Chapter 12

A Secure Behavior Modelling for IoT Networks Using Blockchain:

Blockchain-Based Reputation-Based Agent Grouping in the Internet of Things

Jameel Ahmad Qurashi
https://orcid.org/0000-0003-0763-595X
Poornima University, India

Vikram Singh
Poornima University, India

Bright Keswani
https://orcid.org/0000-0003-1464-0431
Poornima University, India

Saurabh Shandilya
https://orcid.org/0009-0002-3508-9298
Poornima College of Engineering, Poornima University, India

Adarsh Kumar Pandey
Poornima University, India

Shikha Sharma
https://orcid.org/0000-0001-6339-9731
Poornima University, India

ABSTRACT

The Internet of Things (IoT) lets smart devices and humans use enticing services. Fostering adaptive machine-to-machine cooperation among intelligent objects may help IoT devices reach powerful sensing, reasoning, and real-time acting capabilities. To employ multiagent systems and the social attitude of engaging and cooperat-

DOI: 10.4018/979-8-3693-8151-9.ch012

ing for services, IoT devices must be paired with software agents. As IoT devices move across numerous settings, it may be challenging to locate credible partners for cooperation. As reputation may affect social groups, grouping agents in each IoT environment by social skills may be a solution. This study emphasizes agent reputation capital in a reputation model. Second, reputation capital organized IoT agents. The last contribution is employing blockchain technology to authenticate reputation capital, because this competition needs trustworthy and verified device or agent reputation information. Our testing shows that the model can identify almost all deceptive agents and provide good group composition findings if their proportion is below a threshold.

I. OVERVIEW

The "Internet of Things" (IoT) (Ashton, 2009) creates dispersed, context-aware smart environments around us, which pose challenges in terms of technology, society, and cost for altering our reality (Augusto, Callaghan, Cook, Kameas, & Satoh, 2013). Since the complicated needs constitute an expanding trend, promoting adaptive forms of collaboration (Fortino, Guerrieri, Russo, & Savaglio, 2014) to IoT smart objects (i.e., IoT devices) may make services accessible to other IoT devices (Fortino, Messina, Rosaci, & Sarné, 2018). This can help to meet such requirements. A wide range of networking, information, communication, and sensing technologies have been used in several IoT designs and standards that have been proposed to achieve this goal (Kortuem, Kawsar, Sundramoorthy, & Fitton, 2010; Fortino, Messina, Rosaci, & Sarné, 2018; Sheng, Yang, Yu, Vasilakos, McCann, & Leung, 2013). One effective strategy for promoting social interactions amongst smart devices is to implement a multiagent system, where each software agent is connected to a device that functions on its behalf (Zhang, Choo, & Beebe, n.d.; Uckelmann, Harrison, & Michahelles, 2011; Zhu & Zhou, 2006).

While it is very desirable for an Internet of Things device to be able to interact with other devices cooperatively and communicate across several federated administrative domains, selecting the right "partners" (Chiu, Hsu, & Wang, 2006) in a similar setting may be challenging. It should be noted that this task has a significant impact on the quality of the interactions between the collaborating devices and, consequently, the level of "satisfaction" that each device can obtain from these interactions. Examples of such interactions include situations in which the devices must interact critically, imply the use of significant resources, or require a high financial cost in order to obtain a service.