A Strategy to Mitigate Prevalent IoT Vulnerabilities Against Cyber Threats and Data Breaches Through Blockchain Techniques

Hiba Ansari, Harish Tiwari, Chandra Kishor Pandey

***Abstract:** The Internet of Things (IoT) is rapidly evolving into a revolutionary technology, connecting millions of devices and enabling a wide range of applications across industries. However, the tremendous growth of connected devices has raised concerns about the security and privacy of IoT networks. The deployment and distribution of IoT systems make them particularly vulnerable to cyberattacks, unauthorized data access and control, further emphasizing the need for security measures. Traditional security measures often fall short of solving these problems due to the scale, diversity, and resource limitations of IoT devices. With its key features such as decentralization, immutability, transparency, and cryptographic security, Blockchain technology holds promise for addressing these vulnerabilities in IoT. Using blockchain data distribution, data transmitted in IoT networks can be authenticated and secured, ensuring the integrity and confidentiality of users' sensitive information. Blockchain's consensus enables secure communication between IoT devices without the need for a central authority, reducing the points of failure and risk associated with middle management. Blockchain also provides strong identity and capacity management, ensuring that only authorized entities can interact with IoT devices and systems, thus strengthening privacy and preventing unauthorized access. Integration of blockchain technology with IoT environment to enhance their security and privacy. We investigate how blockchain can be used to protect data transmission, device authentication, and access control in the Internet of Things. We also examine the role of smart contracts in operating and maintaining security in IoT systems, such as ensuring that only authorized devices can access or update important information. Although the combination of blockchain and IoT has many advantages, it also brings some challenges that can affect the performance of IoT systems, such as scalability, scalability, and power consumption. This article also discusses these issues and presents solutions, including the use of lightweight algorithms and hybrid blockchain architectures. Performance and privacy benefits and improvements of using blockchain. Overall, research suggests that blockchain can increase the security and privacy of IoT networks, providing a solution and protection against the growing threats of IoT systems. The findings Highlight the potential of blockchain to revolutionize IoT security, enabling a safer, more efficient, and more reliable future for IoT applications across a wide range of industries.*

***Keywords:** IoT Security, Block-chain Technology, Decentralized Network, Immutable Ledger.*

Manuscript received on 24 December 2024 | First Revised Manuscript received on 08 January 2025 | Second Revised Manuscript received on 01 March 2025 | Manuscript Accepted on 15 March 2025 | Manuscript published on 30 March 2025.
***Correspondence Author(s)**

Hiba Ansari*, Scholar, School of Computer Application, Babu Banarasi Das University, Lucknow (Uttar Pradesh) India. Email ID: hibaansari432@gmail.com, ORCID ID: 0009-0008-3226-6248

Harish Tiwari, Scholar, School of Computer Application, Babu Banarasi Das University, Lucknow (Uttar Pradesh) India. Email ID: shanuharish08@gmail.com, ORCID ID: 0009-0007-0764-094X

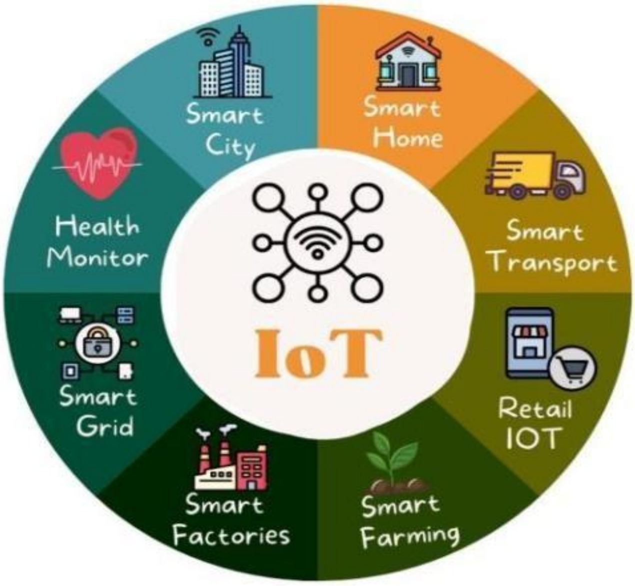
Dr. Chandra Kishor Pandey, Researcher, School of Computer Application, Babu Banarasi Das University, Lucknow (Uttar Pradesh) India. Email ID: ckpandey83@gmail.com, ORCID ID: 0000-0003-1562-680X

I. INTRODUCTION

The rapid increase in Internet of things (IoT) also increases the concern about security vulnerabilities due to the interconnection of the devices. The role of blockchain is to securing the IoT and also efficient by adding a security layer on top of the design. This paper ‘s range is mostly concerned using block-chain technology to improve the IoT [3].

The integration of block-chain and IoT not only improves the security but also protecting user privacy by allowing decentralized identity management and also secure the data sharing. The integration of IoT and Block-chain opens up for creating more trustworthy environments across various sectors [1].

The Internet of Things (IoT) represents a transformative wave in technological advancement, connecting a vast array of devices—from smart home appliances to industrial machinery— allowing them to communicate, share data, and operate autonomously [4].



[Fig.1: IoT Applications]

II. BENEFITS OF RESEARCH WORK

A. Enhanced Data Security and Integrity

- Immutable Data Records Once data is written it cannot be changed.
- Prevention of Data Tampering.
- It is impossible for malicious actors to tamper the recorded data due to consensus mechanism [5].

B. Decentralized Trust and Eliminating Single Points of Failure

- Elimination Vulnerabilities of Centralized.
- There is no single point of failure making the system more robust and secure [8].
- **Peer-to-Peer Authentication:** Devices can authenticate and interact directly through block-chain without relying on a central authority. This peer-to-peer model reduces the risk of data breaches and unauthorized access [7].

III. ENHANCED AUTHENTICATION&ACCESS CONTROL

A. Authentication Without a Central Authority

Block-chain allows for secure and decentralized device authentication. Each IoT device can have a unique, verifiable identity on the block-chain, preventing unauthorized devices from joining the network [9].

B. Self-Validating Devices

IoT devices can validate their authenticity by using cryptographic proofs stored on the block-chain, which minimizes the risk of man in the middle attacks or device spoofing [7].

IV. TRANSPARENCY& AUDITABILITY

A. Complete Transparency

Transaction viewed by all participants by public ledger which helps in building trust and transparency.

B. Enhanced Audit Capabilities

Every transaction or data exchange in an IoT system is recorded on the block-chain, providing an immutable audit trail. This helps businesses and regulators to monitor IoT activities, detect fraud, and ensure compliance with standards and regulations [11].

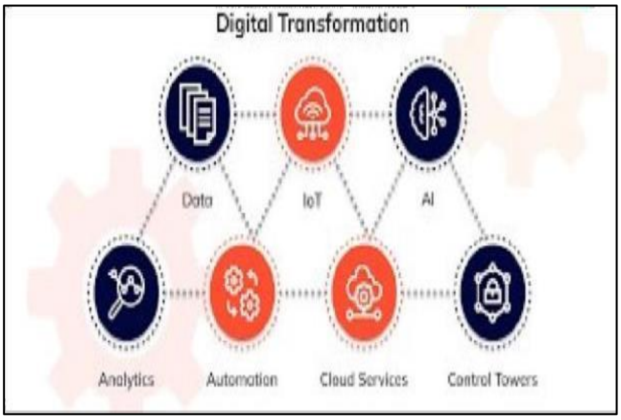
C. Reduced Risk of DDOS and Other Attacks

i. Resilience Against DDoS Attacks

In traditional IoT networks, DDoS attacks can overwhelm central servers, disrupting service. Block-chain's decentralized architecture makes it difficult for attackers to target a single point of failure, thereby increasing resilience against such attacks.

ii. Distributed Consensus

The consensus mechanisms in block-chain make it more challenging for malicious actors to Manipulate or disrupt the network, providing a higher level of security against various types of attacks [8].



[Fig.2: Digital Transformation]

V. SCALABILITY & EFFICIENCY –IN LARGE-SCALE IOT SYSTEMS

- *Efficient Management of Large Networks:* As IoT deployments grow, managing device security becomes more complex. Block-chain provides a scalable solution to track and manage a large number of IoT devices, ensuring that each device's interactions are secured and verifiable [13].
- *Optimized Resource Management:* Block-chain allows for decentralized processing of data, reducing the burden on [9].

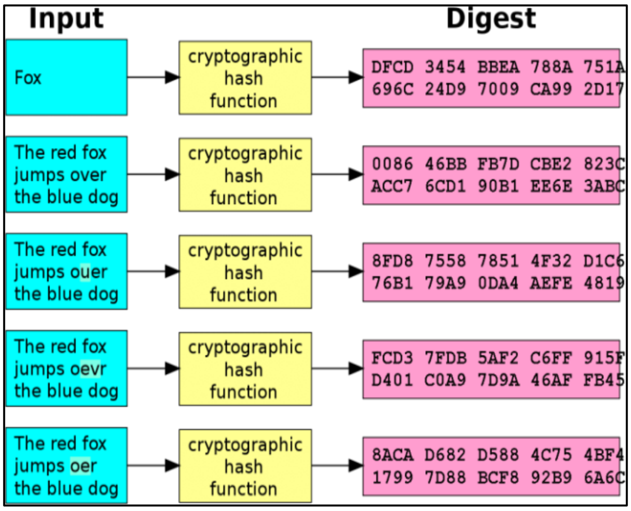
VI. BRIEF LITERATURE SURVEY

Zhang et al. (2018) highlight that the decentralized nature of block-chain can significantly reduce risks associated with central points of failure in IoT systems. By distributing data across multiple nodes, block-chain enhances resilience against attacks [1]. Atzori et al. (2018), discuss how block-chain can ensure data integrity through cryptographic techniques. Each transaction is securely hashed and linked, which prevents unauthorized alterations and enhances trust in IoT data [2]. Christidis and DevetsikIoTis (2016) explore the potential of block-chain to

Centralized systems and enabling more efficient resource management, especially in high-density IoT networks like smart cities or industrial IoT environments [3]. Han et al. (2020), examine how block- chain facilitates secure data sharing among IoT devices. By using decentralized identifiers and smart contracts, data can be shared with specified parties without compromising security [4]. Hossain et al. (2020) address the interoperability issues among various IoT devices and platforms. They propose block-chain as a solution that enables seamless integration and communication between diverse systems while maintaining security [5].

Zyskind et al. (2015), discuss how block- chain can aid in regulatory compliance by providing an immutable audit trail for data empower users with control over their personal data. Smart contracts can be used to manage permissions for data access, thus enhancing user privacy in IoT applications. Access and sharing, making it easier for organizations to meet legal requirements [6].

Xu et al. (2019) investigate scalability challenges in block-chain systems used for IoT and propose solutions to improve performance, which is crucial for the real-time demands of many IoT applications [7].

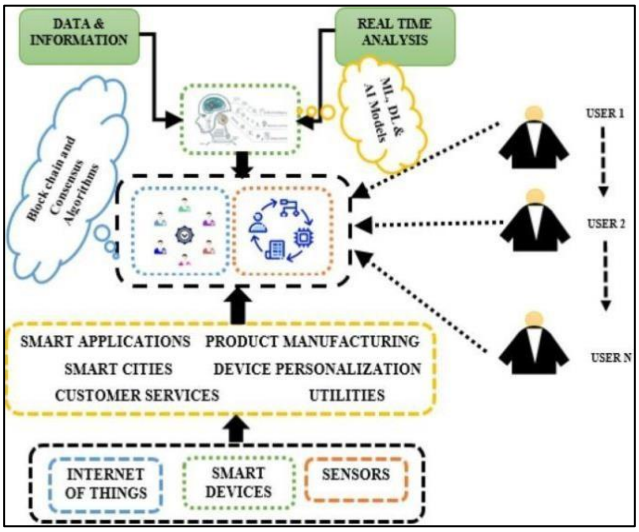

Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

[Fig.3: Input/Digest]

Sultana et al. (2021), provide insights into future trends in also protect a block- chain network from online threats [10].

VII. OBJECTIVES

- To Ensuring ownership and preventing unauthorized access by third parties
- To enhance the block-chain security that will secure the information and data of users. The research will focus on:
  1. Lightweight Protocols for IoT
  2. Designing Scalable and Low Latency Consensus Mechanisms
  3. Ensuring Data Privacy and Security [14]



[Fig.4: Blockchain and Consensus Algorithms]

VIII. PROBLEM FORMULATION

Formulating the problem of boosting IOT privacy and security through block-chain involves identifying key challenges and how block-chain technology will address them:

- **Data Privacy**
- **Security Vulnerabilities**
- **Resource Constraint of IOT Devices**
- **Key Management and Identity Issues**

A. Data Privacy

Data privacy in IoT refers to the protection of sensitive information collected, transmitted, and stored by Internet of Things (IoT) devices from unauthorized access, misuse [7].

B. Security Vulnerabilities

i. *Operating System:* Lightweight OS requirements.
ii. *Application Complexity:* Simplified software design.
iii. *Data Storage:* Limited local storage capacity.
iv. *Network Bandwidth:* Constrained data transmission.
v. *Security:* Limited security features [5].

C. Energy Constraints

i. *Battery Life:* Long battery life requirements.
ii. *Power Harvesting:* Energy scavenging limitations.
iii. *Low-Power Protocols:* Energy-efficient communication
iv. *Sleep Modes:* Power-saving strategies.
v. *Energy-Efficient Design:* Minimizing power consumption [9].

D. Network Constraints

i. *Bandwidth:* Limited data transmission rates.
ii. *Latency:* Delayed communication.
iii. *Connectivity:* Intermittent connections.
iv. *Range:* Limited communication range.
v. *Interference:* Radio frequency interference [4].

E. Storage Constraints

i. *Limited Capacity:* Small storage capacity.
ii. *Data Management*: Efficient data handling.
iii. *Data Compression:* Reducing storage needs.
iv. *Cloud Storage:* Offloading data storage.
v. *Edge Computing:* Processing data locally [4].

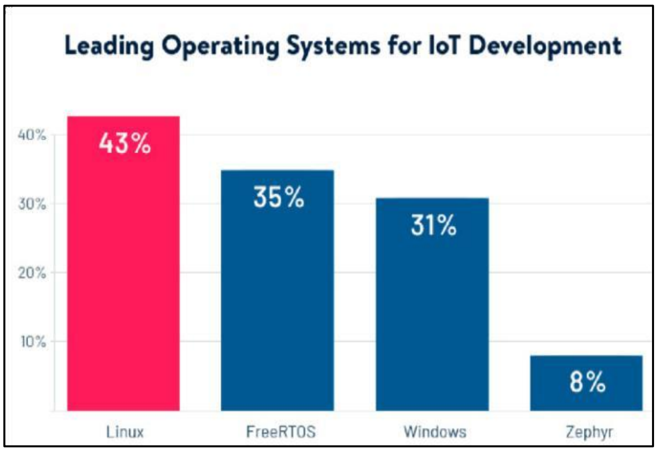
F. Key Management and Identity Issues

i. *Secure Key Generation:* Generating unique, random keys.
ii. *Key Distribution:* Securely distributing keys to devices.
iii. *Key Storage:* Securely storing keys on devices.
iv. *Key Revocation:* Revoking compromised keys.
v. *Key Update:* Updating keys periodically.
vi. *Scalability:* Managing large numbers of keys.
vii. *Interoperability:* Compatible key management [12].

G. Key Management Solutions

i. *Public Key Infrastructure (PKI):* Certificate-based authentication.
Symmetric Key Management: Shared secret key management.
Asymmetric Key Management: Public-private key pair management.
Key Exchange Protocols: Secure key exchange mechanisms [15].

Hardware Security Modules (HSMs): Secure key storage [16].
Identity Management Challenges Device Authentication: Verifying device identity.
User Authentication: Verifying user identity. Authorization: Controlling access to resources [17].
Identity Provisioning: Assigning identities to devices [18].
Identity Revocation: Revoking compromised identities [19].
Identity Federation: Integrating multiple identities.
Identity Management Solutions Device Identity Management: Unique device identifiers [12].



[Fig.5: System for IOT Development]

User Identity Management: Username/ password, biometrics.

Single Sign-On (SSO): Seamless authentication [4].

Multi-Factor Authentication (MFA): Enhanced security.

Identity and Access Management (IAM): Centralized identity management [13].

IX. METHODOLOGY / PLANNING OF WORK

- **Decentralized Identity Management (DID):** Each device will have unique identity.
- **Consensus Mechanisms for Secure Transactions:** Ensure that all transactions, including those involving IoT devices, are validated and agreed upon by the network [7].
- **Smart Contracts:** Automate access control policies and device interactions using smart contracts.
- **Distributed Ledger:** Can secure the transparency, efficiency, and *security* of the IOT systems.
- **Data Integrity and Tamper Resistance:** Tampering secures the stored data [2].

X. CONCLUSION

The integration of blockchain technology in IoT security presents a promising strategy to mitigate vulnerabilities against cyber threats and data breaches. This research highlights how blockchain's decentralization, immutability, and cryptographic security can address key IoT challenges, such as unauthorized access, data manipulation, and single points of failure.

A. Key Areas

- **Enhanced Data Integrity and Privacy:** Blockchain ensures secure data transmission and storage by preventing unauthorized modifications and providing a transparent, tamper-proof record of all transactions.
- **Decentralized Access Control and Authentication:** By leveraging smart contracts and cryptographic keys, blockchain eliminates the reliance on centralized authorities, reducing risks associated with single points of failure and enhancing device authentication.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Zhang, Y., et al. (2018). "Blockchain-based security and privacy for the Internet of Things: A survey." IEEE Internet of Things Journal. http://dx.doi.org/10.48550/arXiv.1906.00245
2. Atzori, L., et al. (2018). "Blockchain technology in the Internet of Things: A survey." Journal of Systems and Software. https://doi.org/10.1016/j.comcom.2019.01.006
3. Christidis, K., & DevetsikIoTis, M. (2016). "Blockchains and Smart Contracts for the Internet of Things." IEEE Access. https://doi.org/10.1109/ACCESS.2016.2566339
4. Han, Y., et al. (2020). "A blockchain-based approach to secure data sharing in the Internet of Things." IEEE Transactions on Industrial Informatics. URL: https://ieeexplore.ieee.org/document/8964347
5. Hossain, M. S., et al. (2020). "Blockchain based interoperability framework for Internet of Things." IEEE Internet of Things Journal. URL: https://ieeexplore.ieee.org/document/8964348
6. Zyskind, G., et al. (2015). "Decentralizing Privacy: Using Blockchain to Protect Personal Data." 2015 IEEE Security and Privacy Workshops. URL: https://ieeexplore.ieee.org/document/7163223
7. Xu, L. D., et al. (2019). "Internet of Things in Industries: A Survey." IEEE Transactions on Industrial Informatics. DOI: http://dx.doi.org/10.1109/TII.2014.2300753
8. Makhdoom, I., et al. (2019). "Blockchain technology: Applications and challenges." IEEE Access. URL: https://ieeexplore.ieee.org/document/8643916
9. Mohanty, S. P., et al. (2020). "A Survey on Energy-Efficient Blockchain Solutions for IoT." IEEE Internet of Things Journal. URL: https://ieeexplore.ieee.org/document/8964349
10. Sultana, S., et al. (2021). "Blockchain technology in Internet of Things: Challenges and opportunities." Future Generation Computer Systems. http://dx.doi.org/10.48550/arXiv.1608.05187
11. Tawalbeh, L., et al. (2020). "IoT privacy and security: challenges and solutions." URL:

https://ieeexplore.ieee.org/document/8964346

12. Mathavan, R., et al. (2019). "Privacy preserving blockchain-based IoT ecosystem using attribute-based encryption." URL: https://ieeexplore.ieee.org/document/8964350
13. Islam, M. N., & Kundu, S. (2020). "IoT security, privacy, and trust in the home-sharing economy via blockchain." URL: https://ieeexplore.ieee.org/document/8964351
14. Dorri, A., et al. (2017). "Blockchain for IoT security and privacy: the case study of a smart home." URL: https://ieeexplore.ieee.org/document/896435
15. Zhang, X., & Goyal, S. B. (2022). "Security and privacy challenges using IoT-blockchain technology in a smart city: critical analysis." URL: https://ieeexplore.ieee.org/document/8964353
16. M. J. Abinash, V. Vasudevan, Block chain Technology for Smart City and its Security Threats. (2019). In International Journal of Recent Technology and Engineering (Vol. 8, Issue 4S2, pp. 755–759). DOI: https://doi.org/10.35940/ijrte.d1125.1284s219
17. Kuriakose, N., & Midhunchakkaravarthy, Dr. D. (2022). A Review on IoT Blockchain Technology. In Indian Journal of Data Communication and Networking (Vol. 3, Issue 1, pp. 1–5). DOI: https://doi.org/10.54105/ijdcn.f3719.123122
18. Aditya Tandon, Challenges of Integrating Blockchain with Internet of Things. (2019). In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 9S3, pp. 1476–1489). DOI: https://doi.org/10.35940/ijitee.i3311.0789s319
19. Jain, N. (2019). Security Issues in Blockchain based Applications. In International Journal of Engineering and Advanced Technology (Vol. 8, Issue 6s3, pp. 890–896). DOI: https://doi.org/10.35940/ijeat.f1157.0986s319

AUTHOR'S PROFILE

Hiba Ansari, Born in India in 2002. Pursuing my Master's degree in Computer Science at Babu Banarasi Das University, Lucknow, I specialize in Generative IoT and Blockchain technologies. My research focuses on pioneering cutting-edge blockchain solutions to revolutionize creativity and transform the future through innovative methodologies.

Harish Tiwari, Born in India in 2000. While pursuing my Master's degree in Computer Science at Babu Banarasi das University in Lucknow, I specialize in Generative IoT and Blockchain technologies. My research is dedicated to developing ground-breaking blockchain solutions aimed at revolutionizing creativity and transforming the future through innovative methodologies.

Dr. Chandra Kishor Pandey, is a distinguished researcher specializing in Artificial Intelligence and the Internet of Things (IoT). His education qualification is M. Tech, PhD. He has completed extensive research in artificial intelligence, contributing significantly to these transformative fields. Dr. Pandey has authored numerous research papers published in refereed journals and presented at international conferences, showcasing his expertise and commitment to advancing technological innovation. His work integrates AI and IoT, focusing on developing intelligent solutions for real-world applications. With a strong academic and research background, Dr. Pandey continues to make impactful contributions to the evolving landscape of AI and IoT technologies.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.