RADemics

Ensuring Data Integrity in IoT Leveraging Blockchain for Immutable Data Transactions and Provenance

Dr Shrikant Dnyandeo Bhopale, N.Mookhambika
ANNASAHEB DANGE COLLEGE OF ENGINEERING AND TECHNOLOGY, HINDUSTHAN INSTITUTE OF TECHNOLOGY

Ensuring Data Integrity in IoT Leveraging Blockchain for Immutable Data Transactions and Provenance

Dr Shrikant Dnyandeo Bhopale, Associate professor, Annasaheb Dange College of Engineering and Technology, Ashta, shrikantbhopale123@gmail.com

N.Mookhambika, Assistant Professor, Department of Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore, Tamalinadu, mookhambika@hit.edu.in

Abstract

The rapid proliferation of Internet of Things (IoT) devices has revolutionized various sectors, from healthcare to smart cities, offering unprecedented opportunities for data-driven innovation. The vast scale and heterogeneity of IoT networks have introduced significant challenges in ensuring data integrity and privacy. This chapter explores the integration of blockchain technology and cryptographic techniques for enhancing the security and immutability of IoT data transactions. By leveraging decentralized models, the chapter outlines how blockchain can provide robust solutions for data authentication, privacy preservation, and provenance tracking. Special emphasis was placed on the design of cryptographic protocols that ensure secure and immutable data flows between IoT devices, highlighting the role of smart contracts in automating secure data exchanges. The chapter examines the vulnerabilities in IoT data transmission and presents security measures to protect against data tampering and unauthorized access. The discussion also extends to the limitations of traditional authentication protocols and the potential of decentralized identity management in mitigating these risks. Overall, this chapter provides a comprehensive framework for addressing the emerging challenges in IoT security, offering insights into the future of secure, privacy-preserving IoT ecosystems.

Keywords:

Internet of Things, blockchain, cryptography, data integrity, smart contracts, decentralized identity.

Introduction

The rapid growth of the IoT has resulted in a highly interconnected world where devices, sensors, and systems communicate seamlessly to deliver real-time data and automate processes across various sectors [1-4]. From smart homes to industrial automation, IoT offers unparalleled opportunities to enhance efficiency, reduce operational costs, and improve decision-making [5]. This proliferation of connected devices and the vast amount of data generated also present significant challenges in ensuring the security, integrity, and privacy of the information being transmitted [6,7]. As IoT devices often operate in decentralized environments with varying degrees of security, maintaining the integrity of data and preventing unauthorized access have become paramount concerns for developers and security professionals alike [8-10].

One of the key challenges in securing IoT data was ensuring its authenticity and preventing tampering during transmission [11,12]. Traditional security measures such as centralized authentication and encryption mechanisms struggle to scale effectively in IoT environments due to the vast number of devices and the limited computational resources available on many IoT endpoints [13-15]. Many IoT networks suffer from vulnerabilities that expose sensitive information to cyberattacks, which can compromise the privacy and security of users [16-18]. Addressing these challenges requires more advanced and scalable solutions capable of providing end-to-end security while ensuring data integrity [19]. Blockchain technology has emerged as a promising solution to these problems due to its decentralized, transparent, and immutable nature [20,21].

Blockchain's decentralized structure inherently offers a more robust approach to securing IoT systems [22]. By providing a distributed ledger, blockchain allows for secure, transparent, and immutable data transactions across IoT devices [23]. The immutability of blockchain ensures that once data was recorded, it cannot be altered or tampered with without detection [24]. This feature makes blockchain particularly well-suited for securing IoT data, as it guarantees the integrity of information while offering a transparent audit trail that can be accessed by authorized users [25]. Additionally, the integration of cryptographic techniques into blockchain ensures that the data remains secure and encrypted, protecting it from unauthorized access and ensuring confidentiality.