A Comprehensive Survey of Access Control Schemes in Block-chain Systems for Ensuring Security and Privacy

Mr. Akshay Shankar Agrawal[1], Dr. Rahul Thour[2]

[1]Ph.D. (CSE) Scholar, Desh Bhagat University, Punjab
[2]Assistant Professor, Department of CSE, Desh Bhagat University, Punjab

ABSTRACT

Access control (AC) is a significant aspect of maintaining a secure system, empowering users to manage who can access their data as well as ensuring the confidentiality of sensitive information. Blockchain technology has the ability to transform access control systems by offering a secure, transparent, and decentralized method for users to control their digital identities. Additionally, a Blockchain based AC system empowers the user to handle their data, allowing them to grant or revoke access as necessary without relying on centralized authorities. Nevertheless, privacy and security problems obstruct the diverse utilization of smart health care systems. In addition, the Internet of Medical Things (IoMT) raises several safety and privacy-related concerns. Furthermore, it is difficult to create a common security standard solution due to the diverse nature of these devices. The analyzed techniques faced some challenges in various protocols such as data security, real-time scenarios, and computational complexity. This research investigates AC schemes to decrease computation complexity as well as develops advanced mobile applications for secure data-sharing. Additionally, it also addresses enriching real-world scenarios with smart contracts as well as better performance metrics which make more effective Blockchain-based access control schemes for ensuring privacy and security issues.

Keywords: Access control policies, Blockchain Networks, Privacy, Third-party Authentication, security.

INTRODUCTION

The widespread use of mobile devices, networking, and wireless communication technologies over the last few decades has made the world a more united place [34]. To reduce the need for repeat evaluations and increase the accessibility of patient medical records, they are increasingly using mobile devices for medical purposes. Nonetheless, there are significant operational, legal, as well as technological obstacles related to the sharing and privacy of medical data [12].

Cloud storage technology offers strong data storage capacity by utilizing the storage capacity of cloud servers [28].

Storing data in the cloud, allows data owners to get around the limitation of user terminal storage resources. As a result, cloud storage has grown in popularity recently in several industries including electronic health records (EHR) [29, 30], the Industrial Internet of Things (IIoT) environment [31], as well as the Internet of Things (IoT) [5] [32, 33]. With the increasing number of digital objects that are connected to the Internet is driving exponential growth in the IoT. The IoT devices gather information from their surroundings and can share this information with different organizations [9].

Unfortunately, the centralized servers used by the current digital health care systems make them more vulnerable to security lapses. Due to several uses as well as enhanced security, Blockchain technology makes the most sense for integrating the digital health care system [22]. In digital asset management, Blockchain technology has a decentralized distributed ledger scheme that offers trace-ability, smart contracts and transparency [23] [35]. Blockchain was built on three main components such as concurrency control, public key encryption, and peer-to-peer networking.

Managing authorization was the foundation for all three types of Blockchain including consortium, private, and public [11]. As a result, in case of the single-point failure, the system can continue to function normally [3]. The single point failure is because of the centralized authorized decision-making entity in access control, which was resolved by utilizing the blockchain's decentralized features. Several agencies must work together to accomplish AC when there is cross-domain access [2]. In addition, a user lacks confidence in the third party as well as unaware of the location and handling of their data. Is it disclosed to third parties without authorization, and who has access to it [9]. One of the key technologies for protecting privacy is AC, which can effectively stop the leak of medical data. Consequently, the integration of AC as well as Blockchain technology can address the issue of distributed storage and anti-tampering with medical data in addition to partially preventing privacy leakage [25]. Applying Blockchain technology to the medical field can help to find quick and efficient ways for various institutions to share medical data, increasing the precision and efficiency of diagnosis in the field of medicine as well as encouraging the development of intelligent medical systems [4] [26, 27]. In contrast, prime-order linearity was utilized in the majority of AC schemes on cloud platforms to minimize computational overhead. The lower security of this design resulted from its reduced computational burden [5].

This research aims to analyze and evaluate various AC schemes in Blockchain systems for ensuring privacy as well as security in several applications. In this survey around 25 research articles are analyzed focusing on the taxonomy of literature review, challenges faced, performance metrics, and future works. The research focused to provide a detailed overview for future research to design advanced techniques in mobile applications, low computation and communication complexity as well as effective Blockchain systems for security and privacy issues.

This article is classified into the following sections. The taxonomy of the literature review of AC schemes in Blockchain systems is explained in Section 2. Section 3 provides a summary analysis of metrics, schemes, limitations and achievements. Section 4 discusses the research gaps. Section 5 evaluates the performance metrics, and the conclusion and future works in section 6.

LITERATURE REVIEW

This section explores the advantages of AC schemes in Blockchain systems for ensuring security and privacy. Figure 2.2.1. displays the taxonomy outline of the AC scheme in Blockchain systems.

Taxonomy of AC Schemes in Blockchain Systems

Kebira Azbeg et al. [1] and Chia-Hung Liao et al. [20] introduced an Ethereum Blockchain - based on proof of authority (PoA), a consensus algorithm, utilized to reach agreements as well as secure permission Blockchain networks. It can enhance efficiency of data storage by expediting the consensus process which is mainly crucial in health care systems that necessitate real-time processing. In [20], PoA depended upon small groups of sealers, and the ecosystem required the involvement of Banks as well as RAs to guarantee the tracking of access records.

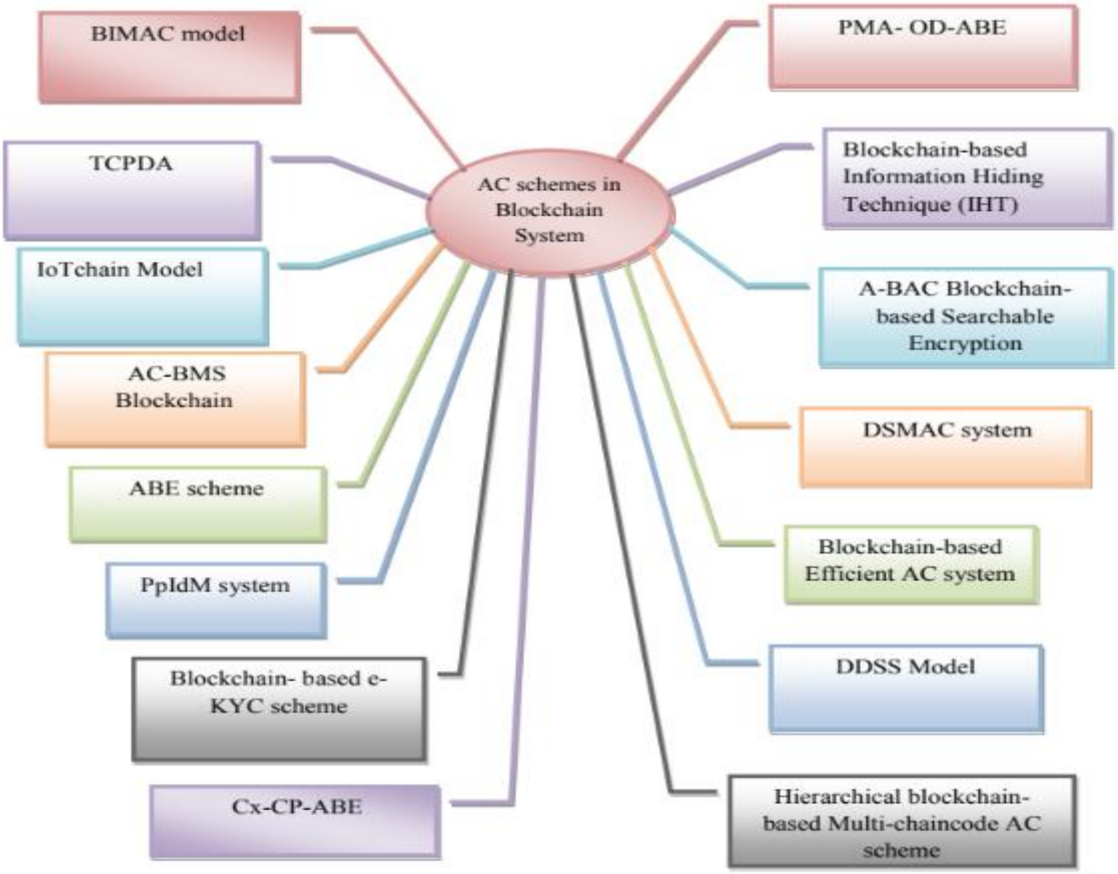
AC schemes in Blockchain System
BIMAC model
TCPDA
IoTchain Model
AC-BMS Blockchain
ABE scheme
PpIdM system
Blockchain- based e-KYC scheme
Cx-CP-ABE
PMA- OD-ABE
Blockchain-based Information Hiding Technique (IHT)
A-BAC Blockchain-based Searchable Encryption
DSMAC system
Blockchain-based Efficient AC system
DDSS Model
Hierarchical blockchain-based Multi-chaincode AC scheme

Figure 2.1.1.: Taxonomy diagram of AC scheme in Blockchain System

To establish a sure and reliable access environment as well as authenticate visitors, Alessandra Rizzardi et al. [17], Bhaskara S. Egala et al. [23], and Liang Yang et al. [25] employed a tamper-proof method. This ensured the safety and dependability of the data used in the accessing process. Through tamper-proof public ledgers based on Blockchain technology, system-level trace ability can be achieved. In addition, Xingyu He et al. [10] presented an Offshore Banking Unit (OBU) which is a tamper-proof device, capable of some computation as well as communication. Vehicles may communicate in real-time via the dedicated short-range communication (DSRC) protocol with nearby cars and restricted stock units (RSUs) about their driving conditions as well as the current state of traffic by utilizing OBUs.

In 2022, Duo Zhang et al. [4] and Zia Ullah et al. [15] provided an A-BAC approach to specify AC guidelines and use smart contracts to automatically carry them out throughout the blockchain network. By analyzing user requests as well as environmental attributes, A-BAC has controlled access to the resource. Furthermore, it has provided cryptographic solutions for issues resolved by conventional AC systems. In Adam Ibrahim Abdi et al. [9] A-BAC encrypted the IoT stream before uploading it to IPFS for improved data security as well as privacy.

Xiaodong Yang et al. [5], Pratima Sharma et al. [12], Somchart Fugkeaw [7], Boubakeur Annane et al. [18], and Yinghui Zhang et al. [24] constructed the CP-ABE scheme, which concealed access policies to prevent privacy breaches as well as ensure that the system was not reliant on a single authority. With fine-grained AC, one-to-many encryption was provided by CP-ABE which permits multiple FIs to access shared transactional encrypted data in the blockchain of a single user under the specified access policy. Furthermore, it has provided more effective and scalable settings for the cloud data. Xueli Nie et al. [19] utilized KP-ABE, another type of ABE, to achieve privacy preservation as well as data security. It ensured that health data in edge-based IoMT was secure and private through the use of the KP-ABE approach.

Haiying Wen et al. [13], Jiujiang Han et al. [21], and Aitizaz Ali et al. [22] introduced a searchable encryption (SE) technology. Encrypted calculations as well as cipher text of data can be realized with SE technology that has enabled users to perform secure keyword-based searches and retrieve keywords from encrypted text. To maintain data security, SE allowed users to store the encrypted data in the Blockchain, conduct searches of keywords through the cipher text domain as well as recover pertinent documents only.

To address unauthorized vulnerabilities Jinshan Shi et al. [2] implemented two methods including TCPDA and PRPDA. As a result, the time overhead of these two methods has increased, as has the space overhead. The permission delegation algorithm (PDA) required a lot less time than the consensus algorithm, as well as the probability of PDA events was increased then the storage overhead gradually decreased. The Conditional Privacy-Preserving and Authentication (CPPA) method was modeled by Kashif Naseer Qureshi et al. [3] to solve the security and privacy issues in VANETs. In addition, CPPA reduced the computational cost of message verification. Duc Anh Luong and Jong Hwan Park [6] implemented z-SNARK, which is a type of zero-knowledge proof (ZKP) that satisfied the soundness property.

This scheme was susceptible to collusion attacks, where several clients can concurrently utilize a certificate as the witness of z-SNARK’s. Yue Wang et al. [8] designed several algorithms such as IIoT, Intelligent Elliptic Curve Digital Signature Algorithm (IECDSA), Reputational-based Delegation Proof of Stake (RDPoS), and DPoS to solve the security sharing problems. Furthermore, these algorithms enhanced the data consistency security among smart factories as well as reducing the probability of vicious nodes being chosen as delegate nodes.

Hanan Naser Alsuqaih et al. [11] presented a Blockchain-based efficient AC system for e-health applications. It has demonstrated the blockchain’s computational and time-saving efficiency as well as its ability to different security threats. An information-hiding technique was employed by Abir El Azzaoui et al. [14] to improve data communication security and privacy in other critical systems.

As a result, it was employed a Hyper-ledger smart contract as well and the required degree of security was feasible. Shuyun Shi et al. [16] introduced a Blockchain-based user authentication scheme that incorporates physical unclonable functions (PUF) and AC to identify the devices as well as facilitate secure data sharing through health care applications. Compared to existing methods, it has achieved minimum computation and communication costs.

Summarized Analysis:

Table 3.1.: The summarized Analysis of AC schemes in a Blockchain system for ensuring security and privacy

S.No	Model	Metrics	Achievements	Research gaps
1	Blockchain-based system for securing IoT health care devices.	Transaction-Throughput.	Transaction throughput- 45 transactions per second (tps).	The performance of the model was limited in real-time analysis.
2	Token-Constrained Permission Delegation Algorithm (TCPDA).	Storage cost.	Storage cost- 73.15%	Due to insecurity in the permission delegation process, the TCPDA scheme has provided permission to the entire receiver.
3	Blockchain-enabled Internet of Vehicles (IoV) networks.	Reputation threshold and transaction throughput.	Reputation threshold- 0.25, and Transaction throughput- 140 tps.	The IoV network has decreased the accuracy of the reputation as well as low efficiency.
4	Medical Data sharing scheme based on a Consortium Blockchain.	Time-cost.	Time-cost- 0.45	This scheme did not apply to human domain networks.
5	Blockchain and Attribute-based Encryption (ABE) scheme.	Time-complexity.	Time-cost- 0.21	Required to improve the cloud storage technology for multi-authorization centers.
6	Privacy-preserving Identity Management (PpIdM) system.	Time-complexity	Time-complexity- 106.24 seconds (s).	The PpIdM system reduced the number of validators which prevented the normal working of (k, n) –threshold SSS scheme.
7	Blockchain-based e-KYC scheme.	Transaction throughput.	Transaction throughput- 200 tps	In this approach, the e-KYC scheme was only suitable for small-scale data.
8	Blockchain-based Privacy Information Security sharing scheme in IIoT.	-	-	This method did not perform in real local area networks (LAN).
9	Hierarchical Blockchain-based Multi-chain code AC scheme.	Transaction latency and transaction throughput.	Transaction latency- 107 ms, and Transaction throughput- 100 tps	The hierarchical Blockchain-based technology has high latency.
10	Hierarchical blockchain-assisted CPPA scheme for Vehicular Adhoc Networks (VANETs).	Communication cost.	Communication cost- 180 bytes.	The Vehicle Adhoc Network has less improvement in the authentication scheme.
11	Blockchain-based Efficient AC system.	Processing time.	Processing time- 5 s	This scheme did not resist the quantum attack techniques.
12	Decentralized Self-Management of Data Access Control (DSMAC) system.	Encryption time.	Encryption time- 26 ms	The performance of the EHR was poor in this system.
13	Privacy-preservation scheme in Mobile Medical.	Latency and Transaction throughput.	Latency- 0.48, and Throughput- 256.1	This scheme has limited diversified search functions.
14	Blockchain-based Information Hiding Technique (IHT).	Latency.	Latency- 60 s	In real-world scenarios, the encryption and decryption phase of smart contract-based One-Time Hash (OTH) was limited in other critical systems.

15	IoT chain Model.	Transaction cost and Execution cost.	Transaction cost-304076, and Execution cost-214378	The IoT chain model could not support user attribute revocation as well as updating of A-BAC policy.
16	Blockchain-based User Authentication scheme with AC for Telehealth system.	Computation cost as well as Communication cost.	Computation cost-13.218 ms, and Communication cost- 4320 bits.	This technology required more flexible AC updates as well as high computational and communication complexity.
17	Permissioned Blockchain-based IoT scheme.	Data rate and latency.	If the data rate is-10 tps, then the latency rate is- 8 s	It was not suitable for complex environments as well as diverse data sources.
18	Electronic-health Mobile Application-based Context-aware Cipher-text Policy-ABE (Cx-CP-ABE) algorithm.	Execution time as well as Communication cost.	Execution time-8149 ms, and Communication cost- 3100 bits	Difficult to predict all possible behaviors of invaders in this model.
19	Blockchain-assisted Data sharing scheme.	Computational overhead.	Computational overhead- 368 ms	Limited performance in edge-based IoMT applications.
20	Blockchain-based Identity Management and AC (BIMAC) model.	Transaction throughput.	Throughput of authorization- 150 tps Throughput of revocation- 350 tps	The generalization ability was limited in the BIMAC model.
21	A-BAC Blockchain-based Searchable Encryption.	Gas cost.	Gas cost- 38, 347, 029 wei	A-BAC scheme has high computational complexity.
22	Deep-learning-based Secure Searchable Blockchain system.	Accuracy.	Accuracy- 90.6%	For better classification, the model required more deep-learning approaches.
23	Blockchain-based Distributed Data Storage System (DDSS)	Storage cost.	Storage cost- 0.13	This technique did not improve the health care services due to poor robustness as well as limited quality of services (QoS).
24	Blockchain-based Payable multi-authority ABE scheme with Outsourcing Decryption (PMA-OD-ABE).	Computational overhead.	Computational overhead- 80 ms	Implementing the trace ability mechanism and attribute revocation of the Smart Health System (SHS) was a challenging task in this scheme.
25	AC-based Blockchain main and side chains (AC-BMS)	Access time.	Average access time- 6.523 s	Ethereum master chain nodes' request type was difficult to recognize under high concurrent access requests.

Research Gaps

- The IoT network has decreased the accuracy of the reputation as well as low efficiency. Implementing with real-world application made this scheme more realistic which led to a challenging task [3].
- The medical data-sharing method based on consortium Blockchain did not apply to human domain networks. Developing security sharing of medical data in wearable devices as well as IoT was more challenging in this scheme [4].
- In real-world scenarios, the encryption and decryption phase of smart contract-based OTH was not enhanced in other critical systems [14].
- Blockchain-based user authentication technology for Telehealth systems has required more flexible AC updates as well as high computational and communication complexity [16].
- The Blockchain-based IoT faced difficulties in more complex environments as well as diverse data sources [17].
- The A-BAC technique has high computational complexity because of two-layer circular matching [21].
- The DL-based SSE model did not perform with different DL approaches due to poor classification [22].
- The DDSS technique did not improve health care services due to poor robustness as well as limited QoS capability [23].

- Implementing the trace ability mechanism and attribute revocation of the SHS was a challenging task in the PMA-OD-ABE scheme [24].
- The Ethereum master chain nodes' request type was difficult to recognize under high concurrent access requests because of the large complexity [25].

Performance Metrics

There are various performance metrics analyzed in this research including transaction throughput, transaction latency, execution time, computation, and communication cost which are described as follows:

Transaction Throughput

The transaction throughput (T_{rth}) defines the speed at which the network of Blockchain processes and confirms validated transactions within a specific time frame. This is commonly expressed as Transaction per Second (TPS) and is indicative of the network's capacity. The mathematical representation of the transaction throughput is shown in equation (1).

$$T_{rth} = T_{rcom} / T_{tot} \times N_{com} \tag{1}$$

where T_{rcom} stands for the committed total transactions, T_{tot} represents the time in seconds, and N_{com} is the number of committed nodes.

Transaction Latency

The transaction latency (T_{rlat}) defines the duration that takes for a transaction's impact to be accessible across the network which is mathematically expressed in equation (2).

$$T_{rlat} = (T_{con} \times N_{tr}) - T_{sub} \tag{2}$$

Where T_{con} denotes the confirmation time, N_{tr} stands for the network threshold, and T_{sub} is the submit time of the transaction.

Execution time

The time takes to encrypt or decrypt messages depends on the total number of features in the access policy. This is known as Execution time.

Computational and Communication Cost

The computational cost is defined by the total number and complexity of tasks that a processor executes per time step in a simulation. Similarly, the communication cost of a localization scheme is determined by the average number of messages exchanged to complete the localization task. These costs are critical factors in the design and efficiency of computational processes and communication protocols, respectively. The analysis of several AC schemes in the Blockchain systems based on performance metrics is illustrated in Table 5.4.1. and Figure 5.4.1.

Table 5.4.1.: Analysis based on performance metrics

S. No	Performance metrics	Citations
1	Transaction Throughput	[1] [3] [7] [9] [13] [20]
2	Storage cost	[2] [23]
3	Transaction Latency	[9] [13] [14] [17]
4	Computation cost	[16] [19] [24]
5	Communication cost	[10] [16] [18]
6	Time cost	[4] [5]
7	Accuracy	[22]
8	Access time	[25]
9	Gas cost	[21]
10	Execution time	[18]
11	Execution cost	[15]
12	Processing time	[11]
13	Encryption time	[12]
14	Transaction cost	[15]
15	Time complexity	[6]

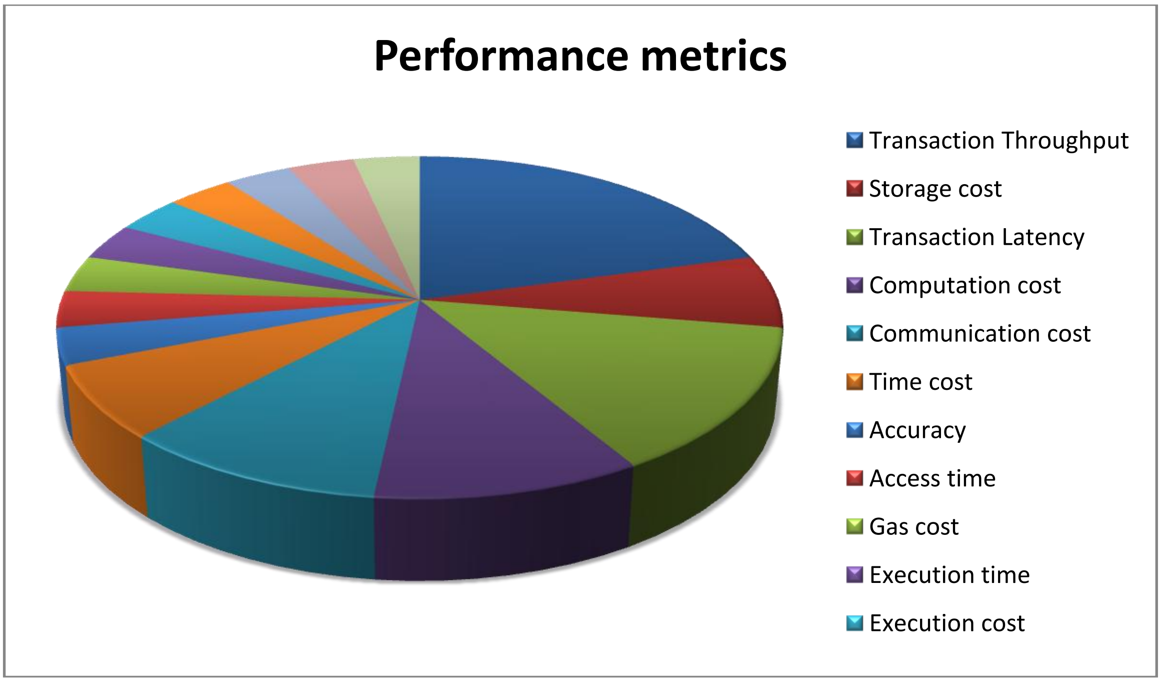

Figure 5.4.1.: Analysis based on performance metrics

CONCLUSION AND FUTURE WORK

This survey addresses AC schemes in Blockchain systems for ensuring security as well as privacy in several fields including IoT, IoMT, and health care applications. In this survey, various AC schemes in Blockchain systems are analyzed. Blockchain-based user authentication technology for Telehealth systems has required more flexible AC updates as well as high computational and communication complexity. In addition, the IoT chain model could not support user attribute revocation as well as updating of ABAC policy. Blockchain-based ABE scheme has required improving the cloud storage technology for multi-authorization centers. Moreover, the generalization ability was poor in the BIMAC approach. The analyzed techniques have faced more challenges in various protocols such as data-sharing mechanisms, data security, high latency, real-time scenarios, and computational complexity. To overcome these limitations, the future avenue will be focused on implementing advanced technologies in mobile applications, developing smart contracts in real-world scenarios as well as improving the performance of metrics including latency, transaction throughput, and so on. Furthermore, it will investigate the AC scheme to reduce the computational complexity and also an effective Blockchain system for ensuring security and privacy.

REFERENCES

[1]. Azbeg, K., Ouchetto, O. and Andaloussi, S.J., 2022. Access control and privacy-preserving Blockchain-based system for diseases management. IEEE Transactions on Computational Social Systems.

[2]. Shi, J., Li, R. and Hou, W., 2020. A mechanism to resolve the unauthorized access vulnerability caused by permission delegation in Blockchain-based access control. IEEE Access, 8, pp.156027-156042.

[3]. Qureshi, K.N., Shahzad, L., Abdelmaboud, A., Elfadil Eisa, T.A., Alamri, B., Javed, I.T., Al-Dhaqm, A. and Crespi, N., 2022. A Blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the internet of vehicles. Applied Sciences, 12(1), p.476.

[4]. Zhang, D., Wang, S., Zhang, Y., Zhang, Q. and Zhang, Y., 2022. A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain. Security and Communication Networks, 2022(1), p.2759787.

[5]. Yang, X., Chen, A., Wang, Z. and Li, S., 2022. Cloud Storage Data Access Control Scheme Based on Blockchain and Attribute-Based Encryption. Security and Communication Networks, 2022(1), p.2204832.

[6]. Luong, D.A. and Park, J.H., 2023. Privacy-preserving identity management system on Blockchain using Zk-SNARK. IEEE Access, 11, pp.1840-1853.

[7]. Fugkeaw, S., 2022. Enabling trust and privacy-preserving e-KYC system using Blockchain. IEEE Access, 10, pp.49028-49039.

[8]. Wang, Y., Che, T., Zhao, X., Zhou, T., Zhang, K. and Hu, X., 2022. A Blockchain-based privacy information security sharing scheme in Industrial Internet of Things. Sensors, 22(9), p.3426.

[9]. Abdi, A.I., Eassa, F.E., Jambi, K., Almarhabi, K., Khemakhem, M., Basuhail, A. and Yamin, M., 2022. Hierarchical Blockchain-based multi-chaincode access control for securing IoT systems. Electronics, 11(5), p.711.

[10]. He, X., Niu, X., Wang, Y., Xiong, L., Jiang, Z. and Gong, C., 2022. A hierarchical blockchain-assisted conditional privacy-preserving authentication scheme for vehicular ad hoc networks. Sensors, 22(6), p.2299.

[11]. Alsuqaih, H.N., Hamdan, W., Elmessiry, H. and Abulkasim, H., 2023. An efficient privacy-preserving control mechanism based on Blockchain for E-health applications. Alexandria Engineering Journal, 73, pp.159-172.

[12]. Sharma, P., Jindal, R. and Borah, M.D., 2022. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. the Journal of Supercomputing, 78(6), pp.7700-7728.

[13]. Wen, H., Wei, M., Du, D. and Yin, X., 2022. A Blockchain-Based Privacy Preservation Scheme in Mobile Medical. Security and Communication Networks, 2022(1), p.9889263.

[14]. El Azzaoui, A., Chen, H., Kim, S.H., Pan, Y. and Park, J.H., 2022. Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems. Sensors, 22(4), p.1371.

[15]. Ullah, Z., Raza, B., Shah, H., Khan, S. and Waheed, A., 2022. Towards Blockchain-based secure storage and trusted data sharing scheme for IoT environment. IEEE access, 10, pp.36978-36994.

[16]. Shi, S., Luo, M., Wen, Y., Wang, L. and He, D., 2022. A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems. Security and Communication Networks, 2022(1), p.6735003.

[17]. Rizzardi, A., Sicari, S., Miorandi, D. and Coen-Porisini, A., 2022. Securing the access control policies to the Internet of Things resources through permissioned Blockchain. Concurrency and Computation: Practice and Experience, 34(15), p.e6934.

[18]. Annane, B., Alti, A., Laouamer, L. and Reffad, H., 2022. Cx-CP-ABE: Context-aware attribute-based access control schema and Blockchain technology to ensure scalable and efficient health data privacy. Security and Privacy, 5(5), p.e249.

[19]. Nie, X., Zhang, A., Chen, J., Qu, Y. and Yu, S., 2022. Blockchain-empowered secure and privacy-preserving health data sharing in edge-based IoMT. Security and Communication Networks, 2022(1), p.8293716.

[20]. Liao, C.H., Guan, X.Q., Cheng, J.H. and Yuan, S.M., 2022. Blockchain-based identity management and access control framework for open banking ecosystem. Future Generation Computer Systems, 135, pp.450-466.

[21]. Han, J., Li, Z., Liu, J., Wang, H., Xian, M., Zhang, Y. and Chen, Y., 2022. Attribute-based access control meets blockchain-enabled searchable encryption: A flexible and privacy-preserving framework for multi-user search. Electronics, 11(16), p.2536.

[22]. Ali, A., Pasha, M.F., Ali, J., Fang, O.H., Masud, M., Jurcut, A.D. and Alzain, M.A., 2022. Deep learning based homomorphic secure search-able encryption for keyword search in Blockchain health care system: A novel approach to cryptography. Sensors, 22(2), p.528.

[23]. Egala, B.S., Pradhan, A.K., Badarla, V. and Mohanty, S.P., 2021. Fortified-chain: a Blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal, 8(14), pp.11717-11731.

[24]. Zhang, Y., Wei, X., Cao, J., Ning, J., Ying, Z. and Zheng, D., 2022. Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart health care. Journal of King Saud University-Computer and Information Sciences, 34(10), pp.8350-8361.

[25]. Yang, L., Jiang, R., Pu, X., Wang, C., Yang, Y., Wang, M., Zhang, L. and Tian, F., 2024. An access control model based on Blockchain master-sidechain collaboration. Cluster Computing, 27(1), pp.477-497.

[26]. Hölbl, M., Kompara, M., Kamišalić, A. and Nemec Zlatolas, L., 2018. A systematic review of the use of Blockchain in health care. Symmetry, 10(10), p.470.

[27]. Mackey, T.K., Kuo, T.T., Gummadi, B., Clauson, K.A., Church, G., Grishin, D., Obbad, K., Barkovich, R. and Palombini, M., 2019. 'Fit-for-purpose?'–challenges and opportunities for applications of Blockchain technology in the future of health care. BMC medicine, 17, pp.1-17.

[28]. Yang, H., Yi, Z., Li, R., Tu, Z., Wang, X.A., Cui, Y. and Yang, X., 2021. Improved outsourced provable data possession for secure cloud storage. Security and Communication Networks, 2021(1), p.1805615.

[29]. Joshi, M., Joshi, K. and Finin, T., 2018, July. Attribute based encryption for secure access to cloud based EHR systems. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 932-935). IEEE.

[30]. Walid, R., Joshi, K.P., Choi, S.G. and Kim, D.Y., 2020, December. Cloud-based encrypted ehr system with semantically rich access control and searchable encryption. In 2020 IEEE international conference on big data (Big Data) (pp. 4075-4082). IEEE.

[31]. Qi, S., Lu, Y., Wei, W. and Chen, X., 2020. Efficient data access control with fine-grained data protection in cloud-assisted IIoT. IEEE Internet of Things Journal, 8(4), pp.2886-2899.

[32]. Cai, H., Xu, B., Jiang, L. and Vasilakos, A.V., 2016. IoT-based big data storage systems in cloud computing: perspectives and challenges. IEEE Internet of Things Journal, 4(1), pp.75-87.

[33]. Kim, W.B., Seo, D., Kim, D. and Lee, I.Y., 2021. Group Delegated ID-Based Proxy Reencryption for the Enterprise IoT-Cloud Storage Environment. Wireless Communications and Mobile Computing, 2021(1), p.7641389.

[34]. Tao, J. and Ling, L., 2021. Practical medical files sharing scheme based on Blockchain and decentralized attribute-based encryption. IEEE Access, 9, pp.118771-118781.

[35]. Biswas, S., Sharif, K., Li, F. and Mohanty, S., 2020. Blockchain for e-health-care systems: Easier said than done. Computer, 53(7), pp.57-67.