JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IOT Based Secure Data Sharing System

Prof. Nisha G.Rabde 1) Vijay Pravin Navsare 2) Abhishek Pravin Raje 3) Yash Sanjay Sonawane 4) Shubham Ashok Bhoi.
Computer Science Engineering Department, Padm. Dr. VBKCOE, Malkapur, Maharashtra, India.

ABSTRACT - *The advent of the Internet of Things (IoT) has ushered in a new era of interconnected devices and data-driven applications. This review paper delves into the realm of secure data sharing systems within the IoT landscape, exploring the challenges, solutions, and implications of sharing sensitive information in a connected environment. The study investigates the current state of IoT-based data sharing, aiming to provide a comprehensive understanding of the security measures, protocols, and frameworks employed to safeguard shared data.*

The research emphasizes the significance of secure data sharing in fostering collaboration and maximizing the potential benefits of IoT-enabled ecosystems. By analyzing existing literature, standards, and practices in the field, the paper aims to identify common trends, highlight areas of improvement, and propose recommendations for enhancing the security of IoTbased data sharing systems. The abstract concludes by underlining the importance of continuous research and development in this dynamic field to address emerging challenges and ensure the sustained growth of secure data sharing practices in the IoT era.

Keywords *- Internet of Things (IoT), Data Sharing, Security, Connected Devices, IoT Protocols.*

INTRODUCTION -

The proliferation of Internet of Things (IoT) devices has revolutionized the way we interact with our surroundings, embedding intelligence into everyday objects and enabling seamless communication between devices. As the IoT ecosystem expands, the volume of data generated by interconnected devices grows exponentially, presenting both opportunities and challenges. This paper introduces a comprehensive exploration of IoT-based secure data sharing systems, focusing on the crucial intersection between data sharing and security within the context of the IoT paradigm.

In recent years, IoT technology has become omnipresent, touching various aspects of our lives, from smart homes and healthcare to industrial processes and smart cities. The ability of devices to collect, exchange, and utilize data in real-time has paved the way for innovative applications and services. However, the sharing of sensitive information across interconnected devices raises concerns about privacy, confidentiality, and security. This study aims to dissect the intricate relationship between data sharing and security in the IoT landscape, shedding light on the existing challenges and proposing strategies to fortify the integrity and confidentiality of shared data.

The research delves into the fundamental motivations behind the need for secure data sharing in IoT environments. With an emphasis on fostering collaboration and enabling data-driven decisionmaking, the paper explores how secure data sharing can unlock the full potential of IoT applications. By understanding the complexities and nuances of data sharing mechanisms, the study sets the stage for a detailed investigation into the methodologies and frameworks employed to ensure the security and privacy of shared data in the dynamic and interconnected world of IoT.

The subsequent sections will delve into existing literature, analyze security protocols and frameworks, and propose recommendations for enhancing the security posture of IoT-based data sharing systems. Through this exploration, the paper seeks to contribute valuable insights to the ongoing discourse on securing the vast network of interconnected devices in the IoT era.

PROBLEM FORMULATION -

Despite the transformative potential of IoT-based data sharing systems, several challenges and concerns hinder their widespread adoption. One of the primary issues is the vulnerability of shared data to security threats, including unauthorized access, data breaches, and malicious attacks. As IoT devices often operate in resource-constrained environments, implementing robust security measures becomes a complex task. This paper addresses the core problem formulation by scrutinizing the existing vulnerabilities and threats associated with data sharing in IoT ecosystems, aiming to identify key challenges that impede the establishment of secure and trustworthy data sharing frameworks.

One significant challenge revolves around the heterogeneity of IoT devices, which encompass a diverse range of technologies, communication protocols, and security standards. Integrating these disparate elements into a cohesive and secure data sharing environment demands a nuanced approach. Additionally, the sheer volume of data generated by IoT devices introduces concerns related to data integrity, confidentiality, and secure transmission. The research formulates the problem by dissecting these multifaceted challenges and recognizing the need for tailored solutions that accommodate the intricacies of the IoT landscape.

Furthermore, the paper investigates the implications of privacy concerns and regulatory compliance in the context of IoT-based data sharing. As the data shared between devices often contains sensitive and personal information, ensuring compliance with data protection regulations becomes imperative. The problem formulation encompasses an in-depth analysis of the privacy challenges associated with data sharing in the IoT domain and seeks to propose strategies that reconcile the benefits of data-driven insights with the imperative to safeguard user privacy.

PROPOSE SYSTEM METHODOLOGY -

To address the identified challenges in the IoT-based data sharing ecosystem, this paper proposes a comprehensive methodology that amalgamates advanced security measures, device heterogeneity management, and privacy-preserving techniques. The methodology unfolds in several key stages, ensuring a systematic and effective approach to enhancing the overall security and reliability of data sharing in IoT environments.

1. Security Enhancement through Blockchain:

The proposed system advocates for the integration of blockchain technology to fortify the security aspects of IoT-based data sharing. Blockchain's decentralized and immutable ledger ensures data integrity and traceability. Each data transaction is recorded in a tamper-resistant manner, reducing the risk of unauthorized access or malicious alterations. Smart contracts within the blockchain can be employed to enforce predefined security policies, enabling automated and trustless interactions between IoT devices.

2. Device Heterogeneity Management:

Given the diverse nature of IoT devices, a middleware layer is introduced to manage the heterogeneity challenge. This layer acts as an abstraction, providing a standardized interface for communication and data exchange. By implementing protocols such as the Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT), the proposed methodology streamlines interoperability among varied devices. Moreover, the middleware layer facilitates secure communication channels, ensuring that data is exchanged seamlessly while adhering to standardized security protocols.

3. Privacy-Preserving Data Sharing:

To tackle privacy concerns, the proposed system incorporates techniques for privacy-preserving data sharing. Differential privacy mechanisms are employed to anonymize and aggregate data, mitigating the risk of individual device identification. Additionally, encryption methods, such as homomorphic encryption, enable secure computations on encrypted data, ensuring that sensitive information remains confidential even during data processing.

4. Dynamic Policy Enforcement and Compliance:

The methodology introduces a dynamic policy enforcement mechanism that adapts to evolving security and privacy requirements. Device-centric policies are established, governing the access, sharing, and processing of data. Compliance with data protection regulations, such as GDPR, is embedded within the system's architecture, ensuring that data practices align with legal frameworks.

5. Continuous Monitoring and Adaptation:

A real-time monitoring system is integrated into the proposed methodology, continuously assessing the security posture of the IoT-based data sharing environment. Anomaly detection algorithms and intrusion prevention measures are employed to identify and respond to potential security threats promptly. The system adapts its security measures based on emerging threats and evolving device landscapes.

In essence, the proposed methodology provides a holistic approach to fortifying IoT-based data sharing systems, addressing security, heterogeneity, privacy, and compliance challenges. By leveraging blockchain, middleware, privacy-preserving techniques, and dynamic policy enforcement, the system aims to establish a resilient and trustworthy foundation for data sharing in the complex IoT ecosystem.

WORKING ON LANGUAGES -

The implementation of the proposed IoT-based secure data sharing system involves strategic choices in programming languages and development tools to ensure efficiency, scalability, and compatibility with diverse IoT devices. The chosen technology stack revolves around Java as the primary coding language, Apache IDE and Netbeans 16 as development tools, and MySQL as the database management system.

1. Coding Language - Java:

Java is selected as the core programming language due to its platform independence, object-oriented nature, and extensive libraries. Java provides a robust and secure environment for developing IoT applications, making it well-suited for handling the intricacies of data sharing in diverse device ecosystems. Its portability allows the system to run seamlessly across various IoT devices, ensuring broad compatibility.

2. Development Tools - Apache IDE, Netbeans 16:

The development process is facilitated by Apache IDE and Netbeans 16, both of which offer comprehensive Integrated Development Environments (IDEs) for Java applications. Apache IDE, equipped with features like code assistance, debugging tools, and a user-friendly interface, streamlines the development workflow. Netbeans 16 provides additional support for Java development, enhancing collaboration and code organization.

3. Database Management - MySQL:

MySQL is chosen as the relational database management system (RDBMS) to store and manage the IoT-generated data securely. With its proven reliability, performance, and open-source nature, MySQL is wellsuited for handling the structured data inherent in an IoT environment. The use of MySQL ensures efficient data retrieval, storage, and management within the proposed system.

By leveraging these technologies, the working languages and tools create a robust development environment for implementing the IoT-based secure data sharing system. The combination of Java, Apache IDE, Netbeans 16, and MySQL aligns with the system's requirements, fostering efficient coding practices, seamless development, and reliable data management within the IoT ecosystem.

RELATED WORKING -

To understand the context and challenges in the domain of IoT-based secure data sharing systems, it is essential to review related works that have explored similar themes. Although the specific details of related works may vary, they contribute to the collective knowledge and advancements in the field. Several key studies and projects have paved the way for the proposed system.

Secure Data Sharing in IoT Environments:
Numerous research endeavors have focused on the secure sharing of data within IoT environments. Studies such as [Reference 1] have delved into encryption techniques, access control mechanisms, and authentication protocols to enhance data security in IoT ecosystems. These works provide insights into the complexities of securing data in interconnected environments, forming the foundation for secure datasharing frameworks.

Authorization Frameworks for IoT Applications:
Building on the concept of secure data sharing, authorization frameworks tailored for IoT applications have been explored. Research efforts, like [Reference 2], propose innovative authorization models that consider the unique challenges posed by diverse IoT devices. Understanding the nuances of authorization in an IoT context is crucial for developing a robust and scalable system.

Integration of Relational Databases in IoT: Addressing the storage and retrieval aspects of IoTgenerated data, studies such as [Reference 3] have investigated the integration of relational databases. This integration ensures efficient data management and retrieval, crucial for maintaining the integrity and accessibility of shared data. Insights from these studies contribute to the proposed system's approach to database management.

Security Challenges in IoT:
Comprehensive examinations of security challenges in IoT ecosystems, like [Reference 4], shed light on vulnerabilities and potential threats. Understanding these challenges is vital for designing a secure datasharing system. Insights from such works guide the incorporation of robust security measures in the proposed methodology.

Cross-Domain Data Sharing in IoT: As IoT applications span multiple domains, enabling seamless cross-domain data sharing has been a focus of research [Reference 5]. Exploring approaches to facilitate secure sharing across diverse domains is relevant to the proposed system, which aims to provide a comprehensive solution for secure data exchange.

By examining these related works, the proposed IoTbased secure data sharing system gains a nuanced understanding of the existing landscape. Insights from these studies contribute to the formulation of an effective and innovative methodology that addresses the unique challenges of secure data sharing in IoT environments.

REFERENCES -

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347– 2376, Oct./Dec. 2015.

[2] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127–144.

[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47–53. [4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506–522.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, vol. 4. Citeseer, Feb. 2004, pp. 5–6.

[6] D. Balfanz et al., “Secret handshakes from pairingbased key agreements,” in Proc. IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.

[7] R. Canetti, S. Halevi, and J. Katz, “Chosenciphertext security from identity-based encryption,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004, pp. 207–222.

[8] T. Koponen et al., "A data-oriented (and beyond) network architecture," in Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun., Aug. 2007, pp. 181–192.

[9] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, "Developing information networking further: From PSIRP to pursuit," in Proc. Int. Conf. Broadband Commun., Netw. Syst., Springer, Oct. 2010, pp. 1–13.

[10] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops,2010, pp. 1–6.

[11] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme for content-based networking," in Proc. IEEE INFOCOM 2004, vol. 2, 2004, pp. 918–928.

[12] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for informationcentric networks," in Proc. 2nd ed. ICN Workshop Inform.- Centric Netw., Aug. 2012, pp. 55–60.

[13] Y. Sun et al., "Trace-driven analysis of ICN caching algorithms on videoon-demand workloads," in Proc. 10th ACM Int. Conf. Emerging Netw. Exp. Technol., Dec. 2014, pp. 363–376.

[14] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, 2008. Available: https://bitcoin. org/bitcoin. pdf

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[16] N. Park, "Secure data access control scheme using type-based reencryption in cloud environment," in Semantic Methods Knowledge Management and Communications. Berlin, Germany: Springer, 2011, pp. 319– 327.