Monitoring Data Sharing and Data breaches on the Internet of Things using Block chain

Jetti Aasha[1], Mrs.K.Nirusha[2], Mr.M.Venkateswara Rao[3], Mr.M.JayaKumar Raju[4]

[1]PG student ,Department Of Computer Science & Engineering, Mother Teresa Institute Of Science And Technology Autonomous, Sanketika Nagar, Kothuru (V), Sathupally - 507303, Khammam Dist., Telangana,India

[2,3,4]Assistant Professor , Department Of Computer Science & Engineering, Mother Teresa Institute Of Science And Technology Autonomous, Sanketika Nagar, Kothuru (V), Sathupally - 507303, Khammam Dist., Telangana,India

***Abstract*—**The Internet of Things (IoT) is one of the fastest-growing technologies in the modern world. IoT connects physical devices such as sensors, smart appliances, wearable devices, vehicles, industrial machines, and healthcare equipment through the internet. These devices continuously collect, process, and exchange large amounts of data in real time. IoT technology is widely used in smart homes, healthcare, agriculture, transportation, manufacturing industries, and smart cities because it improves automation, efficiency, and decision-making processes. However, the rapid growth of IoT systems has also increased security risks related to data sharing and data breaches. Since IoT devices exchange sensitive information over networks, attackers can exploit vulnerabilities to gain unauthorized access, steal data, manipulate communications, or disrupt services. Traditional centralized security systems are often unable to provide strong protection because IoT networks are distributed, heterogeneous, and resource-constrained environments.

The proposed blockchain-based monitoring framework improves confidentiality, authentication, traceability, transparency, and privacy protection. Unlike traditional centralized machine learning systems, blockchain eliminates single points of failure and reduces risks associated with data manipulation. The framework also enables transparent auditing of all IoT transactions, making it easier to trace malicious activities and identify the source of breaches. This project contributes to the development of secure and scalable IoT environments capable of resisting modern cyber threats.

I. INTRODUCTION

The Internet of Things has transformed the digital world by enabling billions of devices to communicate and exchange information through the internet. IoT devices include smart sensors, wearable gadgets, industrial machines, home automation systems,

Doi:10.48047/ijiee.2026.16.2.53

environmental monitoring devices, and connected vehicles. These devices continuously generate large amounts of data that help organizations improve automation, operational efficiency, and intelligent decision-making. IoT technology is now widely used in healthcare systems, agriculture, smart cities, transportation, industrial automation, military operations, and environmental monitoring.

Despite the benefits of IoT systems, security and privacy remain major challenges. IoT devices are usually connected through wireless networks and often operate with limited computational power and memory. Many devices lack strong security mechanisms, making them vulnerable to cyberattacks such as malware injection, phishing, spoofing, distributed denial-of-service attacks, and unauthorized access. Since IoT systems exchange sensitive information continuously, attackers target these systems to steal confidential data or disrupt operations.

II. LITERATURE SURVEY

1. Towards Blockchain-Based Auditable Storage and Sharing of IoT Data

Authors: Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, Simon Duquennoy

- **Technique Used:** Blockchain-based auditable storage, decentralized access control, and secure IoT data sharing.
- **Pros:**
  - Ensures secure and transparent data sharing.
  - Provides data ownership and auditability.
  - Prevents unauthorized data access.
- **Cons:**
  - Increased storage overhead.
  - Scalability challenges for large IoT networks.

2. Blockchain Based Proxy Re-Encryption Scheme for Secure IoT Data Sharing

Authors: Ahsan Manzoor, Madhsanka Liyanage, An Braeken, Salil S. Kanhere, Mika Ylianttila

- **Technique Used:** Blockchain, smart contracts, and proxy re-encryption for secure IoT data exchange.
- **Pros:**
  - Secure data sharing without trusted third parties.
  - Fine-grained access control.
  - Improved privacy protection.
- **Cons:**
  - Smart contract execution costs.
  - Cryptographic processing overhead.

3. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in IoT: A Systematic Literature Review

Authors: Haider Dhia Zubaydi, Pál Varga, Sándor Molnár

Doi:10.48047/ijiee.2026.16.2.53

- **Technique Used:** Blockchain-based privacy preservation, authentication, and data integrity mechanisms.
- **Pros:**
  - Enhances confidentiality and integrity.
  - Eliminates single points of failure.
  - Improves trust among IoT devices.
- **Cons:**
  - High energy consumption.
  - Blockchain scalability limitations.

4. Blockchain-Enabled Access Control to Prevent Cyber Attacks in IoT

Authors: R.S. Rinki Singh, D.K. Deepika Kukreja, D.K. Deepak Kumar Sharma

- **Technique Used:** Blockchain-based access control framework for IoT networks.
- **Pros:**
  - Prevents unauthorized access.
  - Improves accountability and traceability.
  - Enhances IoT network security.
- **Cons:**
  - Complex implementation.
  - Latency in transaction verification.

5. Blockchain-Based Intrusion Detection/Prevention Systems in IoT Network: A Systematic Review

Authors: Various Researchers

- **Technique Used:** Blockchain-integrated Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
- **Pros:**
  - Detects malicious activities in real time.
  - Protects against data breaches and cyberattacks.
  - Improves network resilience.
- **Cons:**
  - Increased computational requirements.
  - Complex IDS deployment.

III. EXISTING SYSTEM

The existing system for monitoring data sharing and detecting data breaches in Internet of Things environments mainly depends on centralized architectures and machine learning techniques. In traditional IoT security systems, all data generated by sensors, smart devices, and connected equipment is transmitted to centralized cloud servers where monitoring and analysis operations are performed. Machine learning algorithms are used to analyze communication patterns, detect anomalies, and identify malicious activities within the network. These systems use algorithms such as Decision Trees, Random Forest, Support Vector Machine, Naive Bayes, and Neural Networks for intrusion detection and threat classification.

In the existing approach, IoT devices continuously collect information and send it to cloud servers through gateways. The centralized server stores and processes all

Doi:10.48047/ijiee.2026.16.2.53

incoming data. Security monitoring tools analyze traffic patterns, login activities, device behaviors, and communication frequencies to identify abnormal activities. If suspicious behavior is detected, alerts are generated to notify administrators about possible cyberattacks or unauthorized access attempts.

Disadvantages

One of the major disadvantages of the existing system is the dependence on centralized architecture. Since all IoT data is stored and processed in centralized cloud servers, attackers can target these servers to steal sensitive information or disrupt operations. If the central server fails due to cyberattacks, hardware failures, or software errors, the entire IoT network may become unavailable.

Another significant disadvantage is poor data privacy and security. Traditional systems store confidential information such as healthcare records, industrial data, and personal user details in centralized databases. Unauthorized access to these databases can lead to data breaches, privacy violations, identity theft, and financial losses. Attackers may exploit vulnerabilities in cloud platforms to gain access to sensitive information.

IV. PROPOSED SYSTEM

The proposed system introduces a blockchain-based framework for monitoring secure data sharing and detecting data breaches in Internet of Things environments. Unlike traditional centralized systems, the proposed framework uses decentralized blockchain architecture to improve transparency, security, trust management, and data integrity.

In the proposed system, every IoT device is registered within the blockchain network and assigned a unique cryptographic identity. This identity is used for secure authentication and communication between devices. Before sharing any information, the system verifies the identity of devices using blockchain authentication mechanisms. Unauthorized devices are automatically denied access.

Whenever a device shares data, the transaction is verified using blockchain consensus algorithms such as Proof of Stake, Proof of Authority, or Practical Byzantine Fault Tolerance. After verification, the transaction is stored in immutable blockchain blocks containing timestamps, cryptographic hashes, and device identities. Since blockchain records cannot easily be modified or deleted, the system ensures strong protection against data tampering.

Advantages

The proposed blockchain-based monitoring system provides several advantages compared to traditional IoT security frameworks. One of the most important advantages is enhanced security. Blockchain technology uses cryptographic hashing, decentralized consensus mechanisms, and immutable ledgers to protect transaction records from unauthorized modification. This ensures data integrity and prevents

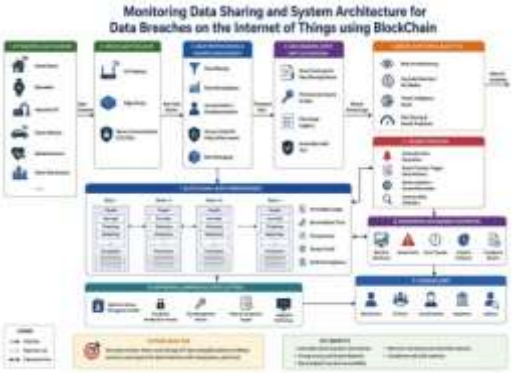
Doi:10.48047/ijiee.2026.16.2.53

attackers from manipulating stored information.

Another major advantage is decentralization. Unlike centralized cloud-based systems, the proposed framework distributes transaction records across multiple blockchain nodes. This eliminates single points of failure and reduces the risk of large-scale cyberattacks targeting central servers.

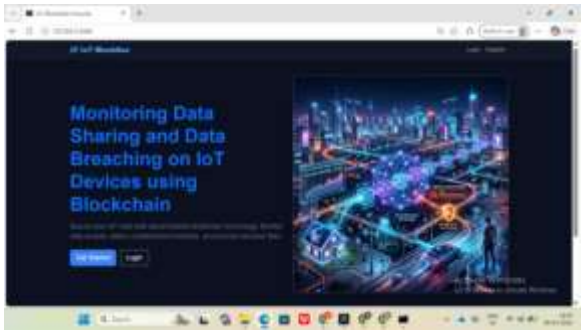
The proposed system also improves transparency and accountability. Every data-sharing transaction performed within the IoT network is permanently recorded in blockchain ledgers. Administrators can trace all communication activities and identify the source of suspicious behavior. This transparency improves trust among users and organizations.

V. SYSTEM ARCHITECTURE

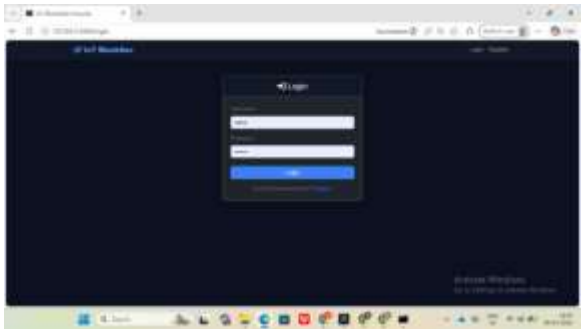


This architecture is suitable for multiple real-world applications including smart healthcare, industrial automation, smart homes, transportation systems, military communication, agriculture monitoring, and intelligent city infrastructures. In healthcare systems, blockchain-based IoT architectures protect patient records from unauthorized access. In smart industries, the system prevents manipulation of sensor data and secures machine communication. Therefore, the proposed architecture provides a scalable, reliable, and efficient solution for monitoring data sharing and preventing data breaches in IoT environments

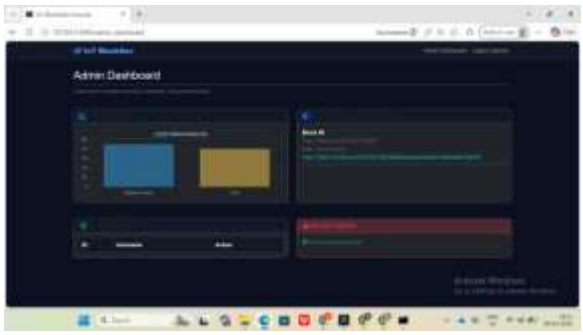
VI. RESULTS AND OUTCOMES



Screen 1: Home page



Screen 2: Login Page



Screen 3: Prediction Page

Doi:10.48047/ijiee.2026.16.2.53

VII. CONCLUSION

The project titled "Monitoring Data Sharing and Data Breaches in Internet of Things Using Blockchain" presents an advanced and secure framework for protecting sensitive information exchanged among IoT devices. In recent years, the rapid growth of the Internet of Things has connected billions of smart devices in healthcare, agriculture, transportation, smart homes, industrial automation, and many other domains. Although IoT technology improves communication and automation, it also introduces serious security challenges such as unauthorized access, data leakage, hacking, malware attacks, identity theft, and privacy violations. Traditional centralized security systems are often unable to handle the dynamic and distributed nature of IoT environments because they depend heavily on a single server or authority. If the centralized server is attacked, the entire network becomes vulnerable. To overcome these limitations, the proposed blockchain-based monitoring system offers a decentralized, transparent, secure, and tamper-resistant approach for managing IoT data sharing and breach detection.

VIII. BIBLIOGRAPHY

[1] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[2] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[4] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 2016, pp. 1–6.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[6] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[7] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*. Cham, Switzerland: Springer, 2019.

[8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.

[9] Y. Yuan and F. Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

Doi:10.48047/ijiee.2026.16.2.53

[10] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

Doi:10.48047/ijiee.2026.16.2.53