RADemics

Identity and Access Management in IoT Utilizing Blockchain for Secure Device Authentication and Control

Dr.B.Devanathan, Vanitha.T
ANNAMALAI UNIVERSITY, ERODE SENGUNTHAR ENGINEERING COLLEGE

Identity and Access Management in IoT Utilizing Blockchain for Secure Device Authentication and Control

Dr.B.Devanathan MCA., M.Phil.,Ph.D., Assistant Professor, Department of Computer and Information Science, Annamalai University, devacisau@gmail.com

Vanitha.T, Assistant professor, Department of Artificial Intelligence and Data Science, Erode Sengunthar Engineering College, Erode, Tamilnadu, India, vanitha.sty3375@gmail.com

Abstract

The rapid proliferation of IoT devices across various industries has amplified the importance of secure and efficient identity and access management (IAM). This chapter explores the integration of blockchain technology for decentralized authentication in IoT ecosystems, addressing critical limitations of traditional authentication methods. Key discussions include the challenges posed by the resource-constrained nature of IoT devices and the dynamic behavior of IoT networks. The chapter delves into cryptographic solutions optimized for IoT environments and evaluates the balance between security, scalability, and performance. The potential benefits of decentralized approaches, such as improved resilience, enhanced privacy, and reduced reliance on central authorities, are critically assessed alongside their inherent challenges. Emerging trends and future directions for leveraging blockchain to enhance IoT device security are also highlighted. This comprehensive analysis aims to guide researchers and industry professionals toward developing robust, scalable IAM solutions for IoT.

Keywords:

IoT security, blockchain, decentralized authentication, cryptography, identity management, scalability.

Introduction

The Internet of Things (IoT) has rapidly evolved from a conceptual framework to a crucial technology shaping the modern world [1,2]. IoT encompasses a vast network of interconnected devices that range from industrial sensors and home automation tools to wearable health monitors and smart city infrastructure [3,4]. These devices continuously collect, exchange, and analyze data to enhance operational efficiency and improve quality of life [5]. As the number of connected devices grows exponentially, so do the security challenges associated with managing access and protecting sensitive data [6-8]. The scale and complexity of IoT ecosystems present unique demands for identity and access management (IAM) solutions that are both robust and adaptable [9].

The traditional centralized approaches to IAM face significant limitations when applied to IoT environments [10-13]. Centralized models often rely on single points of control that, if compromised, can jeopardize the entire network's integrity [14]. IoT devices often operate in

resource-constrained environments with limited processing power, memory, and energy, making it difficult to implement traditional cryptographic methods [15,16]. These constraints create vulnerabilities that malicious actors can exploit, leading to unauthorized access, data breaches, and compromised network security [17]. To address these challenges, the integration of blockchain technology offers a promising path toward decentralized authentication methods that are resilient, scalable, and secure [18,19].

Blockchain technology, with its distributed ledger capabilities, eliminates the need for centralized authorities and enhances trust through transparent, tamper-resistant records [20,21]. By decentralizing the authentication process, blockchain mitigates the risk of single points of failure and provides a framework that supports real-time verification across a vast array of devices [22,23]. Blockchain's ability to enable trustless interactions and cryptographically secure transactions can strengthen IAM processes in IoT, ensuring that only verified and authorized devices have access to network resources [24,25]. While blockchain-based systems present significant advantages, they also come with their own set of challenges, particularly in terms of resource usage and scalability.