Chapter 15
Current Trends in Integrating the Blockchain With Cloud-Based Internet of Things

Anchitaalagammai J. V.
Velammal College of Engineering and Technology, India

Kavitha S.
Velammal College of Engineering and Technology, India

Murali S.
Velammal College of Engineering and Technology, India

Hemalatha P. R.
Velammal College of Engineering and Technology, India

Subanachiar T.
Velammal College of Engineering and Technology, India

ABSTRACT

Blockchains are shared, immutable ledgers for recording the history of transactions. They substitute a new generation of transactional applications that establish trust, accountability, and transparency. It enables contract partners to secure a deal without involving a trusted third party. The internet of things (IoT) is rapidly changing our society to a world where every "thing" is connected to the internet, making computing pervasive like never before. It is increasingly becoming a ubiquitous computing service, requiring huge volumes of data storage and processing. The stable growth of the internet of things (IoT) and the blockchain technology popularized by cryptocurrencies has led to efforts to change the centralized nature of the IoT. Adapting the blockchain technology for use in the IoT is one such efforts. This chapter focuses on blockchain-IoT research directions and to provide an overview of the importance of blockchain-based solutions for cloud data manipulation in IoT.

DOI: 10.4018/978-1-6684-7132-6.ch015

I INTRODUCTION

IoT is a network system in both wired and wireless connection that consists of many software and hardware entities such as manufacturing management, energy management, agriculture irrigation, electronic commerce, logistic management, medical and healthcare system, aerospace survey, building and home automation, infrastructure management, large scale deployments and transportation.

There is a need of an advanced prototype for security, which considers the security issues from a holistic perspective comprising the advanced users and their intercommunication with this technology. Internet is primary of IoT hence there can be security loophole. Intercommunication paradigms are developed based on sensing programming for IoT applications, evolving an intercommunication stack to develop the required efficiency and reliability. Securing intercommunication is a crucial issue for all the paradigms that are developing based on sensing programming for IoT applications (Choudhury et al., 2017). Data generated by the IoT devices is massive and therefore, traditional data collection, storage, and processing techniques may not work at this scale. Furthermore, the sheer amount of data can also be used for patterns, behaviors, predictions, and assessment. Additionally, the heterogeneity of the data generated by IoT creates another front for the current data processing mechanisms. Therefore, to harness the value of the IoT-generated data, new mechanisms are needed. If we provide good solution which insures about security of the cloud storage system and communication between IoT device and cloud, then there is no problem to accept cloud storage to store IoT data.

Blockchains, or distributed ledgers for recording transactions, are showing potential for changing how the IoT operates. With the emergence and rapid popularization of the blockchain technology, mainly because of the hype around cryptocurrencies such as Bitcoin (Hussain et al., 2018), people started looking at blockchains as a possible alternative to the centralized solutions. An implicit immutability and decentralization are properties highly desirable in particular IoT scenarios. However, due to certain limitations of blockchains, such as limited scalability, or high computational cost of operating blockchain networks, blockchains are not originally suitable for work with IoT devices. Naturally, research of adapting blockchains for use in the IoT ecosystem has quickly evolved. The chapter the reader to navigate through the blockchain-IoT research directions and to provide an overview of the existing approaches and solutions.

II POTENTIAL ATTACKS IN IOT

A handful of IoT-related attacks seem to receive the most attention in the popular press which few of them are as follows.

1. **Denial of Service (DoS) attacks**: A denial-of-service (DoS) attack deliberately tries to cause a capacity overload in the target system by sending multiple requests. Unlike phishing and brute-force attacks, attackers who implement denial-of-service don't aim to steal critical data. However, DoS can be used to slow down or disable a service to hurt the reputation of a business. For instance, an airline that is attacked using denial-of-service will be unable to process requests for booking a new ticket, checking flight status, and canceling a ticket. In such instances, customers may switch to other airlines for air travel. Similarly, IoT security threats such as denial-of-service attacks can ruin the reputation of businesses and affect their revenue.