Review Article

ACCENTS Transactions on Image Processing and Computer Vision, Vol 9(24)
ISSN (Online): 2455-4707
http://dx.doi.org/10.19101/TIPCV.2023.924001

A review of blockchain cyber security

Animesh Kumar Dubey[*]
Assistant Professor, Madhyanchal professional University Bhopal, India

Received: 04-January-2023; Revised: 10-February-2023; Accepted: 14-February-2023

Abstract

The aim of this review paper is to provide a comprehensive understanding of blockchain security. As cyber-attacks continue to increase, there is a growing need for secure technologies, and blockchain technology has emerged as a promising solution. However, this technology also faces its own set of challenges related to attacks and code encryption. The paper delves into these challenges, along with potential solutions for enhancing blockchain security. The review paper discusses various methods and techniques that have been proposed to ensure the security of blockchain technology. It covers topics such as consensus algorithms, encryption methods, and access control mechanisms. It provides detailed results about several methods used in blockchain security. The paper also discusses the potential implications of using blockchain technology for security purposes in different domains, such as finance, healthcare, and supply chain management. By providing a comprehensive understanding of the challenges and potential solutions in blockchain security, this review paper can serve as a useful resource for researchers and practitioners working in the field.

Keywords

Blockchain security, Cyber-attacks, Consensus algorithms, Encryption methods, Access control mechanisms.

1.Introduction

Blockchain technology enables people in managing trusted transactions among mistrusted contributors in the existing network system [1]. Different blockchain systems such as Hyperledger Fabric and Ethereum have emerged with private and public accessibility exterior of the electronic voucher and fiat currency systems. As stated by Zhang et al. (2019) [2], in recent times, Blockchain technology has become more popular in the field of scientific research. As opined by Tanwar et al. (2019) [3], from the perceptive of data management, it can be said that Blockchain is a distributed database, which records a list of transaction records by arranging them into a hierarchical order. As per the view of Dwivedi et al. (2019) [4], under the context of security, the Blockchain is maintained and created by utilising an overlay network and secured through decentralised and intelligent use of cryptography along with crowd computing. In contrast to Islam and Kundu (2019) [5], blockchain enables people to traceability and verification multiple transactions requiring verification. It may offer secure transactions by speeding up the process of data transfer and reducing compliance costs.

The number of cyberattacks is significantly increasing day by day, which creates a grievous impact on the living standard of people [1]. Both individuals and organisations are facing cybersecurity issues, resulting in hindering the brand reputation and raising the cost of data breaches. Around 51% of cyberattacks may occur when attackers gain control of the blockchain token [6]. Besides, the attack can take place if the Blockchain does not work properly in terms of verification and secure transactions. It is noticed that Blockchain attackers have stolen $1.4 billion by the end of 2021 due to poor security measures in blockchain networks [7]. As stated by Demirkan et al. (2020) [8], since the rise of Bitcoin in 2008, Blockchain technology has come into the trend. Although the use of blockchain technology has increased in managing the security field, data breaches are also rising gradually. However, it indicates the poor security measure and policies that have been adopted by organisations. As suggested by Le et al. (2020) [9], encrypted code and machine learning methods need to be used by people while making financial transactions. Previous research work did not include effective strategies that can help to reduce the rate of cyberattacks. Therefore, developing a security policy for Blockchain has become a major challenge in recent times. Major challenges in the blockchain adoption are shown in *Figure 1*.

[*]Author for correspondence

In recent times, the emergence of blockchain technology has become the most disruptive, trending, and unique technology [3]. As per the view of Taylor et al. (2020) [1], blockchain technology mainly supports transactions and the decentralised database in the financial sector. It is used as a secure technology in every field like Internet of Things (IoT) applications, Cloud applications, financial activities and many others. According to Aldasoro et al. (2022) [10], the number of cyberattacks is growing, in turn, the average cost of global data breaches has increased to 2.6% in 2022. That is why people and organisations need to place a strong emphasis on using blockchain technology to maintain security in various types of applications. In this instance, the researcher has decided to choose this blockchain security topic to increase the utilisation of this technology in managing security and address the gap of this existing technology.

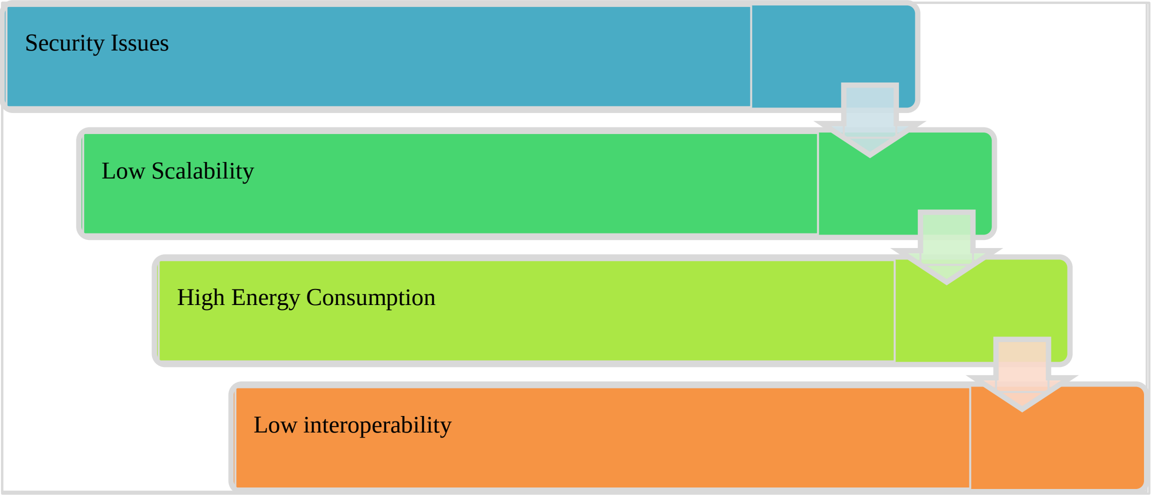


Figure 1 Major challenges in blockchain adoption

The primary objective of this research paper is to analyse the concept of blockchain cybersecurity. Additionally, this research work will highlight the ways of securing IoT and cloud generated data through blockchain technology.

The research work presented in this paper has thoroughly analyzed and reviewed all the complex aspects related to blockchain security. The study covers a broad range of factors that contribute significantly to the security of blockchain. One of the significant contributions of this research is the classification and evolution of blockchain, which critically discusses specific privacy and security issues associated with it. In addition to identifying the threats, the research paper provides detailed and practical recommendations to improve the security of blockchain technology. The authors emphasize the importance of employing multiple layers of security, including cryptographic protocols, access control, and secure coding practices.

2.Literature review

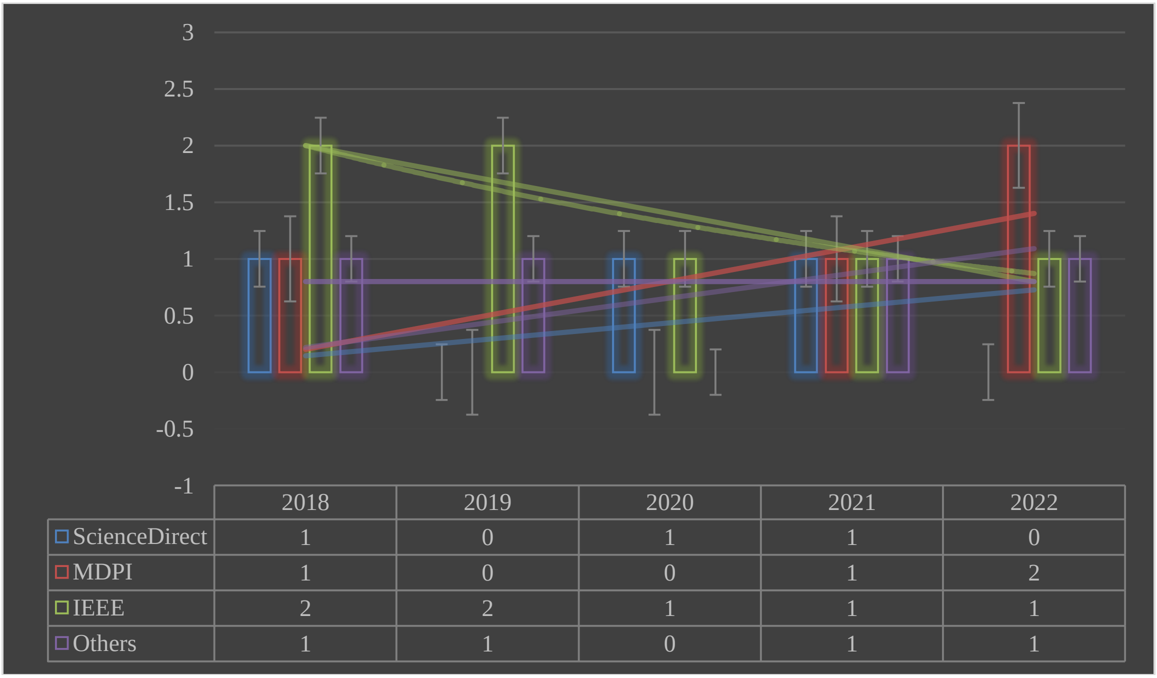
As per the view by Taylor et al. (2020) [1], blockchain and its usage are highly essential to financial security. To track financial misconduct, this technology helps to trace all these activities. It has been analysed that blockchain intends to manifest the smart grid planning to aim the cyber security effectively. As per the view of Demirkan et al. [8], a "Smart Contract for Digital Certificates" is a settlement for the manifestation of the blockchain in an effective way. The usability of blockchain is high [11]. It has been analysed that digital event and IT service management can be performed as a public ledger. Paper distribution is shown in *Figure 2.*

There is an example of a transition which is the bitcoin network transition. In recent times, blockchain has had a direct relationship with the crypto market. Peer-to-peer networks can be manifested through the help of blockchain technology in an effective way. This network is known as the P2P network. Blockchain register to store transactions has a deep relationship with each other [12].

The different paper has an indication that privacy and security can be highly managed through the help of BC technology and it has been shown that several applications fell victim to the cyberattack. The total equilibrium power of the computer assigned to bitcoin mining can be expressed as,

$n(t)m(t) = (1/n) \wedge (1+y/ 1-y) [y (n(t)) -1) (E(P(T)) \times \{R(t)/ c(t)+ (\rho + \eth) q(t)\}$

The above depicted equation implies that the bitcoin security, that is measured by the computer capacity, relies on the mining rewards, Mining costs, intensity of competition, cost efficiency of computer equipment and discounted rate. M(t) denotes the computer power (per miner) n(t) represents as a total number of minors. E(p(t)) signifies the expected price of the bitcoin and R(t) is the mining reward. Therefore, by using this equation developers can identify the bitcoin security and other security aspects with the use of blockchain technology.



	2018	2019	2020	2021	2022
□ScienceDirect	1	0	1	1	0
□MDPI	1	0	0	1	2
□IEEE	2	2	1	1	1
□Others	1	1	0	1	1

Figure 2 Distribution of selected papers

Most blockchain technology is not inspired by quantum technology, but rather is based on cryptographic principles that have been around for decades. Blockchain technology provides end-to-end traceability, which is one of its significant advantages [13]. This traceability is made possible using a distributed ledger, which records all transactions in a secure and transparent manner. The three essential properties of blockchain technology, known as the CIA triad, are confidentiality, data integrity, and availability. These properties ensure that data stored on the blockchain is secure and cannot be altered without proper authorization. The use of blockchain technology has undoubtedly made many aspects of life more manageable and efficient, including communication and asset registry. In addition to its use in asset registry and communication, blockchain technology has also been integrated with the IoT protocol. This integration has enabled secure and efficient data exchange between IoT devices, facilitating the creation of a decentralized and secure IoT ecosystem.

As per the view by Zhuang et al. (2020) [14], in large-scale quantum-inspired quantum walks (QIQW), blockchain has an extended role. A distributed ledger can be managed by blockchain technology, it has been evident. This technology has a major concern for trust management. As an example, in recent times, there is an incorporation of a major thing which is the 5G technology. In blockchain technology, there is a major thing which is the use of a single trusted party for the storage purpose effectively. It can be said that this technology is completely and mutually trusted by all parties.

In the financial industry, to do a payment, one payer can use one coin for the purpose of two or more payments, and it is a contribution of the blockchain model. This model opens a novel application and model which is known as social manufacturing and others. Layout-based contribution can be manifested through blockchain technology. As per the view of Gimenez-Aguilar et al. (2021) [15], blockchain technology can be maintained through the "Proof of Work (PoW) mechanism". It has been analysed that 80% of the research project is done on the bitcoin project.

Among the researcher, it is a topic to discuss and analyse. It can be said that Blockchain technology has an impact and innovation which is a side chain security [15]. Different findings have shown that the need and use of authentication have been enhanced by 67%. Blockchain helps to manifest technological positioning day by day [16]. There are examples of other technologies which are "Cite Space, Pajek, technology knowledge status (TKS) and technology knowledge reliability (TKR) and VOSViewer". Patterns of security and innovation can be improved through the help of blockchain. There is an example of a grid is the DC-micro grids (DC-MGs), and it has a major advantage which is the "intelligent control, monitoring and operation methods" [17]. Along with blockchain technology, there is another technology which is the Hilbert-Huang transform methodology. Robust detection needs to be incorporated in the recent era. This blockchain-based ledger technology is highly used in this smart plan [14].

As per the view of Demirkan et al. (2020) [8], blockchain technology helps to settle down different agents in the transaction princess thus smart load can be managed in terms of message delivery and other processes [18]. In today's smart city, automation is based on the internet of things, big data, machine-to-machine learning, artificial intelligence and others. Thus, cyberinfrastructure can be managed in an effective way. As per the view by Abdulkader et al. (2019) [19], all these technologies help to manifest the cyber-vigilance plan. Along with the cyber-vigilance plan, the activity of the citizen is highly connected [20]. It can be said that in recent times, people need to be concerned about their privacy rights [20].

As stated by Giannoutakis et al. (2020) [21], blockchain technology has a major advantage in the smart ecosystem. Blockchain framework has played the role of a defence framework. It is considered a technical methodology [22]. The "Cyber security vulnerability assessment tools, frameworks, and methodologies" has emphasised over the usage of blockchain technology. Discussion of other frameworks is enlisted in the different articles which are "cyber security vulnerability mitigation framework through empirical paradigm (CyFEr), blockchain cyber security framework (BC2F) and others" [23]. As per the view of Moradi et al. (2019) [24], "Blockchain, a sustainable solution for cyber security using crypto currency" in this context of the smart grid.

Table 1 Analysis based on selected papers regarding Blockchain security

S. No.	Source	Method	Results	Gap
1	Sun and Yu (2020) [25]	Formal verification of BNB contracts	Formal verification methods have been used by the researcher to identify the major security issues that arise due to the improper working condition of the blockchain networks. In this research, the researcher has proposed an effective verification model for blockchain smart contracts.	Provides verification for the maximum 200 million tokens
2	Khan *et al. (*2020) [26]	Deep learning, ANN, SVM, Decision Tree and MLP	The result section of this research exhibits that the DT model gives the best accuracy (90.12%) in analysing the performance of smart homes that is totally blockchain-based. Moreover, the researcher has proposed a new deep-learning-based model that provides 94.6% accuracy in evaluating the performance of blockchain-based homes.	Limited sample size
3	Farooq *et al.* (2022) [27]	RTS-DELM (*Real-Time Sequential Deep Extreme Learning Machine*), ANN-based IDS, Generative Adversarial Networks and initial neural networks	Based on the findings of this research paper, DELM gives a high accuracy (93.91%) in analysing the data of smart home networks. The proposed blockchain model provides 95.28% of accuracy which can help them easily monitor the smart home networks that are connected through blockchain technology.	Limited portion and size of the dataset.

4	Liu *et al.* (2020) [28]	ANN, Machine learning models and Blockchain security	The result section exhibits that a robotic system is required to be used to improve communication capabilities and the learning process. Both machine learning and blockchain technology are in use in HRI (Human-Robot Interaction) to improve the communication process and maintain security among devices.	Limited ranges of quality and rang
5	Li *et al.* (2021) [29]	Machine learning, Artificial Intelligence, Blockchain and Sensor Cluster	The result section found that Blockchain technology plays a vital role in making decisions by analysing the data of the healthcare sector. Even, the researcher has proposed a unique blockchain framework to continuously monitor the movement of medicines in the supply chain.	Safety of the pharmaceutical or healthcare supply chain
6	Shahbazi and Byun, (2021) [30]	Machine learning-based predictive analysis, Gradient Booster and KNN	The result section exhibits that the smart manufacturing industry can update, delete and insert records in the Blockchain network. Besides, customers can update details in the blockchain network by sharing an update request to the user interface of the blockchain technology. It is also found that Gdadient Booster provides better accuracy (95.56) in the case of predictive analysis.	Safety concern
7	Jamil *et al.* (2021) [31]	AI, IoT, ML algorithms and proposed blockchain framework	In this research, the researcher has proposed a fitness blockchain framework that is totally dependent on the intelligent system. The Hyperledger Composer has also been used by the researcher as an open-source toolkit to develop applications based on blockchain technology.	Low scalability and requires high computation power
8	Khan *et al.* (2021) [32]	Blockchain decentralised ML framework and Python implementation	The delivery drones such as UAVs, Amazon Prime Air and so on need to use machine learning algorithms and blockchain technology to perform ongoing operations easily and maintain security for devices. This is because UAV has the chance of experiencing cyberattacks, which may result in data losses and data theft.	Accuracy can be limited in the case of different machine learning methods.

3.Discussion and analysis

After analyzing and reviewing several research papers, several findings have been identified. The first finding is that the Decision Tree Classifier and Artificial Neural Network (ANN) are both useful in improving the accuracy of predictive analysis. Furthermore, machine learning and deep learning technologies have been shown to be effective in detecting security issues and threats related to blockchain technology. Both classification and regression models have also been found to be useful in identifying security flaws. To secure the current network system and different software applications such as Cloud and IoT applications, organizations and individuals must set up an efficient Intrusion Detection System (IDS) and utilize blockchain technology. In addition, to protect computer systems and mobile applications against cyberattacks, users should use strong passwords, encrypted code, blockchain technology, and up-to-date antivirus software.

The review presented in this paper covers different components related to blockchain technology, including the peer-to-peer process, internet of things, big data, and others. This study also highlights some limitations and identifies future research directions. The paper has used various keywords and terms related to the technology, blockchain technology, and assessment frameworks.

This paper also provides a taxonomy of blockchain threats and vulnerabilities, which includes alternative threats and risks such as cybersecurity attacks and vulnerabilities. It has been discussed that the advantages of cryptography, such as immutability, digital signature, and hashing, have been manifested effectively in blockchain technology. Additionally, the paper identifies five different layers in blockchain technology and reports a total of 60 cybersecurity incidents related to blockchain technology from 2009 to 2019.

The analysis of different research papers highlights several issues and limitations of blockchain technology. One of the major problems is the hacking of the cryptographic mechanism. Retailers of various business organizations face different types of financial-driven proliferation cyberattacks, ransomware, denial of service (DDOS), and other issues. However, in industries such as healthcare, banking, and pharmacy, blockchain can provide a trustless performance. Despite its potential benefits, some unjustified problems are found in the technology that needs to be addressed.

A limitation of different papers is the single point of failure risk, which is a major threat that can limit accessibility and capability. False data injection attacks (FDIAs) are another major attack that needs to be mitigated. It is essential to manage and implement security and privacy effectively as there is a fundamental difference between them.

In recent times, smart homes have become vulnerable to cyber-attacks, and traditional security methodology has some issues that need to be addressed. Another limitation of blockchain technology is its low computational ability, which needs to be improved. In conclusion, while blockchain technology offers numerous benefits, it is essential to address the issues and limitations mentioned above to ensure its successful implementation in different industries. *Figure 3* shows the methodology used in blockchain technology.

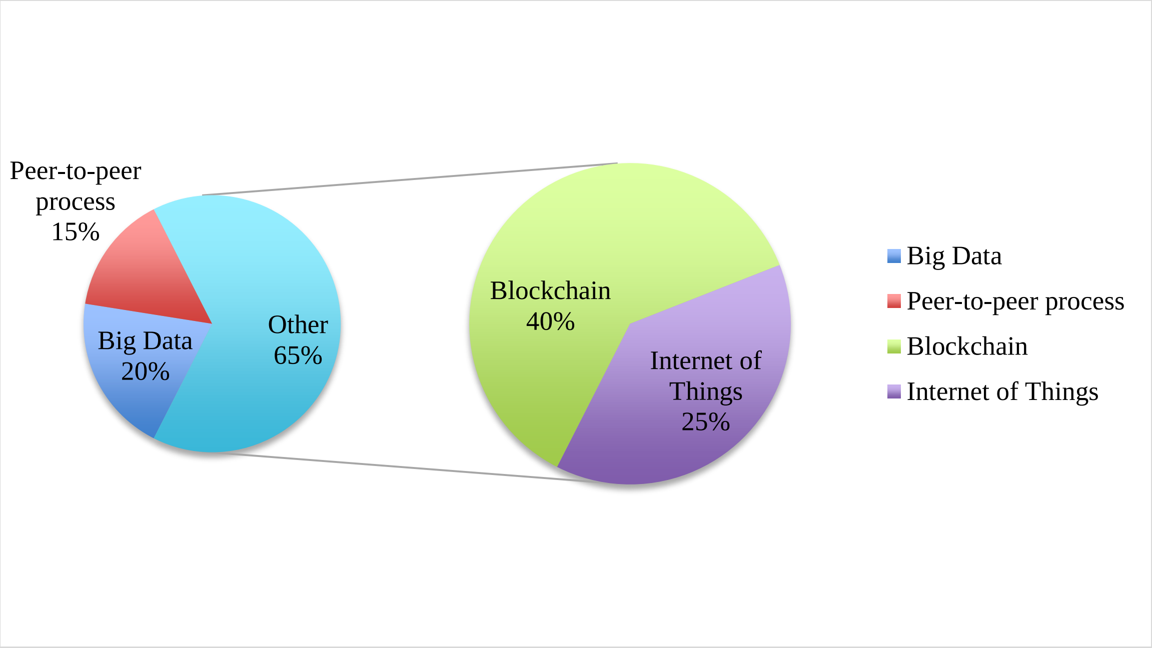


Figure 3 Methodology used in Blockchain security

4.Conclusion

Blockchain technology has emerged as a unique and disruptive technology, providing a secure way of managing trusted transactions in the existing network system. However, the increasing number of cyberattacks is a major concern for individuals and organizations, resulting in hindering the brand reputation and raising the cost of data breaches. Despite the rise of blockchain technology, data breaches are also increasing, indicating the poor security measures and policies adopted by organizations. This work aimed to analyze the concept of blockchain cybersecurity and highlight the ways of securing IoT and cloud-generated data through blockchain technology.

The study covered a broad range of factors that contribute significantly to the security of blockchain. It classified and discussed specific privacy and security issues associated with blockchain and provided detailed and practical recommendations to improve the security of blockchain technology. The importance of employing multiple layers of security, including cryptographic protocols, access control, and secure coding practices have been emphasized.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2020; 6(2):147-56.

[2] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys (CSUR). 2019; 52(3):1-34.

[3] Tanwar S, Bhatia Q, Patel P, Kumari A, Singh PK, Hong WC. Machine learning adoption in blockchain-based smart applications: the challenges, and a way forward. IEEE Access. 2019; 8:474-88.

[4] Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors. 2019; 19(2):1-17.

[5] Islam MN, Kundu S. Enabling ic traceability via blockchain pegged to embedded puf. ACM Transactions on Design Automation of Electronic Systems (TODAES). 2019; 24(3):1-23.

[6] https://economictimes.indiatimes.com/markets/cryptocurrency/what-are-51-attacks-in-cryptocurrencies/articleshow/85802504.cms. Accessed: 12th November 2022.

[7] https://www.cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-bridges.html. Accessed: 12th November 2022.

[8] Demirkan S, Demirkan I, McKee A. Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics. 2020; 7(2):189-208.

[9] Le Nguyen B, Lydia EL, Elhoseny M, Pustokhina I, Pustokhin DA, Selim MM, et al. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Computers, Materials & Continua. 2020; 65(1):87-107.

[10] Aldasoro I, Gambacorta L, Giudici P, Leach T. The drivers of cyber risk. Journal of Financial Stability. 2022.

[11] Serrano W. The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities. Journal of Network and Computer Applications. 2021.

[12] Maulani G, Gunawan G, Leli L, Nabila EA, Sari WY. Digital certificate authority with blockchain cybersecurity in education. International Journal of Cyber and IT Service Management (IJCITSM). 2021; 1(1):136-50.

[13] White J, Daniels C. Continuous cybersecurity management through blockchain technology. In technology & engineering management conference (TEMSCON) 2019 (pp. 1-5). IEEE.

[14] Zhuang P, Zamir T, Liang H. Blockchain for cybersecurity in smart grid: a comprehensive survey. IEEE Transactions on Industrial Informatics. 2020; 17(1):3-19.

[15] Gimenez-Aguilar M, De Fuentes JM, Gonzalez-Manzano L, Arroyo D. Achieving cybersecurity in blockchain-based systems: a survey. Future Generation Computer Systems. 2021; 124:91-118.

[16] Daim T, Lai KK, Yalcin H, Alsoubie F, Kumar V. Forecasting technological positioning through technology knowledge redundancy: patent citation analysis of IoT, cybersecurity, and blockchain. Technological Forecasting and Social Change. 2020.

[17] Ghiasi M, Dehghani M, Niknam T, Kavousi-Fard A, Siano P, Alhelou HH. Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. IEEE Access. 2021; 9:29429-40.

[18] Smith KJ, Dhillon G. Assessing blockchain potential for improving the cybersecurity of financial transactions. Managerial Finance. 2020; 46(6):833-48.

[19] Abdulkader O, Bamhdi AM, Thayananthan V, Elbouraey F, Al-Ghamdi B. A lightweight blockchain based cybersecurity for IoT environments. In international conference on cyber security and cloud computing (CSCloud)/ 5th international conference on edge computing and scalable cloud (EdgeCom) 2019 (pp. 139-44). IEEE.

[20] Mora OB, Rivera R, Larios VM, Beltrán-Ramírez JR, Maciel R, Ochoa A. A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures. In international smart cities conference (ISC2) 2018 (pp. 1-4). IEEE.

[21] Giannoutakis KM, Spathoulas G, Filelis-Papadopoulos CK, Collen A, Anagnostopoulos M, Votis K, et al. A blockchain solution for enhancing cybersecurity defence of IoT. In international conference on blockchain (Blockchain) 2020 (pp. 490-5). IEEE.

[22] Wang X, Xu C, Zhou Z, Yang S, Sun L. A survey of blockchain-based cybersecurity for vehicular networks. International Wireless Communications and Mobile Computing (IWCMC). 2020:740-5.

[23] Gourisetti NG, Mylrea M, Patangia H. Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework. In 9th annual computing and communication workshop and conference (CCWC) 2019 (pp. 206-13). IEEE.

[24] Moradi J, Shahinzadeh H, Nafisi H, Gharehpetian GB, Shaneh M. Blockchain, a sustainable solution for cybersecurity using cryptocurrency for financial transactions in Smart Grids. In 24th electrical power distribution conference (EPDC) 2019 (pp. 47-53). IEEE.

[25] Sun T, Yu W. A formal verification framework for security issues of blockchain smart contracts. Electronics. 2020; 9(2):1-23.

[26] Khan MA, Abbas S, Rehman A, Saeed Y, Zeb A, Uddin MI, et al. A machine learning approach for blockchain-based smart home networks security. IEEE Network. 2020; 35(3):223-9.

[27] Farooq MS, Khan S, Rehman A, Abbas S, Khan MA, Hwang SO. Blockchain-based smart home networks

security empowered with fused machine learning. Sensors. 2022; 22(12):1-13.

[28] Liu Y, Yu FR, Li X, Ji H, Leung VC. Blockchain and machine learning for communications and networking systems. IEEE Communications Surveys & Tutorials. 2020; 22(2):1392-431.

[29] Li Y, Shan B, Li B, Liu X, Pu Y. Literature review on the applications of machine learning and blockchain technology in smart healthcare industry: a bibliometric analysis. Journal of Healthcare Engineering. 2021; 2021:1-11.

[30] Shahbazi Z, Byun YC. Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. Sensors. 2021; 21(4):1-21.

[31] Jamil F, Kahng HK, Kim S, Kim DH. Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms. Sensors. 2021; 21(5):1-31.

[32] Khan AA, Khan MM, Khan KM, Arshad J, Ahmad F. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. Computer Networks. 2021.

Animesh Kumar Dubey is working as Assistant professor with the department of Computer Science and Engineering, at Madhyanchal Professional University, Bhopal, India. He has completed his Bachelor of Engineering (B.E.) and MTech. degree with Computer Science Engineering from Rajeev Gandhi Technical University, Bhopal (M.P.). He has more than 15 publications in reputed, peer-reviewed national and international journals and conferences. His research areas are Data Mining, Optimization, Machine Learning, Cloud Computing and Artificial Intelligence.
Email:animeshdubey123@gmail.com