Chapter 12

Towards the Integration of Blockchain and IoT for Security Challenges in IoT:
A Review

K. Dinesh Kumar
https://orcid.org/0000-0003-0843-1561
VIT University, Chennai, India

Venkata Ramana R.
Sri Venkateswara College of Engineering, Tirupati, India & Jawaharlal Nehru Technological University, Anantapur, India

Venkata Rathnam T.
Annamacharya Institute of Technology and Sciences, Tirupati, India & Jawaharlal Nehru Technological University, Anantapur, India

M. Sudhakara
https://orcid.org/0000-0002-2559-4074
VIT University, Chennai, India

Ravi Kumar Poluru
https://orcid.org/0000-0001-8591-5266
VIT University, India

ABSTRACT

Internet of things (IoT) technology plays a vital role in the current technologies because IoT develops a network by integrating different kinds of objects and sensors to create the communication among objects directly without human interaction. With the presence of internet of things technology in our daily comes smart thinking and various advantages. At the same time, secure systems have been a most important concern for the protection of information systems and networks. However, adopting traditional security management systems in the internet of things leads several issues due to the limited privacy and policies like privacy standards, protocol stacks, and authentication rules. Usually, IoT devices has limited network capacities, storage, and computing processors. So they are having more chances to attacks. Data security, privacy, and reliability are three main challenges in the IoT security domain. To address

DOI: 10.4018/978-1-6684-7132-6.ch012

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

the solutions for the above issues, IoT technology has to provide advanced privacy and policies in this large incoming data source. Blockchain is one of the trending technologies in the privacy management to provide the security. So this chapter is focused on the blockchain technologies which can be able to solve several IoT security issues. This review mainly focused on the state-of-the-art IoT security issues and vulnerabilities by existing review works in the IoT security domains. The taxonomy is presented about security issues in the view of communication, architecture, and applications. Also presented are the challenges of IoT security management systems. The main aim of this chapter is to describe the importance of blockchain technology in IoT security systems. Finally, it highlights the future directions of blockchain technology roles in IoT systems, which can be helpful for further improvements.

INTRODUCTION

The Internet of Things (IoT) has created a remarkable role in all environments of our daily lives. The Internet of Things technology already adopted in several fields to create the flexible environments like automobiles, healthcare, entertainments, sports, industries and homes etc. The adoption of IoT technology in daily activity environments, makes the life comfortable and easy. The main idea of the IoT technology is, all physical objects connected with each other under one network. So that, connected objects analyse the data and makes the proper decisions by sharing the information with each other. The IoT technology transforms these objects as a smart things by using the several technologies like sensors networks, internet protocols, communication technologies, ubiquitous computing, embedded devices and applications. Smart things along with supported technologies perform the tasks while using data analytical models and ubiquitous computing services. The complete concept of the IoT technology is, each and every connected application has to interact with other independent services to make the proper decisions. For example, smart traffic system will enable the vehicles to automatically respond when vehicles met with accidents. To get this potential technology and innovation, the traffic system application need to improve and growth. Additionally, the vehicles need to be manufactured to match the system requirements and robust communication protocols has to be developed for proper communication among different kinds of things. With this vision, traditional devices has become autonomous and smart intelligence and developing technology towards smart cities, smart homes, smart vehicles and smart everything.

The further development of IoT technology is more important to everyday life. This can be rapidly grows the evolution of hardware techniques like increasing the bandwidth by integrating the connected based networks to address issue of underutilization of bandwidth spectrum. The supporting technologies to IoT technology like Cloud computing, Bigdata analytics, Wireless sensor networks and Machine-to-Machine have now developed rapidly as supporting components for the IoT development. On the other hand, the privacy and security issues related to Machine-to-Machine, Cloud computing and Wireless sensors networks remain to increasing in the view of challenges in communication protocols with the IoT. So, the complete architecture of IoT needs to be robust and secured from several attacks which may arise the issues to integrity, privacy and confidentiality of collected data. Still adopting traditional secure paradigms in IoT technology which can lead major issues, because IoT is a collection of heterogeneous devices and several collections of interconnected computer networks. Additionally, the IoT things have sensors which may have limited memory and power. Due to the limited power of sensors, having more

15 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/towards-the-integration-of-blockchain-and-iot-for-security-challenges-in-iot/310448

Related Content

Managing the Commonplace: Small Water Emergencies in Libraries
Gerald Chaudron (2016). *International Journal of Risk and Contingency Management (pp. 42-61).*
www.irma-international.org/article/managing-the-commonplace/148213

Critical Path Stability Region: A Single-Time Estimate Approach
Hossein Arshamand Veena Adlakha (2014). *Analyzing Security, Trust, and Crime in the Digital World (pp. 35-60).*
www.irma-international.org/chapter/critical-path-stability-region/103810

Several Oblivious Transfer Variants in Cut-and-Choose Scenario
Chuan Zhao, Han Jiang, Qiuliang Xu, Xiaochao Weiand Hao Wang (2015). *International Journal of Information Security and Privacy (pp. 1-12).*
www.irma-international.org/article/several-oblivious-transfer-variants-in-cut-and-choose-scenario/148063

A Comprehensive Review of the Security and Privacy Issues in Blockchain Technologies
Mangesh Manikrao Ghonge, N. Pradeep, Renjith V. Raviand Ramchandra Mangrulkar (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 1293-1308).*
www.irma-international.org/chapter/a-comprehensive-review-of-the-security-and-privacy-issues-in-blockchain-technologies/310509

IPSec Overhead in Dual Stack IPv4/IPv6 Transition Mechanisms: An Analytical Study
M. Mujinga, Hippolyte Muyingi, Alfredo Terzoliand G. S. V. Radha Krishna Rao (2010). *Web Services Security Development and Architecture: Theoretical and Practical Issues (pp. 273-294).*
www.irma-international.org/chapter/ipsec-overhead-dual-stack-ipv4/40597