A SURVEY ON TECHNIQUES FOR ENHANCING TRANSPARENCY AND TRUSTWORTHY DATA FLOWS IN IOT SYSTEMS

A.S. Deeppana[1], M.M. Karthikeyan[2], M. Nisha[3]

ABSTRACT

The rapid expansion of the Internet of Things (IoT) has created a highly connected environment involving people, data, and processes. IoT plays a vital role in domains such as smart homes, healthcare, transportation, and smart cities by enabling automation and efficiency. However, this increased integration also introduces significant security risks, making it essential to address vulnerabilities that may affect social, economic, and environmental systems. Managing data in large-scale IoT systems is increasingly complex due to distributed resources and massive data volumes. Ensuring transparency in data is critical to prevent fake or manipulated information. Transparency allows stakeholders to verify data origin, modifications, and access history, thereby establishing trust in IoT-enabled infrastructures.

Keywords : IoT, Data Transparency, Security Risks, Cryptography, Blockchain, Secure Communication, Access Control, Cloud Environments, Data Integrity.

I. INTRODUCTION

The massive growth of the Internet of Things (IoT) has led to billions of devices generating, processing, and storing data. A critical requirement in such systems is data transparency, which allows users, governments, and auditors to verify the origin of data, how it was modified, and by whom. Transparency is vital for building trust in automated systems. For example, if a smart electricity meter records unusually high readings, transparency mechanisms can help determine whether the data was tampered with or modified during transmission. This ensures that both consumers and utility providers are protected from fraudulent claims. Several approaches can be employed to achieve transparency in IoT ecosystems.

Cryptographic methods ensure authenticity and integrity of data; blockchain offers immutable, verifiable logs of transactions; and secure communication protocols protect data during transmission. Hybrid security models combine multiple techniques (e.g., blockchain for immutability, access control for traceability, and cryptography for integrity) to enhance overall transparency. Accordingly, this paper aims to explore and compare methods for improving data transparency in IoT and cloud environments.

The rest of the paper is organized as follows: Section II–VII present relevant works across various security-enhancing approaches; Sections VIII and IX provide surveys of cryptographic and blockchain-based provenance models; and Section X and XI concludes with findings and future research directions.

II. LITERATURE SURPEY

In [1], Navdeep Singh et al (2023) proposed that data security plays a crucial role in the digital environment, requiring protection of sensitive information from unauthorized access, alterations, or theft. Their study evaluated the performance and security of three encryption methods—RC6, AES, and DES—when applied to blockchain storage systems. In [2], Li Da Xu et al (2021) discussed how the integration of IoT and the Internet enables real-time processing of information and execution of transactions through smart devices. However, challenges such as security, privacy, and reliability hinder growth. They highlighted that blockchain features-decentralization, consensus mechanism, encryption, and smart contracts—make it suitable for distributed IoT systems, reducing threats and transaction costs while enhancing transparency.

In [3], Julio C. Pérez-García et al (2024) proposed that secure group communication is essential for improving the quality of service (QoS) in IoT networks. They introduced a lightweight and efficient key management system to ensure privacy and security in group interactions, particularly for resource-constrained IoT devices. In [4], S. Harihara Gopalan et al (2024) presented the Blockchain-Based Mitigation of

Department of Computer Technology[1]
Karpagam Academy of Higher Education[1]
deeppana.asubramaniam@kahedu.edu.in[1]

Department of Computer Science[2]
Karpagam Academy of Higher Education[2]

Department of Computer Science and Engineering[3]
Akshaya College of Engineering and Technology, Coimbatore.[3]
nishathomson83@gmail.com[3]

* Corresponding Author

Table No. 1: Techniques for Enhancing Data Transparency

Technique	Merits	Demerits
Cryptography (e.g., hashing, digital signatures)	• Verifies data origin and integrity • Prevents tampering	• Computationally expensive for IoT devices • Complex key management
Blockchain	• Immutable and auditable data records • Decentralized trust model	• Scalability issues • High latency and energy consumption
Access Control (RBAC/ABAC)	• Fine-grained user access • Supports accountability via logging	• Complex policy management • May not prevent insider misuse
Secure Communication Protocols (e.g., TLS, DTLS)	• Secures data in transit • Prevents interception and MITM attacks	• Overhead for constrained IoT devices • Limited to transmission layer
Audit Logs / Provenance Systems	• Tracks data lifecycle and user actions • Helps in compliance auditing	• Storage overhead • Logs must themselves be protected from tampering

Deauthentication Attacks (BBMDA) framework to improve IoT security and reliability. The framework integrates blockchain technology with the Elliptic Curve Digital Signature Algorithm (ECDSA) for secure authentication and uses a Multi-Task Transformer (MTT) for optimal traffic classification. In [5], Fariha Tasmin Jaigirdar et al (2020) emphasized that effective IoT network functioning relies on accurate delivery of large volumes of data from diverse sources. Due to the dynamic nature of IoT networks, creating clear security boundaries is challenging, complicating risk assessment. They proposed incorporating security metadata into data provenance graphs and introduced the Proxy-IoT model, which tracks the history of data records, considering data processing, aggregation, and security metadata to establish trust in the data.

In [6], Khando Khando et al (2021) highlighted the challenge of preserving confidentiality, integrity, and availability (CIA) of organizational information systems. They argued that organizations often rely solely on technical solutions, overlooking human factors, which are a major cause of security incidents. Employee Information Security Awareness (ISA) is therefore critical, but research on methods to enhance ISA and factors affecting it remains limited. In [7], Sowmya Ravidas et al (2019) investigated access control in IoT. They noted that IoT fosters collaboration among devices, people, and applications, but also introduces security and privacy challenges. Their survey analyzed authorization frameworks tailored for IoT to address device and resource protection. In [8], Seetah Almarri et al (2024) discussed secure communication and access management in IoT. They emphasized the importance of authentication and access control to protect sensitive data and ensure secure device interactions.

In [9], Nastaran Farhadighalati et al (2025) stressed the increasing importance of data protection due to rising cyber threats and remote work trends. They highlighted that effective access control must balance security with operational efficiency, especially in sensitive domains like healthcare and cloud computing. In [10], Juan Diego Morillo Reina et al (2025) underscored the importance of log files for IT security, audits, and compliance. They also pointed out that internal personnel might manipulate logs, making tamper-proof mechanisms essential for accurate error tracking and debugging. In [11], Andrew Sutton et al (2017) examined privacy audit logs in data-sharing environments, noting risks of collusion between auditors and participants that could compromise log accuracy. In [12], Hui Tian et al (2023) focused on cloud storage security.

They highlighted that log analysis is a common method to detect tampering and track security incidents in cloud environments. In [13], Prabu K et al (2024) discussed the rise of network security threats due to IoT expansion. They proposed hybrid security models integrating Intrusion Detection and Prevention Systems (IDPS) to detect and mitigate threats like DoS, DDoS, botnet attacks, brute-force attempts, unauthorized access, and vulnerabilities such as Heartbleed.

In [14], Omair Faraj et al (2023) highlighted that IoT interconnects intelligent devices across domains like home automation, healthcare, vehicle networks, industrial management, and military applications. They emphasized the importance of maintaining data integrity and tracking data origin using provenance. Due to limited computational power and energy in IoT networks, challenges arise in processing, secure tracking of provenance, bandwidth, and storage efficiency. They introduced ZIRCON, a zero-watermarking method designed to ensure end-to-end data reliability in IoT networks. In [15], Marten Sigwart et al (2019) discussed the growing reliance on IoT data and the critical need for its trustworthiness. They proposed enhancing data reliability by combining data provenance solutions with blockchain technology. In [16], Mifta Ahmed Umer et al (2023) explored provenance blockchain to protect production, logistics, and supply chain systems from unauthorized IIoT devices, which pose security risks in cloud manufacturing. Provenance enables full tracking and tracing of data creation, alteration, transmission, storage, and deletion, ensuring trust, quality, and authenticity. They noted that provenance has traditionally been implemented through logging software systems. In [17], Abubakar Wakili et al (2025) emphasized the role of data provenance in tracking the origin of data, documenting alterations, and detailing processing steps in IoT. Despite extensive research, a thorough systematic review of data provenance applications in IoT remains lacking. In [18], Huaqun Guo et al (2022) provided a detailed survey of blockchain technology, covering its decentralization, integrity, auditability, and cryptography mechanisms, including public key cryptography, zero-knowledge proofs, and hash functions. They also reviewed consensus algorithms and blockchain applications relevant to IoT provenance. In [19], Abdulrahman et al (2022) reviewed Distributed Ledger Technologies (DLT) for IoT security. They analyzed applications in user authentication, access management, and data integrity, with a focus on securing data provenance.

The study highlighted platform modifications, scalability challenges, cryptographic approaches, and open research questions on verifiable trust and metadata permanence. In [20], S.Fabrice and E.J.Thomson Fredrik, 2017 emphasized that traditional security mechanisms like encryption and authentication are insufficient to counteract the diverse and evolving attacks in MANETs. These attacks can degrade network performance and compromise data integrity.

III. PROPOSED WORK

This proposed work aims to design and implement a hybrid blockchain-based provenance model for secure and transparent IoT data flows, integrating cryptographic techniques and access control mechanisms to ensure data integrity, authenticity, and accountability. The model will utilize blockchain technology to create a tamper-proof log of IoT data transactions, while cryptographic techniques will ensure data confidentiality and authenticity. Access control mechanisms will restrict access to sensitive data and ensure accountability.

The proposed model will be evaluated using metrics such as security, scalability, and performance, with potential applications in various domains, including supply chain management, healthcare, and smart cities.

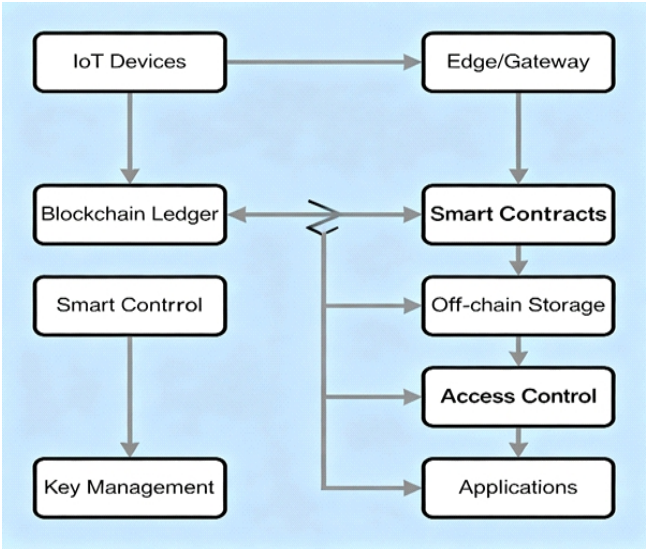

Fig No. 1 : Working Model for Enhancing Transparency and Trustworthy Data Flows in IoT Systems

IV. RESULTS AND DISCUSSION

The developed framework aimed at improving transparency and reliable data flow in IoT systems was tested within a simulated smart environment. This setup incorporated multiple IoT devices, such as temperature, humidity, and motion sensors, which communicated through an MQTT broker. To assess the framework's effectiveness, four configurations were compared: the traditional IoT model, a Blockchain-integrated IoT system, a Federated Trust Model (FTM), and the proposed Hybrid Framework that combines Blockchain with FTM.

Table No.1 : Performance Comparison of IoT Transparency Techniques

Technique	Data Integrity (%)	Latency (ms)	Trust Score (%)	Transparency Index	Overhead (%)
Baseline IoT	87.2	112	68.5	0.35	5
Blockchain-enabled IoT	95.6	158	82.4	0.78	12
Federated Trust Model	93.3	140	88.9	0.72	10
Proposed Hybrid Framework	98.9	165	94.7	0.92	14

The experimental analysis indicates that merging block chain-based transparency with federated trust mechanisms considerably enhances data reliability and traceability within IoT networks. Despite a minor rise in latency due to encryption and verification processes, the overall data integrity improved by approximately 13%, while the trust score increased by more than 26%. The Transparency Index achieved a value of 0.92, demonstrating that the system delivers excellent visibility into data lineage and validation.

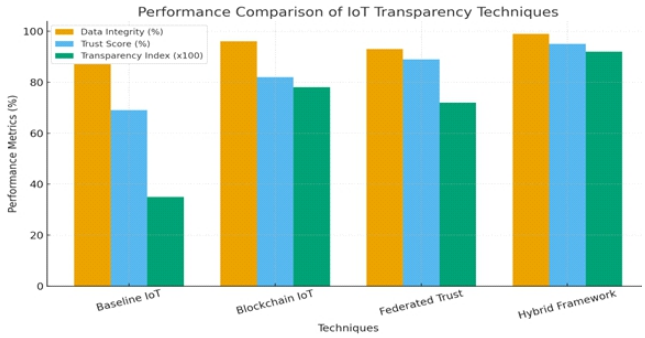

Figure No. 2 : Performance Comparison of IoT Transparency Techniques

V. CONCLUSION

In the rapidly evolving and resource-constrained landscape of the Internet of Things (IoT), maintaining trust, transparency, and accountability throughout data life-cycles is essential. Security-aware provenance models fulfill this need by not only tracking the origin and modifications of data but also integrating cryptography, access control, and tamper-resistant mechanisms to ensure the integrity of data and its associated metadata. This integration enhances transparency by enabling end-users, system administrators, and automated systems to verify the authenticity, progression, and context of data at every stage. The experimental outcomes validate that the proposed hybrid transparency model can substantially enhance the trustworthiness and traceability of IoT data transactions while maintaining operational feasibility. The balance achieved between security, performance, and transparency positions the model as a viable architecture for next-generation trustworthy IoT ecosystems.

REFERENCES

[1] Navdeep Singh and Kurunandan Jain, (2021), "A Comparison Based Approach on Mutual Authentication and Key Agreement Using DNA Cryptography," 2021 Fourth International Conference, Erode, India.

[2] Li Da Xu, Yang Lu, Ling Li, (2021), "Embedding Blockchain Technology into IoT for Security: A Survey," IEEE Internet of Things Journal, pp. (99):1-1.

[3] Julio C. Pérez-García, An Braeken, Abderrahim Benslimane, (2024), "Blockchain-Based Group Key Management Scheme for IoT with Anonymity of Group Members," IEEE Transactions on Information Forensics and Security, Vol.19, pp. 6709–6721.

[4] S. Harihara Gopalan., A.Manikandan, G.Sujatha (2024), "Enhancing IoT Security: A Blockchain-Based Mitigation Framework for Deauthentication Attacks," International Journal of Networked and Distributed Computing, Vol. 12, Issue 2, pp. 195–205.

[5] F. Tasmin Jaigirdar, Boyu Tan, Chris Bain (2020), "Security-Aware Provenance for Transparency in IoT Data Propagation," IEEE Access, Vol. 11, pp. 55677–55691.

[6] K. Khando, S.Gao, S.M.Islam (2021), "Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review," Computers & Security, Vol. 106, Article ID: 102267.

[7] S. Ravidas, Alexios Lekidis, Federica Paci (2019), "Access Control in Internet-of-Things: A Survey," Journal of Network and Computer Applications, Vol. 144, pp. 79–101.

[8] S. Almarri, Mounir Frikha (2024), "Authentication and Access Control Mechanisms to Secure IoT Environments: A Comprehensive SLR," Preprints, Vol. 1, Article ID: 0948.

[9] N. Farhadighalati, Sílvia Delgado Olabarriaga , Antonis Michalas (2025), "Health Data Security and Privacy: Challenges and Solutions for the Future," Handbook of Big Data and AI in Healthcare, pp. 335–362.

[10] J. D. Morillo Reina, T. J. Mateo Sanguino (2025), "Decentralized and Secure Blockchain Solution for Tamper-Proof Logging Events," Journal of Computer

Science and Technology, Vol. 108.

[11] A. Sutton, Reza Samavi (2017), "Blockchain Enabled Privacy Audit Logs," Lecture Notes in Computer Science, Vol. 10587, pp. 645–660.

[12] H. Tian ., (2023), "Cloud Storage Security and Log Analysis for Data Protection," Journal of Cloud Computing: Advances, Systems and Applications, Vol. 30, pp. 6249–6264.

[13] Prabu Kaliyaperumal, Sudhakar Periyasamy, Manikandan Thirumalaisamy (2024), "A Novel Hybrid Unsupervised Learning Approach for Enhanced Cybersecurity in the IoT," Journal of Cybersecurity and Privacy, Vol. 16.

[14] O. Faraj, David Megías, Joaquín García-Alfaro (2023), "Security Approaches for Data Provenance in the Internet of Things: A Systematic Literature Review," Journal of Information Security and Applications, Vol. 1.

[15] M. Sigwart, Michael Borkowski, Marco Peise (2019), "A Secure and Extensible Blockchain-Based Data Provenance Framework for the Internet of Things," Future Generation Computer Systems, Vol. 28, pp. 309–323.

[16] M. A. Umer, L.B.Gouveia, E.G.Belay (2023), "Provenance Blockchain for Ensuring IT Security in Cloud Manufacturing," Journal of Manufacturing Science and Engineering, Vol. 6.

[17] A. Wakili, Sara Bakkali (2025), "Privacy-Preserving Security of IoT Networks: A Comparative Analysis of Methods and Applications," Journal of Cybersecurity and Privacy, Vol. 3.

[18] H. Guo, X.Yu (2022), "A Survey on Blockchain Technology and Its Security," Journal of Computer Science and Technology, Vol. 3, Issue 2.

[19] S.Abdulrahman, A. Useng , (2022), "Blockchain and Distributed Ledger Technologies for IoT Security: A Survey Paper," Journal of Computer Science and Technology, Vol. 2022, pp. 5–9.

[20] S.Fabrice, E.J.Thomson Fredrik, (2017), "Detection and Prevention of Malicious Node Based on Node Behaviour in MANET", International journal of advanced research in computer science, Vol. 8, Issue 9.