Chapter 6
Enhancing Identification of IoT Anomalies in Smart Homes Using Secure Blockchain Technology

Sidra Tahir
UIIT, Pakistan

ABSTRACT

Numerous technologies that automate processes and simplify our lives are included in smart homes. These gadgets may be helpful for various things, including temperature, lighting, and security access. Smart homes fundamentally enable remote control of equipment and appliances for homeowners via the internet of things (IoT) platform. Smart houses are able to understand their owners' routines and modify in accordance with their capacity for self-learning. The requirement to identify abnormalities in data created by smart homes arises from the necessity of convenience and cost savings in such a setting, as well as from the involvement of numerous devices. The topic of anomaly detection using deep learning is covered in this chapter. Additionally, the suggested solution is more secure because to the usage of block chain technology. Results show that the suggested strategy has exceptional accuracy and recall.

INTRODUCTION

Particular industries, such as intelligent transportation and IoT, have seen significant transformations as a result of the development of new generations of wireless communications and big data technology(Alamri, Jhanjhi, & Humayun, 2019; Humayun, Niazi, Jhanjhi, Alshayeb, & Mahmood, 2020). A prevalent application of the Internet of Things and ubiquitous computing is the Smart Home. In this application, ambient intelligence monitors the home's environment to provide context-aware services and facilitate remote home control (Almusaylim & Zaman, 2019; Zaidan & Zaidan, 2020) may include both wired and wireless communication technologies, and is controlled by a smart terminal, such as a mobile phone or

DOI: 10.4018/978-1-6684-7625-3.ch006

a personal computer, over the Internet. This is one of the distinguishing characteristics of a smart home (Humayun, 2020; Sovacool & Del Rio, 2020; Strengers, Kennedy, Arcari, Nicholls, & Gregg, 2019).

IoT devices contribute ease of use and automation to a smart home, however, there is a potential for data errors to occur(Chow et al., 2020; Humayun, Jhanjhi, Alamri, & Khan, 2020). These dangers are caused by flaws, inconsistencies, and mistakes in the data collected, transported, stored, and processed by the IoT (Alamri et al., 2019)(Ferrag, Shu, Yang, Derhab, & Maglaras, 2020; Saura, Ribeiro-Soriano, & Palacios-Marqués, 2021). Defects in the data can result in information that is inaccurate or deceptive, which has the potential to disrupt the operation of the smart home system and put the users' privacy and safety at risk. The proper identification and resolution of these issues are very necessary to guarantee the dependable and trustworthy functioning of smart homes(Alferidah & Jhanjhi, 2020). The dependability of smart homes is dependent on locating and resolving issues like these.

Deep Learning techniques can play a significant role in mitigating the risks associated with data defects in smart homes. (Churcher et al., 2021; Hussain, Hussain, Hassan, & Hossain, 2020). Machine learning models can detect defects by analyzing IoT data patterns and trends. This allows proactive data cleaning, correction, and re-collection. Additionally, machine learning algorithms can be utilized for predictive maintenance, where they learn from historical data to anticipate potential data defects or device failures, allowing for proactive intervention to prevent disruptions in the smart home environment(N. A. Khan, Jhanjhi, Brohi, Usmani, & Nayyar, 2020; Kishore Kumar, 2021; Soe, Feng, Santosa, Hartanto, & Sakurai, 2020; Xiao, Wan, Lu, Zhang, & Wu, 2018).

By bringing decentralized, irreversible, and transparent data management, blockchain technology plays a significant part in assuring the safety of internet-of-things (IoT) devices that are used in smart homes(Alamri et al., 2019; Shi et al., 2020; Taylor, Dargahi, Dehghantanha, Parizi, & Choo, 2020). Devices in a smart home may eliminate the need for a central authority by utilizing the distributed ledger system provided by blockchain. This allows the devices to record and confirm every transaction and interaction in a safe manner. This decentralized method improves security by eliminating the possibility of a single point of failure and cutting down on the system's susceptibility to cyberattacks. In addition, blockchain technology makes it possible to construct smart contracts, which may automate and regulate the way devices interact with one another according to certain predetermined circumstances. These contracts that carry out their own terms increase safety by lowering the likelihood that they will be tampered with or violated by unauthorized parties (S. Khan, Amin, Azar, & Aslam, 2021). The IoTs gadgets in a smart home may improve overall security and build a more resilient and trustworthy ecosystem by establishing trust with one another and preserving the integrity of their data with the use of blockchain technology.

The data deficiencies of smart homes are essential for a variety of reasons. To begin, the IoT technologies included in smart homes require data that is reliable and precise in order to function properly. Incorrect data can have an effect on the automation and management of smart devices, putting the user's comfort and safety in jeopardy(S. Li, Hao, Ding, & Xu, 2019; W. Liang, Li, Long, Kui, & Zomaya, 2019; Tahir, Hafeez, Abbas, Nawaz, & Hamid, 2022). Privacy and safety are given top priority in smart homes. Data flaws can allow for unauthorized access to sensitive data or the injection of harmful commands, posing a hazard to both users' privacy and their physical safety. Fixing data faults, raising user confidence, and increasing adoption of smart homes are all areas in which machine learning may help the IoT ecosystem retain its integrity and credibility(Benkhelifa, Welsh, & Hamouda, 2018; Ojha, Misra, & Raghuwanshi, 2021; Zaheer, Tahir, Almufareh, & Hamid, 2023).

In the context of smart homes, the primary focus of this study is on the identification of anomalies in the network traffic generated by IoT devices. Typically, smart homes have a gateway that is in charge of