ORIGINAL ARTICLE

Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions

Abraham Ayegba Alfa[1] · John Kolo Alhassan[2] · Olayemi Mikail Olaniyi[3] · Morufu Olalere[4]

Abstract

The growth of Internet of Things (IoT) took center stage universally due their capability to advance the course of human lives. Consequent upon this, several challenges were thrown up such as security of huge data stored and transmitted through network communication channels. IoT insecurity is partly due to centralization architecture, low computational strength, resource-constrained devices, variation in standards and protocols of communication. From this Systematic Literature Review (SLR), the 85 articles reviewed showed that privacy and security solutions are still being proposed or at conceptual levels, though a number of researchers favored the integration of Blockchain technology, cryptographic and hashing schemes into IoT. The Blockchain technology in IoT systems remains an open area of interest for top researchers especially in evolving frameworks to fit into the centralized architecture, functionality, and scalability demands of conventional IoT systems. In this article, we investigate security and privacy concerns of IoT from the lens of current trends, pertinent challenges, security methodologies, applications, and gaps for future research directions. Most specifically, there is prospect of utilizing cryptographic and hashing schemes offered by Blockchain technology in IoT. Then, high performance and scalable cryptographic schemes (that is, those in the class of lightweight approach) are suggested to deal with privacy and security of data in Blockchain-based IoT system. More importantly, this study provides basis for evolving secure and decentralized applications and systems in several domains such as smart farming.

Keywords Internet of Things · Blockchain technology · Security · Privacy · Lightweight cryptosystems

✉ Abraham Ayegba Alfa
abraham.alfa@kscoeankpa.edu.ng

John Kolo Alhassan
jkalhassan@futminna.edu.ng

Olayemi Mikail Olaniyi
mikail.olaniyi@futminna.edu.ng

Morufu Olalere
lerejide@futminna.edu.ng

[1] Department of Computer Science, Kogi State College of Education, Ankpa, Nigeria

[2] Department of Computer Science, Federal University of Technology, Minna, Nigeria

[3] Department of Computer Engineering, Federal University of Technology, Minna, Nigeria

[4] Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

1 Introduction

Internet of Things (IoT) is the pioneering technology which incorporates billions of Internet-enabled sensors, displays, cameras, smart phones, and wearable devices for the purpose of communication using the Internet backbone [1, 2]. Researchers consider the IoT to be the future of the Internet project because it vests end-users, machines, and everyday things having the capability to sense, interconnect, and relate with the outside world. The advancements of IoT are motivated by the need to offer humans more convenience, connectivity, real-time data, and safety to improve the quality of life by means of wide range of applications in Industrial IoT, smart homes, Internet of Farming, health, smart city, and transportation [3, 4].

One huge legacy of IoT is in the aspect of remote communication of diverse media, which are mostly referred to as universal movement. This offers possibilities of connecting peoples, things, processes, and data with the goal of enhancing internetworking for different benefits [5]. IoT are systems