# Chapter 48
# Securing IoT Applications Using Blockchain

**Sreelakshmi K. K.**
*Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, India*

**Ashutosh Bhatia**
*Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, India*

**Ankit Agrawal**
*Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, India*

## ABSTRACT

*The internet of things (IoT) has become a guiding technology behind automation and smart computing. One of the major concerns with the IoT systems is the lack of privacy and security preserving schemes for controlling access and ensuring the security of the data. A majority of security issues arise because of the centralized architecture of IoT systems. Another concern is the lack of proper authentication and access control schemes to moderate access to information generated by the IoT devices. So the question that arises is how to ensure the identity of the equipment or the communicating node. The answer to secure operations in a trustless environment brings us to the decentralized solution of Blockchain. A lot of research has been going on in the area of convergence of IoT and Blockchain, and it has resulted in some remarkable progress in addressing some of the significant issues in the IoT arena. This work reviews the challenges and threats in the IoT environment and how integration with Blockchain can resolve some of them.*

DOI: 10.4018/978-1-6684-7132-6.ch048

## I. INTRODUCTION

The rapid advancements in networking technologies have led to an increased number of devices or things being able to connect to the Internet, which forms the Internet of Things, commonly known as IoT. Some of the leading IoT applications are Smart-grid, smart-homes, Industrial IoT, smart healthcare, etc. At a high-level, a typical IoT ecosystem consists of devices like sensors that collect data, actuators, and other devices that perform control and monitoring specific to the application area, communication infrastructure guided by the network protocols and local or centralized storage (cloud) that collects data from different devices and processes it for further analysis. The data generated by the various IoT devices is characterized by its vast volume, heterogeneity, and dynamic nature. Each device in an IoT environment has a unique identifier associated with it. A review work Colakovic and Hadialic (2018) gives a detailed and technical description of IoT and its enabling technologies. To build a sustainable IoT ecosystem that can adapt and perform well in a particular application area is a challenging task. With various smart solutions using a large number of devices, the problem of maintaining security for private or user data in the centralized cloud storage is a very tedious task that needs significant attention. The stakes are high if the private data falls into the hands of malicious entities. Another issue that draws concern is the resource and energy constraints of devices, which make it challenging to run massive cryptographic algorithms that strengthen the security of the data generated. The other challenges that need to be dealt with in specific situations such as a disaster are the fault tolerance and recovery of devices located at remote locations. Also, the diverseness in the IoT application areas and the uncertainty about the technology and the solutions offered creates a lack of trust in these solutions. Thus the need for a decentralized solution to ensure the security in an IoT ecosystem is an essential requirement of any IoT application.

The concept of Blockchain has been very active in cryptographic and security since its revelation in 2008. The remarkable advancements made in the Blockchain research have made cryptocurrencies a reality using BitCoin. The BitCoin with a current value of 5431.43 USD and holding around 5.7 million blocks is continuously increasing at a rapid rate with the help of more hashing power and mining pools. Software giants like Linux Foundation are already hacking the potential of Blockchain by researching on applications like HyperLedger (Blummer et al., 2018). With the Software industry predicting a promising future for the blockchain technology, it is essential that we investigate in detail the applicability of Blockchain in IoT to address the main security issues and how far it can be successful in solving them.

When Blockchain meets IoT, some of the expected benefits with this convergence are the building of trust between entities, completeness, consistency, and integrity of stored data, immutability or tamper-proof preservation of private data, reduction in expenses and thereby cheaper solutions, enhanced security and faster processing of Big Data.

The major objectives of the review work presented in this paper are:

- To investigate the security issues and challenges currently present in IoT applications.
- To highlight the decision criteria for applying Blockchain in IoT.
- To survey the scope of solutions that can be achieved through the convergence of Blockchain with IoT.
- To demarcate what IoT applications need and what distributed ledger technology (DLT) can offer.
- To present the state of the art in the integration of Blockchain with IoT.
- To identify and categorize IoT applications based on the issues addressed by Blockchain in the particular application area.