Chapter 23
Composite Identity of Things (CIDoT) on Permissioned Blockchain Network for Identity Management of IoT Devices

Anang Hudaya Muhamad Amin
https://orcid.org/0000-0002-2010-9789
Higher Colleges of Technology, UAE

Fred N. Kiwanuka
Higher Colleges of Technology, UAE

Nabih T. J. Abdelmajid
Higher Colleges of Technology, UAE

Saif Hamad AlKaabi
Higher Colleges of Technology, UAE

Sultan Khalid Abdulqader Rashed Ahli
Higher Colleges of Technology, UAE

ABSTRACT

Internet of things (IoT) is in the forefront of many existing smart applications, including autonomous systems and green technology. IoT devices have been commonly used in the monitoring of energy efficiency and process automation. As the application spreads across different kinds of applications and technology, a large number of IoT devices need to be managed and configured, as they are capable of generating massive amount of sensory data. Looking from this perspective, there is a need for a proper mechanism to identify each IoT devices within the system and their respective applications. Participation of these IoT devices in complex systems requires a tamper-proof identity to be generated and stored for the purpose of device identification and verification. This chapter presents a comprehensive approach on identity management of IoT devices using a composite identity of things (CIDoT) with permissioned blockchain implementation. The proposed approach described in this chapter takes into account both physical and logical domains in generating the composite identity.

DOI: 10.4018/978-1-6684-7132-6.ch023

1. INTRODUCTION

The rapid growth in the development of Internet-of-Things (IoT) has led to an increase in its utilization for smart applications. In green technology, IoT is becoming a forefront in the monitoring of energy efficiency and process automation. In a complex monitoring systems such as smart building and smart factory, large number of IoT devices need to be managed and configured. In addition, these devices are used in different kinds of integrated applications that could generate massive amount of sensory data. As such, there is a need for a proper mechanism to identify each IoT devices within the system and their respective applications. Participation of these IoT devices in complex-systems requires a tamper-proof identity to be generated and stored for the purpose of device identification. In addition, having an effective identity management mechanism of IoT devices would enable us to eliminate the possibility of identity spoofing and presence of rogue devices in the system. This perhaps could be achieved through integrating multiple information that defines the physical and logical identity of the devices.

With the advent in the field of process automation, Industrial process control and monitoring is a vital task that has been carried out by networks of Internet-of-Things (IoT). Critical event such as a surge in the electrical current or sudden increase in the temperature of boiler could be detected and monitored seamlessly. Rapid growth in the utilization of IoT in smart applications have continuously expand the IoT deployment in large-scale networks.

Sustainability is the key consideration for IoT deployments in smart applications. According to Mahadi et al. (Abu Hassan et al., 2018), there are four important factors that influence the sustainability of IoT usage in smart applications, namely performance expectancy, effort expectancy, social influence, and facilitating conditions. These four factors are derived from the Unified Theory of Acceptance and Use of Technology (UTAUT), as described in (Venkatesh et al., 2003).

There are numerous examples of IoT implementations for smart applications, including the works by Jain et. al. (Jain et al., 2019) in smart foundry and Catarinucci et. al. (Catarinucci et al., 2015) in their works on IoT-aware smart healthcare system. Apart from these initiatives, there are a number of IoT deployments focusing on enhancing and improving existing green technology applications. These can be seen from the works carried out by Garcia et. al. (Garcia et al., 2018) in wireless sensor network (WSN) based monitoring scheme for green technology, and IoT-based smart agriculture by Gondchawar and Kawitkar (Gondchawar & Kawitkar, 2016).

Our particular interest in IoT deployment for smart applications is in the smart building monitoring and management. Smart building usually comprises of different types of IoT devices and different kinds of applications. Rapid advances in different kinds of technology, including IoT, data analytics, and machine learning has risen up the demands for smart-building applications. There are different types of smart building applications ranging from smart office, smart library, smart home, and smart facilities. The benefits of having smart systems in building and infrastructure management is such that it helps in ensuring reduction in the amount of wasted energy used, as well as improved resource utilization.

Smart building applications typically consist of five components as described by Qolomany et. al (Qolomany et al., 2019). Figure 1 shows the composition of these components, which include sensors and actuators, smart control devices, software platform, networking and communication, and HVAC system. Integration of these components is essential in ensuring smooth execution of the applications.

An important aspect of smart building management is to ensure the safety and security of interconnected devices, users, and the applications. Security is an important aspect in smart building applications as its breach impact to the physical objects tend to be at a larger scale since it can directly affects our