain technology ensures secure communication of health care data. This will enable the healthcare assistants to render real-time service to the patient. However, the blockchain methods

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

require further enhancement with various advanced techniques such as ensemble learning, deep learning, and federated learning for securing the data from various attacks.

2.1.2 Data sharing based on vehicle communication

The traditional vehicular ad hoc network experiences challenge due to trust management, data storage, and information storage. Hence to face the challenges such as security risk and data leakage blockchain technology is used in VANET architecture. The blockchain enhances the reputation of the vehicle by exploring smart contracts of the vehicles. Some of the blockchain technology used in VANET architecture is briefly described in this section.

The vehicular communication-based secure data sharing by considering the Blockchain is detailed here. The data-sharing technique based on vehicular edge computing based on the consortium blockchain and the smart contract has been used by researchers [8]. In this, the reputation-based security enhancement was provided through the Blockchain for safer communication between the vehicles. Here the real identity was not revealed to other users of the network. The key generation and its management were performed through the trusted authority and the trust value was evaluated before information sharing for security reasons. The method obtained improved the throughput with minimal overhead for efficient information sharing among the devices.

The authors developed the registration authority-based authentication for secure data sharing among vehicles using the consortium blockchain [9]. The proof-of-work consensus mechanism is utilized to ensure communication transparency, in which the registration authority was used through the unique identity. In addition, the selfish mining attack of the method supports attack prevention through smart contacts. Researchers have further used trust-based data sharing for vehicle communication through the smart contract for sustainable and secure sharing [10]. In this, the inappropriate information was removed through the creditability evaluation. This was also helpful for the attack against malicious behavior. In the blockchain edge layer, message aggregation along with the reputation of the vehicle was employed through the smart contract and, the consensus mechanism was utilized for agreeing. Thus, trusted data sharing was used through the blockchain network in a distributed fashion. The enhanced performance was acquired in terms of throughput.

Researchers also used the anonymous authentication approach for the vehicular social network, in which secure data sharing among the vehicles was done through the integrated pseudonym generation and identity-based signature mechanism [11]. The traceability and security of the information are assured by the consensus and signature strategy. The registration of the vehicle is the initial step, and then the authentication is provided for the registered vehicle before the data sharing. The best performance is obtained in terms of computation cost and time. Others also applied another anonymous authentication mechanism for vehicular communication using the Blockchain [10]. In this, trust-based legality verification was employed before data sharing to ensure safer communication. Initially, vehicle registration was employed, followed by authentication. It was provided before data sharing through the Hess signature strategy. Effective, secure communication was evaluated based on the security and performance analysis. A hybrid cryptography-based system was employed by researchers for secure data sharing in the vehicular network using the Ethereum blockchain [12]. In this, the blockchain immutability and authenticity were obtained through the Keystore modification. The semantic security offered by the system prevents the attacker based on the probabilistic polynomial time. In addition, using the signature approach, authenticity was obtained through several security considerations.

The anonymity of the vehicle is preserved by blockchain technology as it hides the information about the data owners. Further, the attackers fail to reveal sensitive information without obtaining the private key of the data provider. However, the blockchain requires further improvement with recent deep learning techniques to avoid the cracking of the private key by attackers [8].

2.1.3 IoT-based Data sharing using Blockchain

The billions of devices are connected and transmit data in the Blockchain framework, which is found to be complicated to satisfy the IoT demands. The unauthorized IoT devices of various organizations illegitimately access the resources. Trust issues and scalability issues are significant challenges that deteriorate the performance of the IoT framework, which can be handled by blockchain technology. The data sharing based on the IoT scenario using the Blockchain is detailed here. The permissionless Ethereum blockchain-based data sharing is employed in the IoT scenario to solve the trust and scalability issues [13]. Here, encryption is performed for the safer transmission of data. While retrieving the information, it is visible to the users in the smart contract and the data owner through the efficient re-encryption strategy; thus, integrity and confidentiality are preserved. In this, the entities such as Blockchain, cloud, data requester, and sensors were

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

considered for efficient data sharing. The identity-based authentication was employed using the elliptic curve Qu-Vanstone implicit (ECQV) certificates for guaranteeing the public and identity key link. Accordingly, the best performance was analyzed along with the time complexity.

Several apps use cross-border and cross-domain data exchange with centralized cloud infrastructure to guarantee the security and privacy of information in a particular area [14]. In addition, secure gateways are provided for detecting malicious entities in the network; thus, the privacy of the information is preserved. The token-based data access was employed in the system to verify user integrity, in which authorized miners verify each data-sharing entity through the Blockchain. Besides, the authentication of the data is ensured through the Identity-based Signature (IBS), and Ephemeral Elliptic Curve Die-Hellman (ECDHE) approaches, which offer robust performance against attack. The secure and authenticated data sharing in the IoT scenario through an enhanced flaw detection technique in Blockchain was utilized by researchers [15]. In this, mutual authentication was used to prevent malicious attacks, and a lightweight strategy was followed to minimize the computations and energy consumption. The system guarantees data confidentiality through authentication based on the blockchain strategy. The computational cost and time of the system were minimal compared to the other state-of--of-art techniques based on the authentication scheme.

Authors utilized proxy re-encryption-based secure data sharing in the IoT through the identity-based encryption criteria [16]. In addition, the information's security, integrity, and confidentiality are guaranteed through fine-grained access control. Here, the Blockchain is considered the trusted entity generating the keys. Hence the security of the information is obtained in the system model. Besides, the data packet loss was minimized through the data caches in the forward processing technique, and efficient data storage and bandwidth utilization were obtained through multiple delivery techniques. Thus, the developed proxy re-encryption method received flexible authorization and encryption. Decentralized Blockchain-based Authentication (DBA) protocol was employed for secure data sharing in the resource-constrained IoT scenario [17]. In addition, the encryption of the data was performed in the IoT device to ensure the confidentiality of the information transmitted in the network. In the retrieval phase of the stored data, the key exchange based on the Revised Diffie-Hellman approach was used to minimize the processing time and obtain high performance based on the storage space and computation time through the implementation of the Spark architecture.

The research community utilized authentication, authorization, and trust-based data sharing in the IoT through blockchain-based access control [18]. The user's registration in the contract ensures the utilization of the authentication and multiple contracts for enhanced secure data sharing. The behavior judgment system was employed to detect malicious requests and halts those requests for a particular time. Thus, the well-provided user request was executed in the approach, and the Blockchain was utilized for storing the information. The cost analysis was performed by the authentication system and obtained better performance. The inner product encryption-based proxy re-encryption approach was used by [19] for secure data sharing based on the IoT. Here, confidentiality is obtained by dividing the data into two blocks; one is stored in the cloud while the other is stored in the Blockchain. However, the computations were performed in the Blockchain due to the constrained resource in the cloud. Fine-grained access control was acquired by the method through the incorporation of the blockchain technique. The trusted data sharing in the IoT scenario based on the Blockchain was used through the lightweight strategy [20]. In this, the Oracle-based data collection was performed, and the data sharing was employed through the Blockchain, which is computationally expensive. Hence, the lightweight approach minimizes the computation overhead and provides safer communication.

From the analysis of the aforementioned literature, it is evident that blockchain technology results in increased integrity in the data transaction flow. However, service interruption and data breaches are issues that are still prevalent even with the use of blockchain technology.

2.1.4 Data sharing using Blockchain

Data sharing is a crucial aspect in the research community as it helps to attain massive knowledge from the existing works. Data sharing always depends on a trusted third-party system. There is a lack of security, immutability, trust, and transparency due to the third party. Hence to mitigate these issues, blockchain technology is used in the data-sharing application. Considering the benefits of the interplanetary file system (IPFS), researchers have incorporated encryption and an incentive mechanism based on Blockchain [21]. The blockchain-based data sharing using multiple attribute authorities was developed for the prevention of single-point failure in the network [22]. Here, the encryption technique named multi-authority attribute was employed for the reduction of the computation and communication overhead. The smart contract among the multiple authorities ensures safer communication, and the token mechanism is followed in the decryption phase. This method utilized the Hyperledger Fabric blockchain for access control to ensure secure data sharing.

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

The blockchain-based data sharing in the food industry using the cloud scenario was employed by [23]. A fusion scheme named Decentralized Attribute-Based Signature (DABS) for data sharing between the departments of the industry. The high performance, scalability, and low cost were the achievements of the method utilized for secure data sharing. The encryption technique and the regulators treat all the employees equally and promote the governance of the industry. From the analysis, it is evident that the blockchain model is reliable, robust, and provides integrity of data. However, the existing blockchain models are designed for only small-scale applications.

3. Analysis of Related Works

The analysis based on the performance metrics utilized for the evaluation of the prevalent methods and the analysis based on secure data sharing is detailed in this section.

3.1 Analysis based on Methods

An overall analysis based on the mechanisms utilized by the related works is depicted in Table 1 by considering the Blockchain used and the smart contract used in the article, and whether the article is concerned about security, privacy, and integrity. Generally, the blockchain was categorized into private or permissioned blockchain, public blockchain, and consortium. The private blockchains are considered the distributed ledger that is not accessible to the public. The public blockchain can be easily accessed by anyone in the network. The consortium blockchain is categorized under a semi-decentralized network, in which the users are not provided with a single entity. Integrity is the quality that evaluates the consistency, validity, and accuracy of the institutional data. These integrities are focused on some reviewed articles [4, 5, 6, 8, and 11]. The smart contract is also defined as the self-executing acknowledgment that ensures the agreement between the providers and the users, which is mostly utilized in blockchain techniques.

Table 1: Analysis based on Methods

Reference	Domain	Type of Blockchain	Security	Privacy	Integrity	Smart Contract	Method
[1]	Healthcare	Consortium	✓	✓	×	×	Medi-block
[2]	Healthcare	consortium	✓	✓	×	✓	GHOSTDAG
[3]	Healthcare	Not mentioned	✓	×	×	✓	Hyper ledger blockchain
[4]	Healthcare	Consortium	✓	✓	✓	×	Medchain
[5]	Healthcare	Consortium	✓	✓	✓	✓	Sharing Data between Healthcare Providers Framework (SDHPF)
[6]	Healthcare	Permissioned	✓	✓	✓	×	Revocable attribute-based signature
[7]	Healthcare	Permisioned	✓	✓	×	✓	Blockchain + AI
[8]	Vehicle	Consortium	✓	✓	✓	✓	consortium blockchain and smart contracts
[9]	Vehicle	Consortium	✓	✓	×	✓	consortium blockchain-based energy trading algorithm

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

[10]	Vehicle	Consortium	✓	✓	×	✓	consortium blockchain and smart contracts
[11]	Vehicle	Consortium	✓	✓	✓	✓	signature mechanism and the consensus mechanism
[12]	Vehicle	Consortium	✓	×	×	✓	Hybrid Cryptographic Protocol
[13]	IoT	consortium	✓	✓	✓	✓	proxy re-encryption
[14]	IoT	permissioned	✓	✓	✓	✓	Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) and Identity-based Signature (IBS)
[15]	IoT	Consortium	✓	×	×	✓	improved ID-based signature authentication
[16]	IoT	Consortium	✓	✓	✓	×	Proxy Re-Encryption model
[17]	IoT	Not mentioned	✓	✓	×	×	Revised Dife-Hellman algorithm
[18]	IoT	Consortium	✓	×	×	✓	Multiple smart contracts
[19]	IoT	Consortium	✓	✓	✓	×	Proxy-Based Data Sharing Module
[20]	IoT	Consortium	✓	✓	✓	✓	Secure and Lightweight Triple-trusting Architecture (SLTA)
[21]	Communication	Consortium	✓	✓	✓	✓	Interplanetary File System (IPFS)
[22]	Others	Consortium	✓	✓	✓	✓	Decentralized Attribute-Based Signature (DABS)
[23]	Communication	Consortium	✓	✓	×	✓	Blockchain-based Multi-authority Access Control scheme (BMAC)
[24]	IoT	Consortium	✓	✓	×	✓	Hyperledger-Fabric RCA
[25]	Vehicle	Consortium	✓	✓	✓	✓	Consortium Blockchain
[26]	Surveillance	Not mentioned	✓	✓	✓	✓	ABE model with parallel outsourced computation (ABEM-POC)

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

[27]	Smart Industries	Not mentioned	✓	×	✓	×	Blockchain-assisted secure data sharing (BSDS)
[28]	Vehicle	Consortium	✓	✓	✓	✓	Consortium Blockchain
[29]	Communication	Consortium	✓	✓	✓	✓	attribute-based signcryption scheme
[30]	IoT	Coonsortium	✓	✓	×	✓	Identity authentication and Hyperledger Fabric

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

3.2 Analysis based on Performance Metrics

The analysis based on the performance metrics utilized by the related works is illustrated in Figure 2. The prevalent methods used performance metrics such as accuracy, loss, latency, time, cost, throughput, storage error, and other metrics such as responsiveness and bandwidth. A short description of the performance metrics is given as follows:

3.2.1 Accuracy: The accuracy is characterized as the degree of the closeness of the observed value to the standard or real value and it is mathematically represented as

$$A = \frac{T_{Pos} + T_{Neg}}{T_{Pos} + T_{neg} + F_{Pos} + F_{Neg}} \tag{1}$$

Where A denotes the accuracy, T_{Pos} denotes the true positive, T_{Neg} denotes the true negative, F_{Pos} denotes the false positive, and F_{Neg} denotes the false negative.

3.2.2 Loss: The loss is defined as the error condition that occurred in the communication system due to negligence or failure in transmission, processing, and storage.

$$Loss = \frac{\sum_{i=1}^{d_{tot}} \sum_{j=1}^{a_{tot}} \left(d_{i,j}^{org} - d_{i,j}^{privacy} \right)}{d_{tot} \times a_{tot} \times \max_{diff}} \tag{2}$$

where d_{tot}represents the total data, a_{tot}represents the total attributes, $d_{i,j}^{org}$ is the original data, $d_{i,j}^{privacy}$ denotes privacy-preserved data, $\max_{diff}$ and represents the maximum difference between the original and the privacy-preserved data.

3.2.3 Latency: Latency is defined as the delay experienced in the communication system while transmitting the data. The mathematical representation of Latency is given in Eq. 3:

$$L = \frac{Tr_{block} \cdot Z_{Tr}}{\gamma_{down}} + \max_{i \in \{v_{min}, \ldots, v_{max}\}} \left(\frac{Co_{resource}}{Co_{available}} \right) + \psi . Tr_{block} . Z_{Tr} . V_i + \frac{V_{feedback}}{\gamma_{up}} \tag{3}$$

Where L represents the latency, Tr_{block} represents the number of transaction blocks, Z_{Tr} denotes the transaction size, V_i and represents the number of verified users, which lies between the minimum user V_{min} and maximum user V_{max}. $Co_{resource}$ denotes the required computational resource and $Co_{available}$ denotes the available computational resource. ψ represents the pre-defined parameter that can be leveraged from previous block verification. $V_{feedback}$ represents verification feedback size, γ_{down} and γ_{up} denotes the downlink and uplink rate respectively.

3.2.4 Throughput: The throughput is defined as the successful message delivery within a communication channel. For the blockchain framework, the throughput is mathematically represented as:

$$T_{put} = \frac{\left[Z_{block} / Z_{avg} \right]}{I_{block}} \tag{4}$$

where T_{put}denotes throughput, Z_{block}denotes the block size, Z_{avg} denotes the average transaction size, and I_{block}denotes the block interval.

From Figure 2, most of the prevalent methods utilized the time-based evaluation, which is used in 11 papers out of 25 papers selected for review. The second most widely used metric is cost, the third used metric is latency, and the fourth used metric is throughput.

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

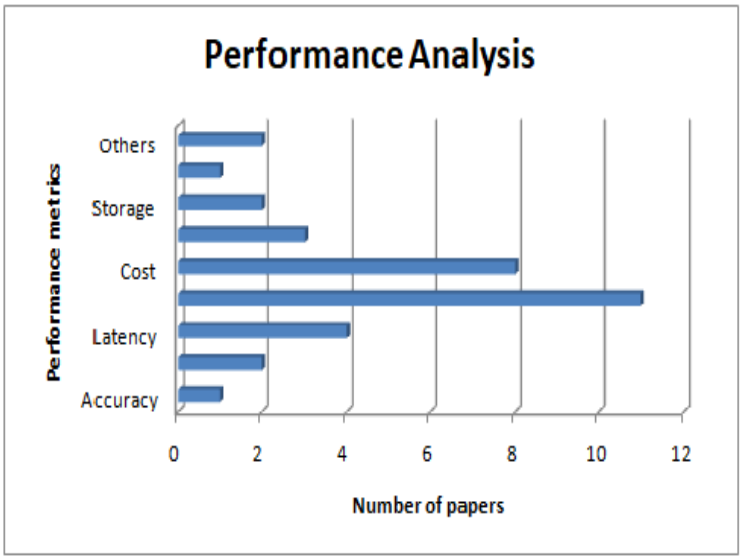

Figure 2: Analysis based on performance metrics

4. Challenges in the usage of Blockchain Technology for data sharing

The analysis of the prevalent blockchain-based secure data-sharing techniques points to certain challenges faced by them. They can be categorized as security and privacy threats, interoperability problems, and storage-related issues. Fig. 3 depicts the categorization of challenges of using blockchain technology for data sharing. These challenges provide research prospects in the area.

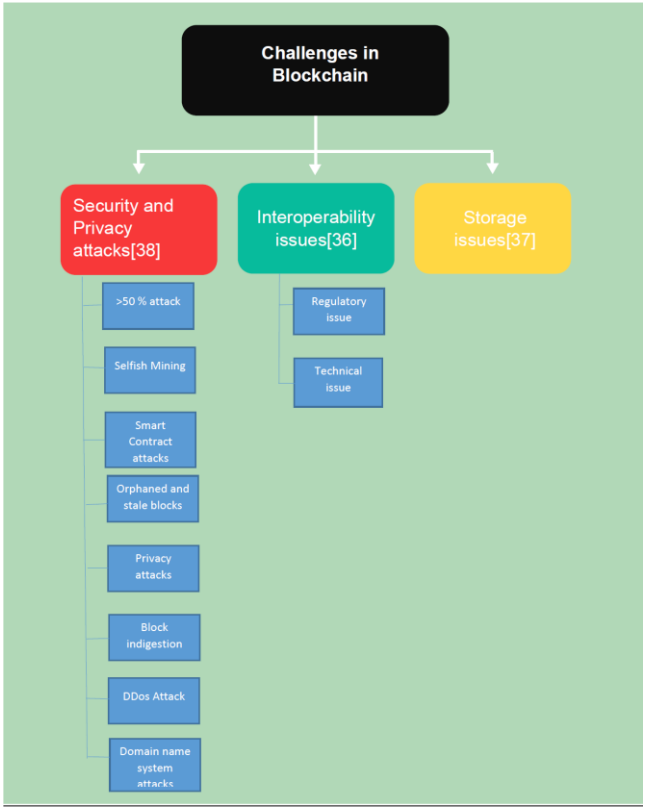

Figure 3: Categorization of challenges in data sharing using Blockchain

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

4.1 Security and Privacy Issues

In blockchain-based data sharing, the need for a third party for privacy preservation is eliminated, and the entire community devises the record verification, and the data authorization is granted to one or more representatives that keep the privacy of data intact and affects the security and privacy of the data. However, security and privacy issues still prevail [31]. Many solutions have been proposed to deal with such issues [32][33][34].

4.2 Interoperability

The communication between the users of Blockchain and the service providers makes them communicate with one another, and hence the hindrances occur that affect secure data sharing leading to the issue of interoperability [23][35]36].

4.3 Storage Issue

Blockchain usage is increasing enormously day to day which occupies enormous data storage. However, the storage space of the Blockchain is limited, which leads to slower data retrieval, and the searching and data accessing will also become slow [37]. Thus, a resilient and scalable blockchain needs to be devised for effective data sharing for real-time applications that require high speed of data access. Researchers are actively working to provide a scalable solution for data sharing using blockchain [38].

5. Conclusion

The decentralized nature of Blockchain technology solves the issue concerning authentication and offers secure data sharing in the network. This technology presents new opportunities to provide services and solutions for internet users. This study presents an analysis of secure data sharing using the blockchain technique. The prevalent secure data-sharing techniques based on Blockchain are analyzed by considering applications such as healthcare, vehicular communication, IoT, and other domains. In addition, an analysis based on the methodologies and the performance metric utilized is provided, which can help the researchers utilize the most preferred metrics. The challenges presented in this study can help researchers develop a novel, secure data-sharing technique based on Blockchain by fulfilling the research gap.

Statements and Declarations

No Competing Interests or Funding are to be disclosed.

Data Availability Statement:

The required data is duly cited in the text of the manuscript. Data would be made available on reasonable request.

Conflict of Interest

On behalf of all authors, the Corresponding author states that there is No Conflict of Interest to disclose.

References

[1] Chaitanya Singh, Deepika Chauhan, Sushama A. Deshmukh, Swati Sudhakar Vishnu, and Ranjan Walia, "Medi-Block record: Secure data sharing using blockchain technology", Informatics in Medicine Unlocked, Vol.24, 2021.

[2] Gautam Srivastava, Reza M. Parizi, Ali Dehghantanha, and Kim-Kwang Raymond Choo, "Data Sharing and Privacy for Patient IoT Devices Using Blockchain", Conference: International Conference on Smart City and Informatization At: Guangzhou, China, November 12-15, 2019.

[3] Atul Banotra, Jyoti Swaroop Sharma, Swastik Gupta, Sachin Kumar Gupta, and Mamoon Rashid, "Use of Blockchain and Internet of Things for Securing Data in Healthcare Systems", In book: Multimedia Security: Algorithm Development, Analysis, and Applications (pp.255-267) Edition: FirstChapter: 14 Publisher: Springer, 2021.

[4] Bingqing Shen, Jingzhi Guo, and Yilong Yang, "MedChain: Efficient Healthcare Data Sharing via Blockchain", Applied Sciences, vol. 9, 2021.

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

[5] Ahmed G. Alzahrani, Ahmed Alenezi, Hany F. Atlam, and Gary Wills, "A Framework for Data Sharing between Healthcare Providers using Blockchain", IoTBDS 2020 - 5th International Conference on Internet of Things, Big Data and Security, 2020.

[6] Qianqian Su, Rui Zhang, Rui Xue, and Pengchao Li, "Revocable Attribute-Based Signature for Blockchain-Based Healthcare System", IEEE Access, vol. 8, 2020.

[7] Rajesh Kumar, WenYong Wang, Jay Kumar, Ting Yang, Abdullah Khan, Wazir Ali, and Ikram Ali, "An Integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals", Computerized Medical Imaging and Graphics, vol. 87, 2021.

[8] Muhammad Firdaus and Kyung-Hyune Rhee, "On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks", Applied Sciences, vol. 11, 2021.

[9] Muhammad Umar Javed, Nadeem Javaid1, Muhammad Waseem Malik, Mariam Akbar, Omaji Samuel, Adamu Sani Yahaya and Jalel Ben Othman, "Blockchain based Secure, Efficient and Coordinated Energy Trading and Data Sharing between Electric Vehicles", Cluster Computing, 2021.

[10] Muhammad Firdaus, Sandi Rahmadika, and Kyung-Hyune Rhee, "Decentralized Trusted Data Sharing Management on Internet of Vehicle Edge Computing (IoVEC) Networks Using Consortium Blockchain", Sensors, vol. 21, 2021.

[11] Yanji Jiang, Xueli Shen, and Sifa Zheng, "An Effective Data Sharing Scheme Based on Blockchain in Vehicular Social Networks", Electronics, vol. 10, 2021.

[12] Kei Leo Brousmiche, Antoine Durand, Thomas Heno, Christian Poulain, Antoine Dalmieres, and Elyes Ben Hamida, "Hybrid Cryptographic Protocol for Secure Vehicle Data Sharing over a Consortium Blockchain", 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, 2018.

[13] Ahsan Manzoor, An Braeken, Salil S. Kanhere, Mika Ylianttila, and Madhsanka Liyanage, "Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain", Journal of Network and Computer Applications, Vol.176, 2021.

[14] Parminder Singh, Mehedi Masud, M. Shamim Hossain and Avinash Kaur, "Cross-Domain Secure Data Sharing using Blockchain for Industrial IoT", Journal of Parallel and Distributed Computing, 2021.

[15] Qing Fan, Jianhua Chen, Lazarus Jegatha Deborah, and Min Luo, "A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain", Journal of Systems Architecture, vol. 117, 2021.

[16] Kwame Opuni-Boachie Obour Agyekum, Qi Xia, Emmanuel Boateng Sifah, Christian Nii Aflah Cobblah, Hu Xia, and Jianbin Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain", IEEE Systems Journal, Vol. 16, No. 1, 2022.

[17] Uma Narayanan, Varghese Paul, and Shelbi Joseph, "Decentralized blockchain based authentication for secure data sharing in Cloud-IoT", Journal of Ambient Intelligence and Humanized Computing, 2021.

[18] Tanzeela Sultana, Ahmad Almogren, Mariam Akbar, Mansour Zuair, Ibrar Ullah and Nadeem Javaid, "Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices", Applied Sciences, vol. 10, 2020.

[19] Kwame Opuni-Boachie Obour Agyekum, Qi Xia, Emmanuel Boateng Sifah, Jianbin Gao, Hu Xia, Xiaojiang Du and Moshen Guizani, "A Secured Proxy-Based Data Sharing Module in IoT Environments Using Blockchain", Sensors, Vol. 19, 2019.

[20] Peichang Shi, Huaimin Wang, Shangzhi Yang, Chang Chen, and Wentao Yang, "Blockchain-based trusted data sharing among trusted stakeholders in IoT", Software practice and Experience, vol. 51, No.10, 2021.

[21] Muqaddas Naz, Fahad A. Al-zahrani, Rabiya Khalid, Nadeem Javaid, Ali Mustafa Qamar, Muhammad Khalil Afzal and Muhammad Shafiq, "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System", Sustainability, vol. 11, 2019.

[22] Xuanmei Qin, Yongfeng Huang, Zhen Yang, and Xing Li, "A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing", Journal of Systems Architecture, 2020.

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023

[23] Q. Tao, Q. Chen, H. Ding, I. Adnan, X. Huang, and X.Cui, "Cross-Department Secures Data Sharing in Food Industry via Blockchain-Cloud Fusion Scheme", Security and Communication Networks Volume 2021, 2021.
[24] Imran Makhdoom, Ian Zhou, Mehran Abolhasan, Justin Lipman, Wei Ni, "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities", Journal of Computers and Security, 2019.
[25] Jie Cui, Fenqiang Ouyang, Zuobin Ying, Lu Wei, and Hong Zhong, "Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain", IEEE Transactions on Intelligent Transportation Systems, 2021.
[26] Feng, C., Yu, K., Bashir, A.K., Al-Otaibi, Y.D., Lu, Y., Chen, S. and Zhang, D., "Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach", IEEE Network, vol.35, no.1, pp.130-137, 2021.
[27] Manogaran, G., Alazab, M., Shakeel, P.M. and Hsu, C.H., "Blockchain assisted secure data sharing model for Internet of Things based smart industries". IEEE Transactions on Reliability, vol.71, no.1, pp.348-358, 2021.
[28] Wang, D. and Zhang, X., "Secure data sharing and customized services for intelligent transportation based on a consortium blockchain", IEEE Access, vol.8, pp.56045-56059, 2020.
[29] Eltayieb, N., Elhabob, R., Hassan, A. and Li, F., "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud", Journal of Systems Architecture, vol.102, pp.101653, 2020.
[30] Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C. and Qiu, T.,"A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things", Journal of Network and Computer Applications, vol.167, pp.102710, 2020.
[31] Joshi, A. P., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. Mathematical foundations of computing, 1(2), 121.
[32] Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. Internet of Things, 8, 100107.
[33] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal, 8(2), 881-888.
[34] Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications, and future research directions. Computers & Electrical Engineering, 90, 106897.
[35] Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. ACM Computing Surveys (CSUR), 54(8), 1-41.
[36] Reegu, F., Daud, S. M., & Alam, S. (2021). Interoperability challenges in healthcare blockchain system-A systematic review. Annals of the Romanian Society for Cell Biology, 15487-15499.
[37] Arigela, S. S. D., & Voola, P. (2022, January). Detecting and Identifying Storage issues using Blockchain Technology. In 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-7). IEEE.
[38] Fan, X., Niu, B., & Liu, Z. (2022). Scalable blockchain storage systems: research progress and models. Computing, 104(6), 1497-1524.

Doi: https://doi.org/10.54216/FPA.100204
Received: November 19, 2022 Accepted: March 09, 2023