JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain as a Paradigm Shift in Cybersecurity Defence Mechanisms

Neha Anand[1], Arpita Vishwakarma[2], Dr. Yusuf Perwej[3], Vaibhav Gupta[4], Sameeksha Gupta[5]

[1]Assistant Professor, Department of Computer Science & Engineering, Shri Ramswaroop Memorial University, Deva Road, Lucknow
[2]Assistant Professor, Department of Computer Science & Engineering, Shri Ramswaroop Memorial University, Deva Road, Lucknow
[3]Professor, Department of Computer Science & Engineering, Shri Ramswaroop Memorial University, Deva Road, Lucknow
[4]Scholar (B.Tech) Department of Computer Science & Engineering, Shri Ramswaroop Memorial University, Deva Road, Lucknow
[5]Scholar (B.Tech) Department of Computer Science & Engineering, Shri Ramswaroop Memorial University, Deva Road, Lucknow

Abstract: As the digital realm expands, cybersecurity has become essential for secure communication, data integrity, and organizational resilience. A decentralized public ledger known as a blockchain facilitates secure transactions across untrusted network nodes. Its essential role in bitcoin systems, where it ensures secure and decentralized transaction records, has garnered significant attention. Over the last decade, Blockchain has garnered significant attention from several businesses because to its potential to revolutionize multiple sectors, including cybersecurity. Nonetheless, this field of inquiry is nascent, and several concerns about blockchain's effectiveness in cybersecurity need more examination. This study used a qualitative research approach to assess the contemporary applications of blockchain-based security and their appropriateness within the current cybersecurity landscape. This research also examined the mechanisms via which blockchain upholds the security triangle. Results indicate that blockchain has significant potential for addressing contemporary issues. Blockchain has the potential to transform defensive mechanisms against the ever-changing threat landscape in the digital age by enhancing trust, transparency, and resilience in digital settings.

Keywords: Blockchain, Cryptocurrency, Confidentiality, Privacy, Cybersecurity, Data Integrity, Decentralization

1. Introduction

The contemporary realm of digital security presents a captivating story via the integration of blockchain technology with cybersecurity. Blockchain, originally designed as the foundational technology for cryptocurrencies, has rapidly evolved into a disruptive force with extensive consequences across all sectors. Its decentralized architecture, cryptographic security, and transparent ledger. The mechanism presents a fundamental change in cybersecurity procedures. Blockchain offers a tamper-resistant framework for documenting transactions and ensuring data integrity, so promising to alleviate the risks associated with centralized systems. This revolutionary power has generated significant attention among academics, policymakers, and business stakeholders, who see blockchain as a formidable partner in the continuing battle against cyber dangers. Computer systems and the internet have transformed data storage and sharing, making data security a critical issue for all enterprises [5]. Cyber-attacks have become more intricate and advanced, complicating efforts to mitigate their effects. Diverse strategies have been used to mitigate the frequency and effects of these assaults; nonetheless, cybercriminals often devise novel methods to circumvent established security measures. To maintain a competitive edge, ongoing research and innovation are essential for enhancing current security systems [6]. Blockchain technology, often linked to cryptocurrencies, has lately surged in popularity. It is now extensively used outside cryptocurrencies, serving as the basis for other applications. A blockchain is a cryptographic decentralized public record that enables safe transactions between untrusted network nodes. Traditional security solutions use a centralized methodology, but Blockchain utilizes a decentralized and distributed framework that may effectively address several contemporary cybersecurity challenges [9]. The use of advanced technology in cybersecurity is crucial for enhancing security measures. Blockchain technology has garnered considerable attention owing to its potential for enhanced security and scalability. This study will examine the prospective advantages of Blockchain in Cybersecurity and analyse the critical elements that may affect its adoption. This will examine the impact of Blockchain technology on the field of cybersecurity. This study will examine the impact of blockchain on cybersecurity and categorize how blockchain attributes enhance the CIA triad. This study will examine the variables affecting the extensive adoption of blockchain in cybersecurity, along with the possible advantages and cons of using blockchain for this purpose. This study will examine the

present condition of blockchain in cybersecurity [12] and will provide suggestions for future research and development in this domain.

2. Background

The advancement of cybersecurity technology has led to the heightened use of sophisticated technologies, like blockchain and other intelligence frameworks, to enhance the security, integrity, and dependability of data across many domains. In 2016, Yli-Huumo et al. performed a systematic literature review to ascertain the published research findings pertaining to the overarching notion of blockchain technology [13]. They omitted legal, economic, and regulatory studies from their evaluation, concentrating instead on articles pertaining to blockchain technology. It was discovered that 80% of the research articles concentrate on Bitcoin initiatives, particularly emphasizing security and privacy themes. Since 2016, the uses of blockchain have expanded; thus, our study aims to examine existing studies primarily related to cybersecurity and blockchain applications.
In late 2016, Conoscenti et al. performed a systematic literature review on the use and adaptation of blockchain, particularly concerns IoT and other peer-to-peer devices [14]. They emphasized that blockchain technology might facilitate the discovery of data misuse without requiring a centralized reporting system. Nevertheless, they did not examine the overarching effects of blockchain on cybersecurity as a whole. Seebacher et al. [15] conducted a systematic literature review in 2017 that emphasized the growing influence of blockchain on service systems [16]. They suggested that further study should include an examination of practical applications [17], which underpins our investigation into the impact of blockchain on cybersecurity issues [18].

Eghmazi et al. (2024) examine the use of blockchain technology to enhance the security of IoT data, a pertinent strategy for healthcare as vital patient information is managed via IoT devices [19]. The integration of blockchain with AI technologies, as articulated by Elisha et al. (2024), presents new avenues for automation and anomaly detection. Although mostly used in precision agriculture, these technologies may also be employed to automate threat detection in healthcare, enabling AI models to forecast and mitigate cyber risks prior to data breaches. [22] The use of machine learning in 5G networks has shown that these approaches are very successful in forecasting and detecting cyber threats across many digital platforms. Fakhouri et al. (2023) provide a comprehensive examination of the role of machine learning in 5G security, including strategies that enhance data safety and assure communication security in 5G-enabled healthcare networks [23]. In widely used cloud computing settings by healthcare organizations, there was a need for safe data-sharing protocols that necessitated two-factor authentication (2FA) and cryptographic solutions. Gadde et al. (2023) assert that blockchain-based systems may considerably augment the security of health information access via two-factor authentication, hence mitigating hazards linked to unlawful access [26]. Blockchain technology may be used to safeguard intellectual property rights in medical research and technology. Huan-Wei et al. (2023) observe that blockchain enhances intellectual property transactions to guarantee secure data transmission and safeguard medical innovations from cyber threats. This is crucial for health organizations who need the protection of their intellectual property.

3. Problem Statement and Aim

The fact that cybersecurity represents a predominant issue in contemporary society, it is essential to safeguard our information via the use of blockchain technology. Although Blockchain is seen as a potentially transformative solution for several cybersecurity difficulties, this technology presents distinct obstacles that need more comprehensive examination. The integration of blockchain technology into cybersecurity is an emerging and intricate subject, with insufficient training and research dedicated to using blockchain for enhancing cybersecurity [28]. The aims of this research are: (1) To examine the utilization of blockchains in enhancing cybersecurity (2) To comprehend the mechanisms used by blockchain to maintain the CIA triad. To ascertain the determinants that affect the extensive use of blockchain in cybersecurity. To ascertain the management of risks related to blockchain-based cybersecurity solutions.

4. Blockchain Models

Blockchains denote decentralized digital ledgers consisting of cryptographically authenticated transactions organized into blocks. Each block is linked with the preceding one via a cryptographic mechanism, guaranteeing that any alterations are easily identifiable. Each block on a blockchain references its predecessor, known as the Genesis block [29]. The genesis block is the first block in a blockchain network, manually generated and hard-coded into the network's software, serving as the foundation for the whole blockchain, since all subsequent blocks are interconnected by cryptographic hashing. Figure 1 is an example of the block structure. The validation of [31] transactions and the consensus mechanism are essential procedures for appending blocks to the chain, hence increasing the difficulty of modifying prior blocks. The ledger is duplicated across many nodes in the network, and any inconsistencies are rectified according to established protocols [32].

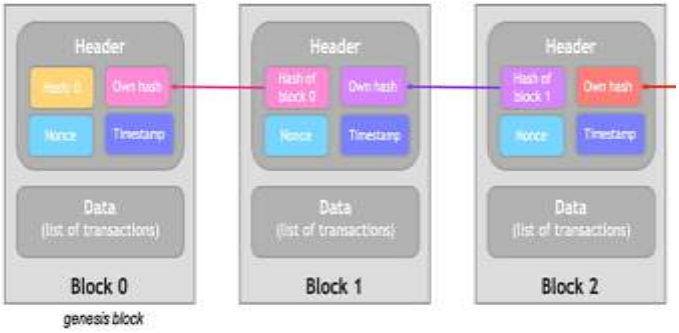

Figure 1. The Blockchain Models

Decentralization is a fundamental characteristic of blockchain technology, entailing the distribution of power and decision-making among several participants rather than reliance on a central authority. A decentralized blockchain network consists of several nodes, each preserving a copy of the blockchain ledger. These nodes interconnect via a peer-to-peer network, enabling information exchange and communication among them, thereby precluding any potential for a single point of failure or control. This characteristic of blockchain guarantees that all transactions documented in a block are unalterable and

irretrievable. This feature is essential for the security and dependability of the blockchain as it inhibits any unauthorized modification of the recorded data. The blockchain's immutability guarantees that its data is resistant to tampering and reliable. Blockchain immutability [33] is achieved by cryptographic hash algorithms, which confer a unique and irreversible digital fingerprint to each block. Blockchain transparency denotes the unrestricted accessibility of information recorded on the blockchain ledger. It enables all network members [34] to see the transaction history, addresses, and balances, hence fostering accountability and enhancing confidence within the network. This characteristic makes the blockchain a dependable platform for the storage of sensitive data without middlemen, hence reducing the danger of fraud or manipulation. Blockchain transactions provide a high degree of verifiability, since each transaction is authenticated and documented with a timestamp.

5. Blockchain Data Security

Data is quickly becoming one of the world's most precious resources due to its ever-increasing value. The top ten corporations by market capitalization are dominated by data-centric firms like Amazon, Facebook, Alphabet, Microsoft, and Apple. As a result, most individuals aren't fully protected, and 34 hackers target critical information. Large companies like Home Depot, Anthem, and Target have suffered massive data breaches in the last several years, affecting countless people. Our data is no longer under our control, according to Tim Berners-Lee, the man responsible for creating the World Wide Web. Our safety cannot be guaranteed by the current methods.

The dependability of conventional PKI may be enhanced by decentralizing PKI (Public Key Infrastructure). Without any privacy features, this system functions as a public ledger that associates public keys with identities. Similarly, Certcoin was built using a fully functional architecture that enables all critical PKI [35] capabilities, such as key registration, update, and registration. Due to their vulnerability to impersonation of previously registered identities, conventional PKIs are unable to guarantee identity preservation. In contrast, Certcoin aims to provide identity preservation assurances that are more dependable than those provided by conventional CA or WoT PKIs. The ability to stop users from enrolling a public key under another user's registered identity is what "identity retention" means in this context. Using an encryption protocol for both data storage and searches makes it possible to verify and monitor nodes in a dispersed network with ease. Every node that joins the system is subject to ongoing supervision and verification using verifiable search queries. Several nodes must agree using a common voting mechanism to decide the result of each verification. The findings will be published on the blockchain as a 36-trustworthy opinion that the nodes have unanimously agreed with. With these protocols set up, the majority of nodes will be able to autonomously identify and eliminate any node that acts maliciously. Expanding Its Cybersecurity, Applications A safe supply chain As a result of blockchain's rising profile, many businesses, both large and small, are looking into the technology's applications outside of the financial industry. In order to meet a wide range of needs, these firms are now doing blockchain application testing. For instance, one business that's working to improve supply chain transparency—Provenance—is using blockchain technology to build trust in the supply chain by making it easier to see where a product comes from and how it gets to the customer. Blockchain technology may also improve the accuracy and transparency of supply chain management's end-to-end tracking. The digitization of physical assets and the establishment of a decentralized,

In order to keep the CIA trifecta in place, how does blockchain technology work? Ensuring the confidentiality, integrity, and availability of vital information assets is the goal of information security. These assets may be strategic, protected, sensitive, or proprietary. The "CIA Triad" describes this group. Hardware, software, data, information, and other resources shown in figure 2 that store information may all be considered information assets [36]. Accountability (also called non-repudiation), availability, confidentiality, and integrity are the four pillars upon which this paradigm of information security rests, according to some experts. Data integrity refers to keeping data valid and unaltered while data privacy refers to protecting data from unwanted access. When information and systems are made available to authorized persons and processes in the proper form, we say that they are available.

Blockchain Maturity Level

	Initial (stage 1)	Repeatable (stage 2)	Defined (stage 3)	Managed (stage 4)	Optimizing (stage 5)
Networks		Network load	Reliability		
Information Systems	Architecture Upgrading Integration	Maintenance Storage Scalability		Business efficiency	
Computing Methodologies	Standardization	Computational complexity			
Security and Privacy			Privacy	Data security Transaction security	

Figure 2. The Blockchain Maturity Level

6. The Function of the Internet of Things (IoT) and Cloud Computing

The Integration of Blockchain in IoT Security The Internet of Things (IoT) has seen significant expansion in recent years, linking billions of gadgets to the Internet and altering our lifestyles and work practices. The phrase "Internet of Things" (IoT) denotes a network of physical devices linked to the Internet that may exchange data, including household appliances, cars, and other things. These devices possess sensors, processors, and communication technologies that provide the collection, analysis, and transmission of data over the Internet autonomously. Vailshery (2017) projects that the worldwide count of Internet of Things (IoT) linked devices would rise markedly from around 13.8 billion units in 2021 to 30.9 billion units by 2025. As the proliferation of Internet of Things (IoT) devices continues, as seen in figure 3, so too does the apprehension over the security of these devices.

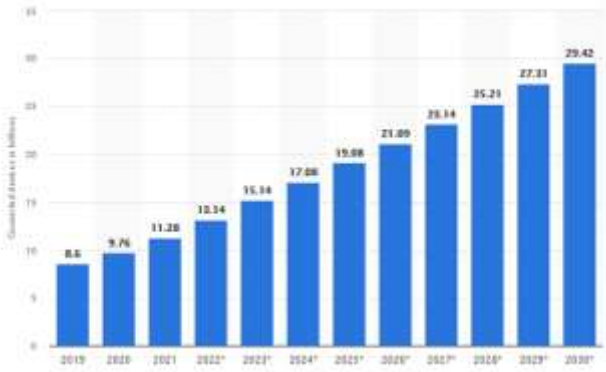

Figure 3. The Number of Internet of Things (IoT) Connected Devices Globally Will Increase Significantly

Armed Forces and National Security Military and defence innovation has yielded substantial technological advancements over the past century, with the U.S. military pioneering the development of the Internet for global information dissemination and the creation of GPS for enhanced military positioning (Daley, 2022). DARPA (Defence Advanced Research Projects Agency), Arlington, Virginia DARPA is doing research on blockchain technology to improve the security of military communications, including what the Department of Defence designates as a "Unbreakable code." The agency is initiating an experiment to use blockchain technologies for the creation of a decentralized ledger. This technology will allow military personnel globally to send secure communications or execute transactions with complete traceability across various channels. Utilizing blockchain for the management of health records Health Linkages (Mountain View, California) employs blockchain technology to guarantee transparent data governance, enhance auditable analytics, and strengthen healthcare compliance. The firm utilizes its blockchain to ensure that only authorized personnel may access and trade medical data. It also preserves a chronological record of all healthcare events for each patient, therefore allowing clinicians to make better educated healthcare choices.

7. The Function of Blockchain Technology in Cyber Defence

Blockchain technology has considerable potential for improving cybersecurity measures by tackling critical issues such as data integrity, identity management, and secure communication. A fundamental contribution of blockchain to cybersecurity is its capacity to create a tamper-proof and transparent transaction record, therefore reducing the risk of data alteration and illegal access. In identity management, blockchain technologies provide decentralized and verified identity identification methods, obviating the need for centralized authority and diminishing the risk of identity theft and fraud. Blockchain systems use cryptographic methods, like digital signatures and public-private key pairs, to allow users to claim ownership of their digital identities while maintaining privacy and security. Moreover, blockchain [38] may enable safe communication and information exchange among stakeholders in cyberspace by creating encrypted and immutable channels for transmitting sensitive data and authenticating digital assets. Smart contracts, which are self-executing agreements stored on the blockchain, may automate trust-based [39] transactions and enforce predetermined norms without intermediaries, therefore optimizing operations and mitigating the danger of human mistake or hostile interference. The incorporation of blockchain technology into cyber defence [40] strategies has the potential to strengthen the resilience of digital infrastructure against emerging threats and vulnerabilities, thereby enhancing the trust, integrity, and security of online transactions and communications.

8. Conclusion

The study collectively evaluated if blockchain-based security models surpass current cybersecurity measures. As threats to cyberspace escalate in scale and complexity, the need for more resilient, transparent, and safe security technology becomes more imperative. Blockchain technology presents a viable alternative to conventional cybersecurity frameworks because to its decentralized architecture, cryptographic assurance of integrity, and immutable record-keeping. Blockchain mitigates significant vulnerabilities inherent in centralized systems via secure identity management, tamper-proof data storage, and decentralized access control. This article has examined the many uses of blockchain in cybersecurity and its potential to revolutionize data protection and the building of trust online. Although several case studies and novel applications provide encouraging outcomes, significant hurdles must be addressed, including those related to scalability, regulatory compliance, energy consumption, and integration with current systems. The report underscores the need of using revolutionary technologies, such as blockchain, to establish solid cybersecurity strategies in the future. It clearly indicates that blockchain transcends a mere trend, representing a legitimate and strategic improvement to cybersecurity frameworks.

References

[1] T. Aste, P. Tasca, T. Di Matteo, Blockchain technologies: the foreseeable impact on society and industry, Computer 50 (9) (2017) 18–28.
[2] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), 2017, p. 557564.
[3] Y. Perwej, Firoj Parwej, Mumdouh Mirghani Mohamed Hassan, Nikhat Akhtar, “The Internetof- Things (IoT) Security: A Technological Perspective and Review” , International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5, Issue 1, Pages 462-482, February 2019., DOI: 10.32628/CSEIT195193
[4] Y. Perwej, Syed Qamar Abbas, Jai Pratap Dixit, N. Akhtar, Anurag Kumar Jaiswal, “A Systematic Literature Review on the Cyber Security”, International Journal of Scientific Research and Management (IJSRM), Volume 9, Issue 12, Pages 669 - 710, 2021, DOI: 10.18535/ijsrm/v9i12.ec04
[5] E. Androulaki, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, 2018, pp. 30:130:15.
[6] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, H. Kai, A multiple blockchains architecture on inter-blockchain communication, in: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018, p. 139145.
[7] N. Akhtar, Bedine Kerim, Yusuf Perwej, Anurag Tiwari, Sheeba Praveen, “A Comprehensive Overview of Privacy and Data Security for Cloud Storage”, International Journal of

Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 08, Issue 5, Pages 113-152, 2021, DOI: 10.32628/IJSRSET21852

[8] Y. Perwej, Nikhat Akhtar, Firoj Parwej, "A Technological Perspective of Blockchain Security", International Journal of Recent Scientific Research (IJRSR), ISSN: 0976-3031, Volume 9, Issue 11, (A), Pages 29472 – 29493, November 2018., DOI: 10.24327/ijrsr.2018.0911.2869

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on Blockchain technology? - a systematic review, PLoS One 11 (10) (2016) 127.

[10] M. Conoscenti, A. Vetr, J.C. De Martin, Blockchain for the internet of things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, p. 16.

[11] Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications", for published in the Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, Pages 30 - 43, October, 2018

[12] Y. Perwej, Kashiful Haq, Uruj Jaleel, Firoj Perwej, **"**Block Ciphering in KSA, A Major Breakthrough in Cryptography Analysis in Wireless Networks**"**, International Transactions in Mathematical Sciences and Computer, India, ISSN-0974-5068, Volume 2, No. 2, Pages 369-385, July-December 2009

[13] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, where is current research on Blockchain technology? - a systematic review, PLoS One 11 (10) (2016) 127.

[14] M. Conoscenti, A. Vetr, J.C. De Martin, Blockchain for the internet of things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, p. 16.

[15] S. Seebacher, R. Schritz, Blockchain technology as an enabler of service systems: a structured literature review, in: Exploring Services Science, 2017, p. 1223.

[16] Y. Perwej, N. Akhtar, Devendra Agarwal, "The emerging technologies of Artificial Intelligence of Things (AIoT) current scenario, challenges, and opportunities", Book Title"Convergence of Artificial Intelligence and Internet of Things for Industrial Automation", SCOPUS, ISBN: 978-1-032-42844-4, CRC Press, Taylor & Francis Group, 2024, Link:https://www.taylorfrancis.com/chapters/edit/10.1201/9781003509240-1/emerging-technologiesartificial- intelligence-things-aiot-current-scenario-challenges-opportunities-yusuf-perwej-nikhatakhtar-devendra-agarwal?context=ubx&refId=537f1a8f-6a94-4439-b337-3ad3d1ce8845, DOI: 10.1201/9781003509240-1

[17]Shobhit Kumar Ravi, Shivam Chaturvedi, Neeta Rastogi, Nikhat Akhtar, Yusuf Perwej, "A Framework for Voting Behavior Prediction Using Spatial Data", International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN: 2347-5552, Volume 10, Issue 2, Pages 19-28, March 2022, DOI: 10.55524/ijircst.2022.10.2.4

[18] Firoj Parwej, Nikhat Akhtar, Y. Perwej, "An Empirical Analysis of Web of Things (WoT)", International Journal of Advanced Research in Computer Science (IJARCS), ISSN: 0976-5697, Volume 10, No. 3, Pages 32-40, May 2019, DOI: 10.26483/ijarcs.v10i3.6434

[19] Eghmazi, A., ataei, m., landry, r.,jr and chevrette, G. (2024). Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy. IoT, 5(1);20.

[20] Asif Perwej, Dr. Kashiful Haq, Y. Perwej, "Blockchain and its Influence on Market", for published in the International Journal of Computer Science Trends and Technology (IJCST), ISSN 2347 – 8578, Volume 7, Issue 5, Pages 82- 91, Sep – Oct 2019, DOI: 10.33144/23478578/IJCST-V7I5P10

[21] Y, Perwej ," The Hadoop Security in Big Data: A Technological Viewpoint and Analysis ", International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE) , E-ISSN: 2320-7639, Volume 7, Issue 3, Pages 1-14, June 2019, DOI: 10.26438/ijsrcse/v7i3.1014

[22] ElishaElikem, K.S., anggraini, l., kumi, j.a., luna, b.k., akansah, e., hafeez, a.s., mendonça, i. and aritsugi, M. (2024). IoT Solutions with Artificial Intelligence Technologies for Precision Agriculture: Definitions, Applications, Challenges, and Opportunities. Electronics,13(10);1894.

[23] Fakhouri, H.N., alawadi, s., awaysheh, f.m., imad, b.h., alkhalaileh, m. and hamad, f. (2023). A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions. Electronics,12(22);4604.

[24] Hina Rabbani, Sana Rabbani, Dr. Yusuf Perwej, Farheen Siddiqui, Dr. Nikhat Akhtar**,** "Cloud-Centric Architectures for Social Media: A Review of Challenges and Evolutionary Trends", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 11, Issue 3, Pages 1055-1071, June 2025, DOI: 10.32628/CSEIT25113389

[25] Y. Perwej, "6G -Secure Data cluster Approach with Blockchain Technology", IEEE 3rd International Conference on Intelligent Engineering and Management (ICIEM), SCOPUS, IEEE Conference Record No: 54221, Electronic ISBN:978-1-6654-6756-8, Amity University 24 Bedford Square Fitzrovia, London WC 1B 3HN, UK, 27th - 29th April 2022, Link - https://ieeexplore.ieee.org/document/9853111, DOI: 10.1109/ICIEM54221.2022.9853111

[26] Gadde, S., rao, g.s., venkata, s.v., yarlagadda, m. and lakshmi patibandla, R.S.M. (2023). Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions. Ingenierie des Systemes d'Information,28(6);1467-1477

[27] Huan-Wei, L., Yuan-chia, c. and han, T. (2023). Fortifying Health Care Intellectual Property Transactions With Blockchain. Journal of Medical Internet Research, 25(1);e44578

[28] Mansi Bajpai, Atebar Haider, Dr. Alok Mishra, Dr. Yusuf Perwej, Dr. Neeta Rastogi, "A Novel Vote Counting System Based on Secure Blockchain" , International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN: 2395-1990 , Online ISSN : 2394-4099, Volume 9, Issue 4, Pages 69-79, July-August-2022**,** DOI: 10.32628/IJSRSET22948

[29] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence, in: IEEE Trans. Emerg. Top. Comput., 2017, p. 11.

[30] A. Kumar, Yusuf Perwej, Ashutosh C Kakde, "Transforming Education Through IoT and AI Opportunities and Challenges", Educational Administration: Theory and Practice, SCOPUS, Volume 30, No. 5, Pages 11610 –11622, 31 May 2024, DOI: 10.53555/kuey.v30i5.4982

[31] Y. Perwej, "Performance Analysis for Cloud Based OLAP over Big Data", IEEE International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES -2022), SCOPUS, IEEE Conference, St. Joseph's Institute of Technology, IEEE Electronic ISBN:978-1-6654-7413-9, Chennai, India**,** 15th &16th July 2022, DOI: 10.1109/ICSES55317.2022.9914266

[32] O. Osanaiye, H. Cai, K.-K.R. Choo, A. Dehghantanha, Z. Xu, M. Dlodlo, Ensemblebased multi-filter feature selection

method for DDoS detection in cloud computing, EURASIP J. Wirel. Commun. Netw. (1) (2016) 2016.
[33] S. Seebacher, R. Schritz, Blockchain technology as an enabler of service systems: a structured literature review, in: Exploring Services Science, 2017, p. 1223.
[34] Y. Perwej, N. Akhtar, Neha kulshrestha, Pavan Mishra, "A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends", Journal of Emerging Technologies and Innovative Research (JETIR), Volume 09, Issue 1, Pages 346 - 371, 2022, DOI: 10.6084/m9.figshare.JETIR2201346
[35] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: securing a blockchain applied to smart contracts, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), 2016, p. 467468.
[36] R.M. Parizi, A. Dehghantanha, On the understanding of gamification in blockchain systems, in: 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, 2018, pp. 214–219
[37] Nagarjuna Tandra, Nikhat Akhtar, K Padmanaban, L. Guganathan, "A finite-element dual-level contextual informed neural network with swarm space hopping algorithm based optimal feature selection and detection for EEG-based epileptic seizure detection", Swarm and Evolutionary Computation, Elsevier , SCIE, Volume 97, Pages 1- 19, August 2025, DOI: 10.1016/j.swevo.2025.102072
[38] Swan, Melanie. "Blockchain: Blueprint for a New Economy." Sebastopol, CA: O'Reilly Media, 2015
[39] Farheen Siddiqui, Sana Rabbani, Dr. Yusuf Perwej, Hina Rabbani, Dr. Nikhat Akhtar, "Leveraging Cloud Computing, IoT and Big Data for Intelligent Infrastructure Management in Smart Cities", Journal of Emerging Technologies and Innovative Research (JETIR), ISSN-2349-5162, Volume 12, Issue 8, Pages 301 - 310, August 2025, DOI: 10.6084/m9.jetir.JETIR2508335
[40] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." IEEE International Congress on Big Data (BigData Congress), 2017