Chapter 8
Blockchain-Enabled Secure Internet of Things

Vinod Kumar
https://orcid.org/0000-0002-3495-2320
Madanapalle Institute of Technology and Science, India

Gotam Singh Lalotra
Government Degree College for Women, Kathua, India

ABSTRACT

This century is the time of ubiquitous, smart, and intelligent devices. These devices have a wide variety of applications in different fields like business, manufacturing, healthcare, retail, education, security, transportation, etc. Internet of things is now becoming the inexorable part of the all these fields. But security has always been a major concern in embracing these technologies. The blockchain technology is the next frontier for securing the internet of things. It will play a pivotal role to secure the communication in internet of things ecosystem. This chapter discusses the blockchain-enabled secure internet of things (IoT).

1. INTRODUCTION

IoT is an internet technology connecting devices, machines and tools to the internet by means of wireless technologies. IoT is the one of the greatest phenomena of this century.

"According to Gartner research, The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." (Gartner, 2019)

IoT is offering new opportunities and providing a competitive advantage for businesses markets. It touches everything—not just the data, but how, when, where and why you collect it. The things connected to internet are changing due to the technologies that have created internet of Things. The services are being offered by devices on the edge of network without the human intervention at different levels

DOI: 10.4018/978-1-6684-7132-6.ch008

Copyright © 2023, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

As the data generation and analysis is indispensable to the IoT, Managing and handling information throughout its life cycle is a multifaceted exercise because data have to pass through many administrative boundaries. A serious thought is to be given for protection of data in its entire life cycle.

Considering IoT as system-of-system is a good practice as the different physical and technological components are involved in actually make up an IoT ecosystem. Providing business value to any organisation is not an easy task as the architect of these systems. The enterprise architects aim for designing integrated solutions which include Protocol, applications, transport, edge devices and analytical competencies for fully functional IoT system. With the increase of complexities, the challenges are posed to keep IoT secure without affecting the other system. (Internet of things beyond-bitcoin, 2019)

The security of data is vital as claimed by International Data Corporation (IDC) that 90% of organizations that implement the IoT have to suffer an IoT-based breach of back-end IT systems in the upcoming couple of years.

2. BACKGROUND

A blockchain is a distributed ledger that maintains a growing number of data records and transactions. As transactions are related to network participants, they are documented in blocks. They are arranged in the right sequence and assigned a record timestamp when they are added. It is a decentralised technology with the removal of intermediaries the tedious inconvenient banking process can be bypassed which is cost and time efficient. Cryptographic algorithms support the blockchain technology which ensure the prevention of data distortion and ensure high security. The intermediate block on the database cannot be replaces as every block has a hash to the previous block. A block can be extended but cannot be changed.

Generally, Blockchain Technology can be categorised in two core types- public blockchain and private blockchain. (Z Zheng, *et* al. 2017)

* In a **public** blockchain, everyone can read or write data. Some public blockchains limit the access to just reading or writing. Bitcoin, for example, uses an approach where anyone can write.
* In a **private** blockchain, all the participants are well known and trusted. This is useful when the blockchain is used between companies that belong to the same legal mother entity.

2.1. The Problem with the Current Centralized Model

The existing IoT ecosystems rely on centralized, brokered communication models also known as the server/client paradigm. All devices are identified, authenticated and connected through cloud servers that support huge processing and storage capacities. Connection between devices has to be established through the internet, whatsoever the distance in-between is.

While this model has connected generic computing devices for many years, and will support small-scale IoT networks for years to come, but will not cater the need of growing huge IoT ecosystems of future.

Current IoT solutions faces many challenges because the networking equipments, large server farms and centralised clouds involves very high expenditure for infrastructure development and their maintenance. As the IoT devices grow to billions consequently it will involve a large amount of investment.

7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/blockchain-enabled-secure-internet-of-things/310444

Related Content

Data Hiding for Text and Binary Files
Hioki Hirohisa (2013). *Multimedia Information Hiding Technologies and Methodologies for Controlling Data (pp. 351-371).*
www.irma-international.org/chapter/data-hiding-text-binary-files/70296

Formulating a Code of Cyberethics for a Municipality
Udo Richard Averweg (2007). *Encyclopedia of Information Ethics and Security (pp. 297-303).*
www.irma-international.org/chapter/formulating-code-cyberethics-municipality/13488

Review on Cryptography and Network Security Zero Knowledge Technique in Blockchain Technology
Anjana S. Chandran (2022). *International Journal of Information Security and Privacy (pp. 1-18).*
www.irma-international.org/article/review-on-cryptography-and-network-security-zero-knowledge-technique-in-blockchain-technology/308306

Interdisciplinary Training and Mentoring for Cyber Security in Companies
Ileana Hamburg (2022). *Research Anthology on Business Aspects of Cybersecurity (pp. 174-190).*
www.irma-international.org/chapter/interdisciplinary-training-and-mentoring-for-cyber-security-in-companies/288678

An Authentication Technique for Accessing De-Duplicated Data from Private Cloud using One Time Password
Prakash Mohanand Saravanakumar Chelliah (2017). *International Journal of Information Security and Privacy (pp. 1-10).*
www.irma-international.org/article/an-authentication-technique-for-accessing-de-duplicated-data-from-private-cloud-using-one-time-password/178641