A Taxonomical Review on Blockchain Technology in Cybersecurity

[*]Srinivasa Rao Gundu[1], Dhanunjaya Rao Reddy[2,] Manjunath. P[3]

[1]Associate Professor, Department of Computer Science, School of Sciences, Malla Reddy University, Hyderabad, India.
[2,3] Assistant Professor, Department of Digital Forensics, School of Sciences, Malla Reddy University, Hyderabad, India.
drg_srinivasarao@mallareddyuniversity.ac.in[*1]
dhanunjayarao.reddy@mallareddyuniversity.ac.in, manjunathp@mallareddyuniversity.ac.in

Abstract

Today, as of 2025, the focus of the Internet is on digital Assets Predicated on Blockchain Technology (BCT). The BCT is a cryptocurrency technology combining cryptographic technology and decentralised information technology (P2P) as part of its basic operation. By providing an extensive systematic literature review of BCT, this paper includes Applications of Blockchain Technology to Cybersecurity. Five Basic Categories are described for Securing Network Services; Protection of Data Integrity; Security in the Internet of Things (IoT); the Identification of Individuals with Private Identity Credentials; and the Intelligence to Discover Cyber Threats. There are also Suggested Types of BCT; Frameworks for Cybersecurity using Blockchain Technology; Current Trends and Challenges Multiple Uses of Blockchain Technology with Artificial Intelligence (AI) and Quantum Cryptography (QC).

Key words: Block Chain, Cryptography, Cyber security, Data Integrity, IOT systems, Cyber threats, Security framework, Artificial Intelligence, Quantum cryptography.

I. Introduction:

The history of cyber threat development, its increase in complexity and the scale of damage it can cause to big businesses has demonstrated us numerous underlying flaws of the traditional centralized cybersecurity paradigm (e.g., DDOS attacks). Such systems normally use one or two trusted end points that can be easily attacked by a hacker. With the increase in size and the complexity of the digital infrastructure, the capacity of ensuring the security of data (integrity, confidentiality, and availability) has never been harder than now [1]. This assertion poses a query on whether or not there is a stronger alternative to the existing centralized system of cyber security. When a mysterious person (Satoshi Nakamoto) released bitcoin in 2008, it introduced a new technology known as blockchain, which is essentially decentralized, i.e., every user is in charge of his/her transactions or records. Such a record keeping has been termed as tamper resistant and transparent (i.e. seeable by all users on the network) since any addition to the ledger has to be approved by the majority of the other users before it will become a part of the official record. It is therefore nearly impossible to change a transaction unless the majority feels that the transaction should be changed. The chronological nature of recording changes made to the blockchain forms a permanent log of all changes made. The blockchain technology enhances the guarantees of security, minimizes chances of a single point failures, and established a high level of traceability and accountability in the entire digital supply chain sector in all sectors of the economy [2].

2. Motivation

Even though centralized systems might be effective in most circumstances, they are prone to all forms of attacks including a single point of failure, the issue of insider threats and

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_39

manipulation of the information that resides in the system since they are managed by a single central authority. A successful attack on or internal intrusion into the central node will cause the inability of the entire system to work and open the possibility of manipulation of the data and distrust, the user base. Moreover, as digital networks continue to expand, the idea of controlling and ensuring the safety of the vast amounts of data in a centralized model becomes more complex and is resource-heavy. Contrastingly, the blockchain has removed or significantly reduced a significant number of these weaknesses of centralized systems. The characteristics of the blockchain technology immutability, decentralization, and cryptographic consensus can be used to minimize the risks of these conventional models. Immutability implies that once the data is included in the blockchain, it cannot be erased or changed without the agreement by the network participants. Thus, the integrity of the data is ensured by the impossibility of their changes in the blockchain. Such a decentralization enables numerous nodes to stay in control and authenticate information, thereby lessening the possibility of failure of one spot, and consequently making the system less vulnerable to internal and external interference. Lastly, using cryptographic consensus such as Proof of Work or Proof of Stake, a minimum level of trust and dependability is formed by making sure that everyone agrees on the legitimacy of the transactions without having to rely on one central authority. Combined with these attributes, blockchain makes an intriguing building block of trustless security, with trust and auditability residing within the protocol and not a firm.

3. Objective and scope

This review provides:

- An ontology of blockchain based cybersecurity applications.
- Discussion of architectural designs and agreement systems.
- Geoffification of new integration paradigms with AI, IoT and Zero trust.
- Determination of gaps and difficulties in research.

4. History of blockchain technology

Block chain is a series of blocks, each block has a number of transactions, time stamps and hashes that connect it to the preceding block. The time sequence of the ledger is preserved by this cryptograph chain, as any change to a single block would invalidate all the subsequent blocks (because the hash will be different). Since the block chain network is decentralized, every single party possesses a copy of the ledger and offers transparency, fault tolerability, resistance to tampering or alteration. Its main layers include [6]:

- **Data layer**: is the basis of the blockchain, the responsibility of which is to store blocks, transactions, and metadata. The blocks contain transaction data, a timestamp and cryptographic hashes connecting them to the last block thereby forming an immutable Data layer: verifiable chain of records. This layer maintains the integrity, transparency and persistence of all the information recorded allowing the participants to trace the previous transactions safely and effectively.
- **Network layer:** Network layer deals with peer-to-peer communication between the blockchain ecosystem nodes. It regulates propagation, validation and synchronization of new transactions and blocks in the distributed network network. This layer maintains a consistent and up-to-date copy of the ledger of every node without an external authority, therefore, facilitating the sharing and coordination of data securely, using decentralized communication protocols. finite state 5.
- **Consensus layer:** Consensus layer ensures that distributed nodes agree on which transactions are valid and in which order they are represented in the blockchain. It constructs one version of the ledger, based on consensus algorithms such as proof of work and proof of stake, that organize the work of the nodes in order to complete and

add new blocks. This layer is based on cryptographic and algorithmic techniques, and does not use a central authority, and guarantees the integrity, consistency, and trustworthiness of the blockchain. It also secures the network against bad activities such as double spending or tampering of the blocks and this gives an assurance of trust in an unwarranted environment.

- **Application layer:** The layer liaising the end users with the blockchain is the application layer. It allows applications, smart contracts and both decentralized and security protocols to run, making blockchain functionality a real-world application, including digital identity, supply chains, financial transactions, and access control. Automation The application layer is based on trustless interaction, enabled by automation into smart contracts, self-running code executed by satisfying some conditions, and reduced intermediary dependencies. It also implements security controls to secure confidentiality, authentication and data integrity, and introduces the blockchain strength to real-life applications. [7].

5. Consensus mechanisms

The mechanism and security implications as well as the consensus type can be similar to the table1 below. Consensus type Mechanism Security implications Evidence of work Computational puzzles Immunity to sybil attacks but energy-consuming. Evidence of stake-based validation Will minimise energy consumption, susceptible to nothing at stake. Delegated Pos, Authority certification Trust based governance, risks of centralization.

Table 1: Consensus mechanisms and security implications

Consensus type	Mechanism	Security implications
Proof of work	Computational puzzles	Resistant to sybil attacks but energy intensive
Proof of stake	Stake based validation	Reduces energy use, vulnerable to nothing at stake
Delegated Pos, Proof of authority	Governance based trust	Improved scalability, centralization risk

6. Blockchain Types Public blockchain:

A public block chain is a complete decentralized and open network where any participant can join it and help validate transactions and provide consensus without any prior approval. This transparency facilitates censorship resistance, immutability, and transparency, which is especially appropriate to a trust less setting in which participants do not require a central authority. Bitcoin and Ethereum are examples where consensus is reached by either the use of a proof of work or proof of stake, such that all transactions become publicly verifiable, and are cryptographically secured. Nevertheless, this model tends to be compromised in respect of scalability and transaction throughput with respect to high degree of decentralization. Examples of such blockchain include hyper ledger fabric, which was a private blockchain with enterprise grade security. [8].

- **Consortium blockchain:** In a consortium blockchain, shared governance is applied: the control and decision-making are shared between a group of select organizations or institutions rather than one. The hybrid model is a mixture of the public and private blockchains that are partially decentralized, yet maintain a higher level of efficiency and access control. Transactions can only be validated by authorized participants and they can participate in consensus, enhancing the performance, scalability, and confidentiality, over fully public

systems. Consortium blockchains are effective in cases of interorganizational cooperation, such as finance, supply chain management and health care where mutual trust, transparency, and information integrity is desired but not open public access.

- **Hybrid block chain:** Hybrid block chain combines both characteristics of a public block chain architecture and a private block chain architecture with features of transparency and confidentiality and control respectively. This model enables organizations to identify specific data or transactions to be publicly accessible to guarantee transparency and verifiability or exploit selective access permission and customizable solutions that optimise the security, scalability and flexibility. They are especially implemented in situations that require data privacy and regulation as in government services, enterprises operations and cross industry alliance. [10].

7. Block chain applications in cyber security Taxonomy and Network security Denial of service mitigation:

- **Distributed denial of service (DDos):** Decentralized DDos and bandwidth allocation systems based on block chain technologies assist in removing centralized points of overload since control and resources management is spread across several nodes. A blockchain based DNS is more resilient, censorship resistant, fault tolerant compared to traditional DNS architecture as it is decentralized and vulnerable to attacks and bottlenecks. On the same note, block chain permitting bandwidth management can provide efficient and tamper proof control of network resources and prevents network congestion and single points of failure. Taken together, these decentralized methods add to the resiliency and scalability of digital infrastructures through the reduction of the vulnerabilities of centralized systems [11].

- **Intrusion detection systems:** block chain technology can be used to protect the logs that the intrusion detection systems produce, making sure that the integrity, immutability and traceability of the security events recorded. The use of IDS logs stored in a block chain enables organization to safeguard these crucial records against manipulation or unauthorized modification of the data of such records, which is necessary in proper forensic investigation and auditing of compliance. Such a method will promote confidence in the detection process, the ability of attackers to share threat information in real-time via fully decentralized networks, and the ability to create collaborative defenses against new cyber threats. [12].

- **Secure routing:** block chain enabled border gateway protocol (BGP) validation: this improves the safety and reliability of network routing by offering a decentralized and tamper-proof platform that verifies routing announcement genuineness. The traditional BGP does not resist route hijacking and man in middle attacks because it is based on the implicit trust among network operators. Using the immutable ledger and consensus of the block chain, network participants will be able to cryptographically confirm route origin and path information, meaning there are significantly decreased chances of a malicious routing updates, and the integrity and overall resiliency of internet communications is enhanced [13].

8. Integrity and confidentiality of data

Irreversible audit trails: the append only ledger model of block chain technology ensures that once records are entered into it they cannot be changed or removed and hence this ensures non-repudiation in audit logs and other digital forensic data. This immutability offers a reliable and open-minded process to retain audit trails which are not susceptible to modifications or fraud which is important to regulatory compliance, incident investigation, and accountability. Through the use of block chain to audit log. Organizations are able to have verifiable and time stamped records that facilitate forensic analysis and assist to have clear chains of custody in cyber security as well as legal environments. [14].

- **Data provenance:** block chain technology will enable the data ownership and history of data changes to be tracked in the secure cloud storage environments, and this will give a permanent and transparent account of all the changes done to a given data set. This means that the source, storage and processing of data can be verified and audited, and this is important in ensuring audit trails that cannot be altered or ruined by fraud, this is essential in regulatory compliance, investigation and accountability of incidents. Using block chain to assist with audit logging, organizations would be able to produce verifiable and time stamped records, which can be used to aid in the same process of forensic analysis as well as enable clear chain of custody, whether in the realms of cyber security or legal proceedings [15].

- **Data provenance:** The block chain technology enables the management of data ownership and history of data modification in the safe cloud storage environments which provides an unalterable and transparent history of all changes of a dataset. This feature will guarantee that the source, custody and transformation of data can be verified and audited, which is essential in preserving the data integrity, responsibility and trust in distributed clouds. With the use of the decentralized ledger of the block chain, organization can remove un-authorized changes to the block chain in order to support compliance with data governance rules and facilitate improved security in collaborative and multi tenant cloud environments.

- **Shared encrypted data:** block chain using smart contracts provides the opportunity to control dynamically and automatically the capacity to access data in an encrypted data sharing environment. Such self-executing contracts provide a preset access control without involving middlemen so that valuable information is not shared with unauthorized individuals under certain circumstances. The strategy will increase the data confidentiality, auditability and trust by offering a transparent, tamper resistant method of managing facilitated encrypted data sharing will aid secure collaboration between organizations and reduce the risks relating to unauthorized exposure of data. [16].

9. Identity and access control (IAM)

- **Decentralized Identity (DID):** Decentralized identity systems enable users to have self sovereign identities where individuals have the capacity to generate, maintain and delegate their online identities without having to go through

centralized identity providers. This has been applied through the use of platforms like uport and soverin that use block chain to safely store verifiable credentials and authentication information in decentralized form. This also removes the risks of centralized repositories of identity, including breach of data, identity theft and loss of control over user identity. DID systems support increased trust, security and interoperability across online services and digital ecosystems by it enabling privacy preserving, user centric identity management. [17].

- **Authentication and authorization:** block chain systems have tokenized access control to substitute the conventional password reliant authentication models. These systems can be used to verify user identities and access rights that are secure, decentralized and tamper resistant by issuing cryptographically secured digital tokens or credentials stored on a block chain. By so doing, vulnerabilities such as password theft, phishing and centralized credential data bases are mitigated, to the overall enhanced security fine grained and auditable access control across the distributed applications that enable seamless and reliable user authentication in trustless environments.

- **IOT Security:** Authentication of devices: In the internet of things system, block chain will be used as a distributed trust anchor to perform secure and decentralized device authentication. The system prevents the inclusion of unverified and unauthorized devices in the network by storing the IoT device, and the cryptographic identities on the block chain ledger to ensure that only known and trusted devices can access the network. This decentralised method eliminates centralisation-related risks, including a point of failure and targeted attack to improve the security of the network. Also, the immutable record that block chain provides makes it easier to maintain transparency of device province and accountability, which is of paramount importance in the management of large scale, heterogeneous Iot environments. [19].

- **Edge security:** The combination of block chain technology and edge computing to improve the scalability and security of internet of things deployments is due to the increased decentralized processing and validation on the network edge. This will minimize the latency and bandwidth usage as data verification and security is done nearer to the source devices, and the block chain ledger will have an immutable record that can be audited and trusted. Through integrating both edge computing and block chain, Iot networks will be able to enjoy a strong defense against the cyber attacks, real time decision making, and information integrity and confidentiality across distributed nodes, thus enabling to achieve secured and efficient large scale IOT systems.

9.1 Cyber threat intelligence and forensics.

- **Threat data sharing:** block chain technology enables verifiable and trusted transfer of cyber security threat intelligence especially indicators of compromise (IoCs) among dissimilar organizations and security systems. Block chain prevents the possibility of misinformation or manipulation of data, and since the IoCs are documented in an immutable and decentralized ledger, shared threat information is genuine, resistant to tampering, and transparently

auditable. This strength improves the collective defense capabilities by providing timely and credible information to the traditional or network of critical threat, cultivates collaboration, and increases the integrity of the entire network related to the dynamic cyberattack. [20].

- **Incident reporting:** block chain technology offers an unchangeable and non-repudiated system in documenting forensic evidence and incident report information, by so doing, organizations will be assured that incident documentation will be untouched and capable of verification during the investigation process. Such immutability increases accountability and facilitates compliance with regulatory demands and improves the trustworthiness of the digital evidence provided in the audit or litigation. Therefore, block chain facilitated incident reporting instills more trust in cyber security intervention and forensic investigation.

- **Multiple organization block chain consortium:** Multi organization block chain consortium allow the development of coordinated and decentralized defense networks that can be used to share threat intelligence, security alerts, and mitigation strategies in real time. Using a common, undiscoverable ledger, these consortiums improve trust, transparency, and responsibility among the involved parties and diminish the threat of misinformation, as well as providing uniformity in response measures. These collaborative defense models will enable organizations to more comprehensively detect, examine and respond to advanced cyber-attacks and threats than individually, enhancing the overall resilience and security posture of interconnected digital ecosystems. [21].

Comparative analysis:

Table 2: Comparative Analysis of Application Domains

Application domain	**Key benefits**	**Limitations**	**Typical platforms**
Network security	Decentralization, trustless validation	Scalability constraints	Ethereum, Hyper ledger
Data integrity	Tamper proof logs	Data storage overhead	IPFS, fabric
IAM	User sovereignty, privacy	Recovery complexity	Sovrin, civic
IoT security	Device trust automation	Resource constraints	IoTA, Vechain
Threat intelligence	Verifiable sharing	Data confidentiality	Hyper ledger, Corda

10. Attack taxonomy and security concerns and Block chain targeted attacks

Type of attack Description Migration 51% attack Bad control of majority hash power Checkpointing, hybrid consensus. Sybil attack Spoofing with nodes, PoS. Vulnerabilities of smart contracts code exploitation such as DAO hack Examples of formal verification, audit tools Eclipse attack Particular node isolation Randomized connections in network monitoring. Privacy leakage Public data inference Zero knowledge proofs, ring signatures.

(i). Incorporation with the new cyber security paradigms and artificial intelligence and block chain : Block chain performance can be improved dramatically with artificial intelligence being used to enable danced anomaly detection and support adaptive consensus mechanism that dynamically optimized network efficiency and security. With the machine learning models, AI has the ability to detect an abnormal pattern or possible attack before they occur enabling the block chain networks to react to the danger and minimize latency. On the other hand, block chain technology guarantees AI training data set data province and integrity by keeping an unalterable and transparent history of Data origins, modifications and usage. Such symbolic association enhances the validity and responsibility of AI systems and strengthens the security and credibility of block chain systems. [22].

(ii). Block chain and zero trust architecture : A combination of a decentralized trust model of block chain and zero trust architecture (ZTA) introduces a setting with context aware and verifiable trust boundaries, which increase the security of the contemporary digital setting. In contrast to the traditional perimeter based security system, zero trust assumes that there is no implicit trust, thus authenticating all users, devices as well as transactions depending on the dynamic circumstances in form of behavior, location and risk factors. This is supplemented by block chain, which offers an irrevocable, transparent and distributed register containing and certifying authentication events, access requests and policy enforcements actions without a centralized authority. This synergy allows the effective enforcement of zero trust policies with the aim that any trust decision is auditable, tamper resistant, and can be adjusted to the changing threats, and in that way, it securely enhances the security posture of an organization to considerable extents. [23].

(iii).Post Quantum cryptography and block chain: The future robustness of block chain technology requirements require the incorporation of post quantum cryptography algorithms that are able to survive the computing power of the emerging quantum computers. Conventional cryptographic schemes e.g. elliptic curve cryptography or RSA can be attacked by quantum algorithms like that by Shore, which would invalidate security in block chains by allowing keys to be factored quickly or could be used to crack cryptographic signatures. To counter the fuzzing of keys in a short time or the cracking of digital signatures. In case of these risks, block chain systems should implement Quantum resistant cryptographic primitives such as lattice based has-based, multivariate polynomial-based and code based algorithms that ensure a high level of security against quantum adversaries. [24]. Introducing them to block chain protocols will ensure the safety of the immutability, confidentiality and integrity of the distributed ledgers in a post quantum world, which will preserve the trust and persistence of the ecosystem that is decentralized.

11. Difficulties and unrestricted research questions

(i). Scalability Vs Security tradeoffs: block chain networks are usually characterised by a trade of between scalability, the capacity to execute a large number of transactions within a short period of time and security. Resource intensive and slow high security consensus mechanisms like proof of work can constrain transaction throughput and alternative mechanisms that are faster may create vulnerabilities. To balance all these factors, it is necessary to have novel protocol designs that maximize

the performance without jeopardizing its resistance in case of attacks, and to guarantee its efficiency and strength.

(ii). Privacy protection in public chains: in public block chains, transparency and immutability are prioritized, and in these situations such openness can contradict privacy considerations, in particular, in cases of sensitive information. Zero knowledge proofs, ring signatures and confidential transactions, are also being implemented and developed in order to allow privacy preserving features that guard user identities and transaction information, and retain the verifiability and trustworthiness of the ledger.

(iii). Standardization and interoperability: Block chain ecosystem contains a wide variety of platforms and protocols, which are usually not standardized, which makes it difficult to have smooth communication and data exchange across networks. It is important to standardize and foster interoperability solutions including cross chain bridges and universal protocols in order to support collaborative block chain environments and general industry adoption.

(iv). Energy efficiency: A lot of block chain consensus algorithms and especially proof of work use significant energy which has put environmental pressures and operational expenses on the table. To deal with this problem, one should consider incorporating the energy efficient consensus algorithms such as proof of stake (PoS), delegated proof of stake (DPoS), or alternative approaches that will minimally affect the carbon foot print without compromising security and decentralization.

(v). Legal and regulatory compliance: block chain is decentralized and frequently pseudonymous, which poses a problem to legal and regulatory frameworks, such as the data privacy issues, the anti-money laundering challenges, and the know your customer (KYC) issues. These complexities can only be overcome by designing the solution of complaint block chains and communicating with relators so as to design balanced policies that support innovation without compromising user rights.

(vi). Threats to quantum computing: The quantum computing advert is a major threat to the security block chain networks of the existing cryptographic algorithms. Digital signatures and hash functions that block chain security is based on may be compromised by quantum attacks. In response to this, it is necessary to incorporate post-quantum cryptographic algorithms and non-stop surveillance improvements in quantum-resistant technologies into block chain infrastructure to future proof. [25,26,27,28,29].

12. Future research directions

(i). Federated learning based on block chain cyber security analytics: federated learning to provide block chain integrated with privacy preserving cyber security analytics. Such a system would enable the sharing of threats and anomalies across several organizations without exchange of any sensitive information, and the inability to change or alter data, which would be provided by block chain as an immutable registry, to provide integrity and trust in the learning process.

(ii). Cross chain security mechanisms: creating strong cross chain protocols and security systems, which will facilitate smooth and safe interoperability across heterogenous block chain networks. These mechanisms are designed to facilitate coordinated cyber defense approaches, so that the threat intelligence, security policies and incident responses can be distributed and applied within various block chain ecosystems successfully.

(iii). Energy efficient consensus models: Exploring new consensus designs including proof of useful works, which are designed to minimize the environmental cost of block chain

mining by recycling computational resources to solve real-world problems that are useful but do not affect the safety of the network or its decentralization.

(iv). Combination with digital twin systems: exploring the application of block chain to improve the security and reliability of digital twin technologies, which develop the virtual versions of physical systems. Block chain can offer tamper proof data provenance, secure synchronization, and decentralized control to digital twins that enhance the resiliency to the cyber threats and operational abnormalities.

(v). Policy driven cyber defense frame work: development of block chain enabled frameworks which embed dynamic policy driven cyber security controls. These systems would allow automatic enforcement, auditing and flexibility and coordinated defense mechanisms in accordance with organizational and regulatory needs.

13. Conclusion

Block chain is providing a paradigm shift in the centralized to trustless security designs. It offers good grounds to secure networks, data, identities and devise though its decentralized consensus and immutable ledger. But in the practical implementation there is a challenge in the aspect of scalability, privacy and compliance to regulations. The way forward of block chain enabled cyber security will be in continued research on hybrid models that integrate AI, zero trust and post quantum cryptography.

References

[1]. S. Jawhar, J. Miller and Z. Bitar, "AI-Driven Customized Cyber Security Training and Awareness," 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2024, pp. 1-5, doi: 10.1109/ICAIC60265.2024.10433829.

[2]. D. R. Birari, V. U. Rathod, A. Dandavate, N. Shelke, R. Kumar and M. M. S. Kulkarni, "The Role of Blockchain Technology in Supply chain Management for Data Security," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-5, doi: 10.1109/ICBDS61829.2024.10837326.

[3]. J. Wieme, M. Baert and J. Hoebeke, "Digital Twin Network for dynamic management of a Bluetooth Mesh Network," NOMS 2024-2024 IEEE Network Operations and Management Symposium, Seoul, Korea, Republic of, 2024, pp. 1-3, doi: 10.1109/NOMS59830.2024.10575077.

[4].T. Soni, D. Gupta, M. Dutta and G. Gupta, "Tracing Food Products in Supply Chain Using DLT Enabled Blockchain Technology," 2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM), Roorkee, India, 2023, pp. 1-6, doi: 10.1109/ELEXCOM58812.2023.10370526.

[5].K. K. Ramachandran, B. Nagarjuna, S. V. Akram, J. Bhalani, A. M. Raju and R. Ponnusamy, "Innovative Cyber Security Solutions Built on Block chain Technology for Industrial 5.0 Applications," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 2023, pp. 643-650, doi: 10.1109/AISC56616.2023.10085577.

[6].M. Vashisth and S. K. Verma, "State of the Art Different Security Challenges, Solutions on Supply Chain: A Review," 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 427-431, doi: 10.1109/ICIDCA56705.2023.10099966.

[7].D. R. Birari, V. U. Rathod, A. Dandavate, N. Shelke, R. Kumar and M. M. S. Kulkarni, "The Role of Blockchain Technology in Supply chain Management for Data Security," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-5, doi: 10.1109/ICBDS61829.2024.10837326.

[8].J. Shree, N. R. Kanimozhi, G. A. Dhanush, A. Haridas, A. Sravani and P. Kumar, "To Design Smart and Secure Purchasing System integrated with ERP using Block chain technology," 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2020, pp. 146-150, doi: 10.1109/ICCCA49541.2020.9250767.

[9].P. Lavanya, I. V. Subbareddy and V. Selvakumar, "Internet of Things enabled Block Level Security Mechanism to Big Data Environment using Cipher Security Policies," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-6, doi: 10.1109/ACCAI53970.2022.9752603.

[10].M. Fischer et al., "Technological Framework for a Secure and Resilient Food Supply Chain," 2025 IEEE International Conference on Cyber Security and Resilience (CSR), Chania, Crete, Greece, 2025, pp. 146-152, doi: 10.1109/CSR64739.2025.11130161.

[11].R. Karthiga, P. K. E, S. Kumari, K. P. G, V. Sureka and V. S. Pandi, "A Logical Cyber Security Enabled Methodology Design for Identifying Distributed Denial of Service Attacks Using Enhanced Learning Principles," 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, 2023, pp. 104-109, doi: 10.1109/ICSCNA58489.2023.10370356.

[12].J. Chen, Y. Guo, K. Shi and M. Yang, "Network Intrusion Detection Method of Power Monitoring System Based on Data Mining," 2022 2nd International Conference on Algorithms, High Performance Computing and Artificial Intelligence (AHPCAI), Guangzhou, China, 2022, pp. 255-259, doi: 10.1109/AHPCAI57455.2022.10087405.

[13].R. Sharma, V. Sharma, T. K. Vashishth, S. Chaudhary, K. K. Sharma and S. Kaushik, "Securing Routing in MANETs: A Comprehensive Review of Enhanced Optimized Link State Routing (EOLSR)," 2025 International Conference on Intelligent Computing and Knowledge Extraction (ICICKE), Bengaluru, India, 2025, pp. 1-6, doi: 10.1109/ICICKE65317.2025.11136709.

[14].G. B. Renuka and D. S. Gnanavel, "Leveraging Block Chain for Scalable and Transparent Cloud Security," 2025 2nd International Conference on Computing and Data Science (ICCDS), Chennai, India, 2025, pp. 1-5, doi: 10.1109/ICCDS64403.2025.11209466.

[15].G. Subramanian and H. Nagabushanam, "Governance of Data Product in Multi-layered IoT system," 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022, pp. 1-4, doi: 10.1109/ICECCME55909.2022.9987960.

[16].S. Lin, X. Wang and S. Nie, "Equipment Data Sharing Method Based on Block chain," 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Beihai, China, 2021, pp. 690-693, doi: 10.1109/ICMTMA52658.2021.00159.

[17].S. B. Öztürk and M. Aydos, "A Blockchain Based Decentralized Identity, Access Management, and Trust Evaluation Framework for IoT," 2023 16th International Conference on Information Security and Cryptology (ISCTürkiye), Ankara, Turkiye, 2023, pp. 1-6, doi: 10.1109/ISCTrkiye61151.2023.10336156.

[18].B. Kim, S. Yoon, Y. Kang and D. Choi, "Secure IoT Device Authentication Scheme using Key Hiding Technology," 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 1808-1810, doi: 10.1109/ICTC49870.2020.9289309.

[19].P. R. Kapula, J. G. Jeslin, G. Hosamani, P. Vats, C. J. Shelke and S. K. Shukla, "The Block Chain Technology to Protect Data Access Using Intelligent Contracts Mechanism Security Framework for 5g Networks," 2022 2nd International Conference on Advance Computing

and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 202-206, doi: 10.1109/ICACITE53722.2022.9823471.
[20].G. Xu, S. Xu, J. Ma, J. Ning and X. Huang, "An Adaptively Secure and Efficient Data Sharing System for Dynamic User Groups in Cloud," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5171-5185, 2023, doi: 10.1109/TIFS.2023.3305870.
[21]. Y. Pan, Z. Cheng, Y. Liu, B. Wang, W. Wang and C. Zhu, "Research on Trusted Data Sharing Method for Multi-party Edge Terminals," 2022 IEEE International Conference on Unmanned Systems (ICUS), Guangzhou, China, 2022, pp. 204-208, doi: 10.1109/ICUS55513.2022.9987168.
[22].J. Li and Y. Guo, "AI Data Analysis Applications and Challenges Based on Block Chain Technology," 2025 7th International Conference on Artificial Intelligence Technologies and Applications (ICAITA), Wenzhou, China, 2025, pp. 425-429, doi: 10.1109/ICAITA67588.2025.11137961.
[23].X. Peng, T. Ma, C. Zheng, Z. Shen and X. Cui, "BCTD-ICS: A Blockchain-Aided Framework for Trusted Detection of Industrial Control System Components," in IEEE Internet of Things Journal, vol. 12, no. 18, pp. 37552-37570, 15 Sept.15, 2025, doi: 10.1109/JIOT.2025.3583304.
[24].G. P. Dubey, A. Giri and J. Moolchandani, "Exploring the Synergy and Challenges of Blockchain Technology in the Quantum Cryptography Era: A Comprehensive Review," 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI), Greater Noida, India, 2025, pp. 165-170, doi: 10.1109/ICCSAI64074.2025.11063720.
[25].W. Hao, F. Zhou, M. Zeng, O. A. Dobre and N. Al-Dhahir, "Ultra Wideband THz IRS Communications: Applications, Challenges, Key Techniques, and Research Opportunities," in IEEE Network, vol. 36, no. 6, pp. 214-220, November/December 2022, doi: 10.1109/MNET.110.2100664.
[26].H. Ren, X. Liu, H. Xu, C. Zhang and K. Li, "CubeChain: Generalized Query Framework for Intra- and Cross-Chain Scenarios," 2024 IEEE 44th International Conference on Distributed Computing Systems (ICDCS), Jersey City, NJ, USA, 2024, pp. 345-355, doi: 10.1109/ICDCS60910.2024.00040.
[27].S. R. Alam, S. Jain and R. Doriya, "Security threats and solutions to IoT using Blockchain: A Review," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 268-273, doi: 10.1109/ICICCS51141.2021.9432325.
[28].A. Dutta, N. I. Rafin, M. A. A. Dewan and M. G. R. Alam, "ROBB: Recurrent Proximal Policy Optimization Reinforcement Learning for Optimal Block Formation in Bitcoin Blockchain Network," in IEEE Access, vol. 12, pp. 31287-31311, 2024, doi: 10.1109/ACCESS.2024.3369896.
[29].J. Ding, A. Bouabdallah and V. Tarokh, "Key Pre-Distributions From Graph-Based Block Designs," in IEEE Sensors Journal, vol. 16, no. 6, pp. 1842-1850, March15, 2016, doi: 10.1109/JSEN.2015.2501429.