

Proceedings of the
SECOND INTERNATIONAL CONFERENCE
ON
**RECENT TRENDS IN MULTI-DISCIPLINARY
RESEARCH AND INNOVATION**
ICRTMRI' 25

19th September 2025

in Association with



Organized by



AVP (Autonomous)
COLLEGE OF ARTS AND SCIENCE



Affiliated to Bharathiar University, Coimbatore
Accredited with 'A' Grade by NAAC (Cycle I)
Recognized under Section 2(f) of the UGC Act 1956
An ISO 9001:2015 Certified Institution, T.M. Poondi, Tirupur.

134	ICRTMRI/25/ T2/134	SECURE WIRELESS SENSOR NETWORKS WITH HYBRID DEEP LEARNING BASED INTRUSION DETECTION	Mr. N. VIGNESH KUMAR Dr. PREETHA,	957
135	ICRTMRI/25/ T2/135	OCEANIC OBLIGATION AND OPPORTUNITY – NAVIGATING THE FUTURE TOGETHER	MERVIN. K, LOGANATHAN. V	966
136	ICRTMRI/25/ T2/136	GAMIFIED LEARNING ANALYTICS WITH MACHINE LEARNING FOR PERSONALIZED EDUCATION	NAVEEN RAMACHANDRAN, RAHUL.S .M	971
137	ICRTMRI/25/ T2/137	A SURVEY OF BLOCK CHAIN APPLICATIONS IN NETWORK SECURITY AND CYBER DEFENSE WITH SOLUTION APPROACHES	JEEVASHANTHINI. S	977
138	ICRTMRI/25/ T2/138	SEMANTIC WEB ONTOLOGY AS A KNOWLEDGE BASE FOR AI DECISION MAKING	YAFIYAH ZENATH. Y, AKILA. S,BHUVANESH WARI.V	985
139	ICRTMRI/25/ T2/139	METHODOLOGICAL WORKFLOW FOR CREATING RAG FOR FARMING ASSISTANTS	KANIGASHREE. R, GOKULALAKSHMI. V, BHUVANESWARI. V	991
140	ICRTMRI/25/ T2/140	FOUNDATIONS AND APPLICATIONS OF QUANTUM COMPUTING : A COMPARATIVE STUDY	Dr.R. RAJ KUMAR, Dr.B.MEENA PREETHI, MEGAVARSHINI. N	998
141	ICRTMRI/25/ T2/141	SECURE PATIENT-CENTRIC EHRS USING BLOCKCHAIN AND CONSENT TOKENS	ANUJA. A.V, NAKULAN. R,	1005
142	ICRTMRI/25/ T2/142	A COMPARATIVE ANALYSIS OF SECURITY AND PERFORMANCE IN EXPRESS.JS AND FASTIFY APIS AGAINST OWASP TOP THREATS	P.GOWRI, Dr.B.MEENA PREETHI, MUGESH BABU. D,	1010
143	ICRTMRI/25/ T2/143	A REVIEW ON NOSQL DATABASES IN BIG DATA: CONCEPTS, METHODS, AND APPLICATIONS	VELAVA. L , Dr. SHANMUGA RAJATHI	1018
144	ICRTMRI/25/ T2/144	ROBUST DATA AUTHENTICITY AND GROUP SIGNATURE MECHANISM FOR ENHANCED CLOUD SECURITY	G.PRAMELA, SWETHA. K	1021
145	ICRTMRI/25/ T2/145	REAL-TIME SIGN LANGUAGE RECOGNITION SYSTEM USING CONVOLUTIONAL NEURAL NETWORK	Mrs. G.PRAMELA, MsM.THIVETHA	1026
146	ICRTMRI/25/ T2/146	THE FLAWED CANVAS - CONFRONTING SELF-DECEPTION TO PAINT A TRUER ETHICAL SELF-PORTRAIT	Mrs.N.KARTHIKA, N.MANOKARAN	1031

A SURVEY OF BLOCK CHAIN APPLICATIONS IN NETWORK SECURITY AND CYBER DEFENSE WITH SOLUTION APPROACHES

Jeevashanthini S

Assistant Professor, Department of Computer Science(SF)
Nallamuthu Gounder Mahalingam College, Pollachi.

Abstract

Blockchain technology has emerged as a groundbreaking innovation in cybersecurity, offering decentralized, transparent, and tamper-resistant mechanisms to safeguard critical data and transactions across a wide range of application domains. This study presents a comprehensive review of the existing literature to explore how blockchain is being leveraged to enhance cybersecurity measures in diverse sectors including defense, healthcare, industrial systems, smart cities, energy infrastructure, and communication networks. By surveying state-of-the-art applications, this paper highlights blockchain's significant role in identity management, secure data sharing, intrusion detection, and mitigation of cyber threats such as distributed denial-of-service (DDoS) attacks. Additionally, the study discusses key challenges hindering the widespread adoption of blockchain in cybersecurity and proposes various solution approaches to overcome these barriers. Finally, it outlines promising future research directions aimed at fully harnessing blockchain's potential to strengthen the security and resilience of modern networked systems.

Keywords:

Blockchain technology, cybersecurity, network security, decentralization, identity management, secure data sharing, intrusion detection, distributed denial-of-service (DDoS) mitigation, cyber defense, blockchain adoption challenges, solution approaches, smart cities, energy infrastructure, communication networks.

1. Introduction

With the rapid growth of interconnected digital systems, cyber security has become a vital priority for businesses, governments, and individuals worldwide. The expansion of networks and the increasing complexity of cyber attacks have revealed weaknesses in traditional centralized security frameworks, resulting in data breaches, identity theft, and service interruptions. Addressing these issues requires innovative solutions that can foster greater trust, transparency, and robustness within network infrastructures.

This paper provides an extensive overview of current blockchain implementations in network security and cyber defense. It also examines the primary obstacles to blockchain adoption—such as scalability, privacy, and system integration—and offers potential solutions to overcome these challenges. Finally, the paper outlines future research opportunities aimed at leveraging blockchain technology to create more secure and resilient digital networks.

II. Utilizing Blockchain to Strengthen Cybersecurity

Blockchain offers a powerful approach to addressing modern cybersecurity challenges. By distributing data storage and control across a decentralized network, it reduces the risks commonly associated with centralized systems—such as unauthorized access, tampering, and data breaches. Additionally, the use of strong cryptographic methods ensures the confidentiality and integrity of sensitive information. As cyber threats continue to evolve

rapidly, integrating blockchain into cybersecurity strategies presents a range of promising opportunities for enhancing protection and resilience.

The growing sophistication of cyber threats has exposed the limitations of traditional, centralized cybersecurity systems. From ransomware attacks to supply chain compromises, adversaries are increasingly exploiting centralized architectures, single points of failure, and delayed threat responses. Blockchain technology offers a decentralized and tamper-resistant infrastructure that can transform cyber defense strategies across organizations and industries.[1]

One of the most impactful uses of blockchain in cyber defense is in **decentralized threat intelligence sharing**. In conventional setups, threat intelligence is often stored in silos, subject to delays and manipulation. Blockchain enables trusted entities—such as governments, enterprises, and cybersecurity vendors—to share verified threat data in real time using a secure, immutable ledger. This not only fosters cross-organizational collaboration but also ensures data integrity and traceability.[3][4]

Another vital application is the creation of **immutable security logs**. Traditional logs can be altered or deleted by insiders, making forensic analysis unreliable. With blockchain, log entries are permanently recorded and cryptographically secured, providing tamper-proof audit trails that enhance accountability and investigation reliability[5]. Blockchain also addresses **insider threats** and data manipulation risks. Its decentralized nature limits control by any single administrator, making unauthorized changes to system configurations or sensitive data detectable and traceable. Access control decisions and other critical actions can be transparently logged and monitored in real time.[6].

Furthermore, **smart contracts**—self-executing programs deployed on the blockchain—can automate security responses. For instance, if a threat is detected, a smart contract can instantly trigger actions such as revoking access, isolating affected nodes, or notifying administrators, thereby reducing response time and human error.

In combating **Distributed Denial-of-Service (DDoS) attacks**, blockchain's decentralized design eliminates central points of failure that attackers typically exploit. Decentralized DNS services and blockchain-based IP verification systems can provide robust defenses that maintain availability even under high-volume attack conditions.

Finally, blockchain enhances **supply chain security**, a critical concern in modern cyber defense. By recording the origin, ownership, and update history of hardware and software components, blockchain provides complete visibility and traceability. This helps organizations detect counterfeit products and ensure integrity throughout the entire supply chain lifecycle.

III. RELATED WORKS

Recent studies have extensively explored the integration of blockchain technology to address cybersecurity challenges in various domains, particularly focusing on IoT security, identity management, and mitigation of cyberattacks such as DDoS.

Abdulrahman and Useng [7] provided a comprehensive survey of blockchain and distributed ledger technologies (DLTs) applied to IoT security. Their work categorizes applications such

as authentication, access control, and data integrity, while also highlighting open challenges like scalability and privacy.

Bao et al. [8] proposed **IoTChain**, a three-tier blockchain-based architecture aimed at enhancing IoT security by providing identity authentication, access control, and resilience against denial-of-service attacks. Their approach reduces overhead in resource-constrained IoT devices while maintaining robust security.

Rahman et al. [9] critically analyzed the performance and scalability limitations of existing blockchain platforms when applied to IoT networks. They emphasized that conventional blockchain protocols often fall short in meeting the low latency and throughput requirements of IoT environments.

In the context of mitigating DDoS attacks, Udousoro [4] demonstrated how smart contracts and Ethereum blockchain can isolate malicious IoT devices, reducing the impact of such attacks on network availability.

The challenge of decentralized identity management was addressed by a recent study proposing the Blockchain Aware Decentralized Identity Management and Access Control system (BADIMAC) [10]. This system enables self-sovereign identity verification without reliance on central authorities, thereby improving transparency and user privacy.

Poonia and Tinker [11] evaluated the cost models associated with blockchain-based DDoS mitigation strategies, highlighting important trade-offs between economic feasibility and system performance.

Finally, Sousa et al. [12] focused on IoT identity management via blockchain, stressing the need for defining device identity and privacy considerations in real-world deployments.

IV. Blockchain-Enabled Security Solutions

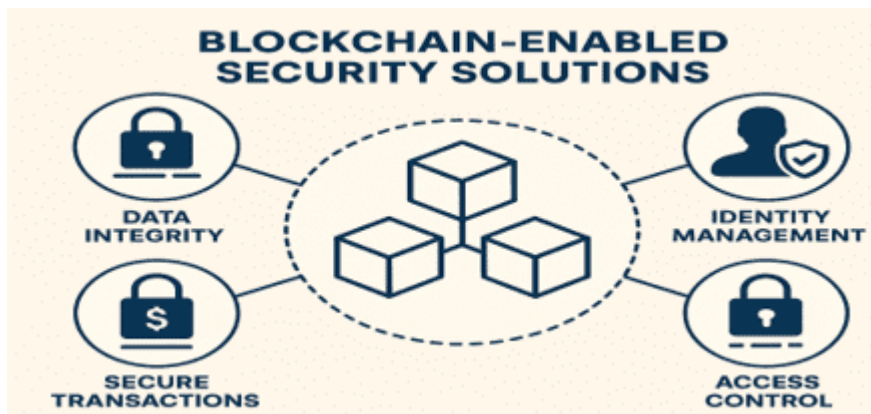


Fig 1:Blockchain –Enabled Security Solution

Blockchain-enabled security solutions leverage blockchain's decentralization, immutability, and cryptographic features to enhance cybersecurity. For example, blockchain-based identity management systems give users greater control over their identities and reduce single points of failure [13]. In another study, immutable logging across multiple sites was implemented on a blockchain ledger to securely store access logs, thus enabling tamper-resilient audit trails and

eliminating manipulation risks by administrators [14]. Smart contract-based frameworks have also been used for advanced authentication and authorization, automating policy enforcement in cloud environments, thereby reducing delays, human error, and centralized trust dependencies [15]. These examples illustrate the promise of integrating blockchain into security strategies to improve confidentiality, integrity, and resilience.

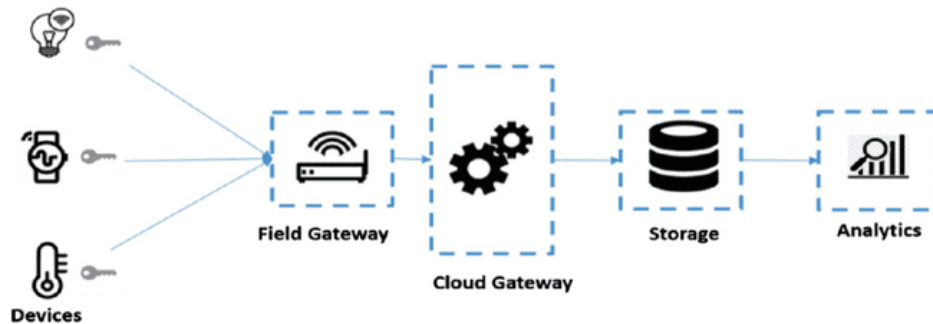


Fig 2: Blockchain for Enhancing Security of IoT Devices

V. Benefits of Blockchain in Enhancing Cybersecurity and Cyber Defense

Blockchain technology is one of the popularly noted and known terms nowadays in the field of secure transmission of credential data over the internet. Each block contains user data with high secure hash code as well as the previous block hash code and forms a secured chain. Any unauthorized accessibility can be easily detected in blockchain technology. With its strong security policy, this technology uses in many areas like Markets (Billing, Marketing, etc.), Government Sector (Document digitization / Contracts, Voting, Registries etc.), IOT (Self-driving cars, personalized robots) [1] , HealthCare systems, Finance, and Accounting and many more.

As we know that in the current scenario where the number of internet users increased day by day, the number of cyber attacks also increased comparatively

Benefit	Explanation	Refs.
Data Integrity & Immutability	Tamper-resistant ledger ensures integrity of logs and transactions.	[16]
Decentralization	Removes single points of failure; more resilient to DoS and centralized attacks.	[16], [20]
Identity Management	Cryptographic identities and self-sovereign authentication reduce identity theft and credential attacks.	[17], [18]
Transparency & Audit ability	All transactions are traceable and verifiable, supporting forensic analysis.	[16], [20]
IoT Security	Lightweight blockchain ensures secure device identity, updates, and certification management.	[18], [19]

Table 1: Benefits of Blockchain in Enhancing Cybersecurity and Cyber Defense

VI. Solutions Enabled by Blockchain and Their Challenges

1. [21] (2019) — Sidechain Security, IoT Security (Public & Private)

- **Solution:** Blockchain sidechains strengthen device, network, and user security. PoW ensures cryptocurrency protection.
- **Challenge:** A decentralized trustless system alone cannot resolve all cybersecurity issues; stronger cryptography and certification standards are needed.

2. [22] (2020) — Smart Home Security (Consortium)

- **Solution:** Blockchain framework replaces centralized databases with decentralized storage, securing IoT-based smart homes.
- **Challenge:** Smart contracts may increase costs; public blockchains are unsuitable due to scalability problems.

3. [23] (2018) — Privacy and Transaction Security (Public, Private & Consortium)

- **Solution:** Blockchain provides verifiable transaction records through consensus across distributed participants.
- **Challenge:** Scalability, privacy, compliance, and governance issues remain unresolved.

4. [24] (2021) — In-Vehicle Network (IVN) Security (Hybrid)

- **Solution:** Hybrid blockchain secures IVNs, with private chains for internal communications and public chains for external links.
- **Challenge:** Balancing internal security with vulnerabilities from public connectivity is difficult.

5. [25] (2018) — Finance & Economics / Cross-Border Payment Security (Public & Private)

- **Solution:** Blockchain enhances financial services by improving cross-border payments, credit evaluation, and market credit systems.
- **Challenge:** Research and applications are still developing; governments must build shared blockchain platforms.

6.[26] (2016) — National Defense (Cyber-enabled Defense Systems) | Private Blockchain

- **Solution:** Blockchain operates independently of security and trust by:
 - Securing digital transactions on the blockchain network, and
 - Using consensus to safeguard events in databases, preventing unauthorized modification.
- **Challenge:** Limited awareness and adoption of blockchain in defense. Research is required to ensure scalable, adaptable, and secure solutions supporting missions in air, space, and cyber domains.

7.[27] (2018) — Electric Vehicles, Cloud and Edge Computing Security | Public & Private Blockchain

Solution: Blockchain-based distributed consensus introduces **data coins** and **energy coins**. Proof-of-Work is achieved through data contribution frequency and energy contribution volume, enabling secure vehicular exchanges.

Challenge: Proof mechanisms relying on data and energy contributions raise issues of secure data transmission from sensors. Risks also arise in wireless charging and trading of energy/data coins, which may expose vulnerabilities.

This paper presented a survey of blockchain technology as an enabler of cybersecurity and cyber defense. We examined recent blockchain-based models and architectures, discussing their role in mitigating cyber threats ranging from data tampering to secure information delivery. Blockchain provides several advantages, including **immutability, transparency, encryption, traceability, fraud prevention, data security, and resilience against single points of failure**, while also reducing reliance on costly infrastructure. Different blockchain types—**public, private, consortium, and hybrid**—were analyzed with respect to their challenges and applicability, offering recommendations for future integration into cyber defense systems.

Despite its challenges, blockchain has already demonstrated its value across domains such as finance, supply chain, digital advertising, and IoT security. Its unique features—particularly decentralization and cryptographic assurance—make it a promising candidate for securing emerging areas such as IoT networks, DNS, data storage, and cyber-physical infrastructure. With continued research and adaptation, blockchain can become a **revolutionary tool for cybersecurity and cyber defense**.

References

- [1] N. Kshetri, C. S. Bhushal, P. S. Pandey, and V. Vasudha, "BCT-CS: Blockchain Technology Applications for Cyber Defense and Cybersecurity: A Survey and Solutions," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 11, 2022. doi:10.14569/IJACSA.2022.0131140
- [2] Y. Zhang, J. Wen, X. Liang, and V. C. M. Leung, "Security and Privacy on Blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp. 1–34, 2019.
- [3] S. K. Singh and N. C. Kaur, "Decentralized Threat Intelligence Sharing Using Blockchain Technology," in *Proc. IEEE Int. Conf. on Cyber Security and Cloud Computing*, 2020, pp. 123–128.
- [4] M. Conti, S. Dehghantanha, N. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.
- [5] <https://www.ironnet.com/topics/what-is-cyber-defense#:~:text=Cyber%20defense%20is%20a%20coordinated,that%20occur%20within%20a%20network>. Accessed on 25/09/2022.
- [6] S. Lee, & S. Kim, "Blockchain as a Cyber Defense: Opportunities, Applications and Challenges", *IEEE Access*, 10, 2602-2618, 2021.
- [7] S. Abdulrahman and M. Useng, "Blockchain and Distributed Ledger Technologies for IoT Security: A Survey," *Mesopotamian Journal of Computer Science*, 2022. [Online]. Available: <https://mesopotamian.press/journals/index.php/cs/article/view/56>

- [8] Z. Bao, W. Shi, D. He, and K.-W. R. Chood, "IoTChain: A Three-Tier Blockchain-based IoT Security Architecture," arXiv, 2018. [Online]. Available: <https://arxiv.org/abs/1806.02008>
- [9] Z. Rahman, X. Yi, I. Khalil, and A. Kelarev, "Blockchain for IoT: A Critical Analysis Concerning Performance and Scalability," arXiv, 2021. [Online]. Available: <https://arxiv.org/abs/2109.02352>
- [10] I. C. Udousoro, "Mitigation of IoT Device Based DDoS Attacks (Using Blockchain)," Journal of Research in Engineering & Computer Sciences, 2023. [Online]. Available: <https://hspublishing.org/JRECS/article/view/236>
- [11] "Blockchain aware decentralized identity management and access control system," Measurement: Sensors, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2665917424000084>
- [12] L. Poonia and S. Tinker, "DDoS Mitigation by Blockchain With Approach of Cost Model," International Journal on Recent and Innovation Trends in Computing and Communication, 2023. [Online]. Available: <https://ijritcc.org/index.php/ijritcc/article/view/9644>
- [13] Blockchain-based identity management systems: A review, Journal of Network and Computer Applications, vol. 166, Sep. 2020, Article 102731.
- [14] Leveraging blockchain for immutable logging and querying across multiple sites, BMC Medical Genomics, 2020.
- [15] Blockchain-Driven Smart Contracts for Advanced Authorization and Authentication in Cloud Security, Electronics, vol. 14, no. 15, 3104, 2023.
- [16] Govea, J., Gaibor-Naranjo, W., and Villegas-Ch, W., "Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience," Computers, vol. 13, no. 5, article 122, 2024. MDPI
- [17] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, Mohammed Samaka, "Security Services Using Blockchains: A State-of-the-Art Survey," arXiv preprint arXiv:1810.08735, 2018. arXiv
- [18] Ricardo Neisse, José L. Hernández-Ramos, Sara N. Matheu, Gianmarco Baldini, Antonio Skarmeta, "Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices," arXiv preprint 1909.07039, 2019. arXiv
- [19] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy," arXiv preprint arXiv:1712.02969, 2017. arXiv
- [20] "The Role of Blockchain in Cyber Security," Semiconductor Science and Information Devices, vol. 3, no. 1, pp. 1–9, 2021. Rafferty, D., & Curran, K. Bilpub Group
- [21] "Secure Cybersecurity Information Sharing for Sectoral Organizations Using Ethereum Blockchain and IPFS," Jurnal RESTI, vol. 7, no. 3, 2021. Tony Haryanto & Kalamullah Ramli.
- [22] KKR Choo et. al (2019). "A systematic literature review of blockchain cyber security, Digital Communications and Networks", ScienceDirect, Volume: 6, Issue: 2, May 2020, Pages: 147-156, DOI: <https://doi.org/10.1016/j.dcan.2019.01.005>.
- [23] M. Imran et. al., "Investigating smart home security: Is Blockchain the Answer? IEEE Access, Special Section on Blockchain-Enabled Trustworthy Systems", Volume: 8, Pages: 117802-117816, 2020, DOI: <https://doi.org/10.1109/ACCESS.2020.3004662>.
- [24] N. Rathod and D. Motwani, "Security threats on Blockchain and its countermeasures", International Research Journal of Engineering and Technology (IRJET) Volume: 05, Issue: 11, e-ISSN: 2395-0056, November 2018, Pages: 1636-1642, DOI: IRJET-Security-threats-onBC-and-its-countermeasures.
- [25] SY Nam et. al., "Security issues with In-Vehicle Networks, and Enhanced Countermeasures based on Blockchain", MDPI Electronics 2021, Volume: 10 (Issue: 8), Pages: 893. Published: 8 April 2021, DOI: <https://doi.org/10.3390/electronics10080893>.

- [26] N. B. Barnas, “Blockchains in National Defense: Trustworthy systems in a Trustless World”, Air University, Maxwell Air Force Base, Alabama, June 2016.
- [27] H. Liu et. al., “Blockchain-enabled security in Electric vehicles cloud and Edge computing”, IEEE Network May/June 2018, DOI: 10.1109/MNET.2018.1700344.