Perspective
Volume 15:6, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

Cyber Security Protection by Using Internet of Things

Esther Leuenberger*

Department of Information Science, University of Melbourne, Australia

Introduction

IoT concepts are becoming more complex by the day as a result of increased demand and expansion in the advanced network system of the Internet of Things (IoT). The Internet of Things is difficult to define because it has evolved and improved since its inception. Still, the best definition is a network of connected digital and analogue computer devices with unique UIDs that can exchange data without the involvement of a human being. This is frequently referred to as a user interface for the centralised location system or application, which is typically a smartphone app that sends data or instructions to one or more edge IoT devices. As needed, the peripheral can perform functions and transmit data to the primary computer system or application, which a user can then access and use. Because of the variety of threat vectors, the uniqueness of IoT devices, and the lack of safety standards and guidelines, IoT devices are vulnerable to Internet attacks [1,2]. Depending on the part of the network targeted and the outcome of the attack, hackers may employ a variety of cyber security risks against IoT devices. As a result, IoT-related cybersecurity research is currently very active.

Description

Concerns about cyber security may be alleviated significantly by artificial intelligence. Artificial intelligence could be a valuable ally in the development of defences against attackers. AI can detect and analyse patterns to detect anomalies. This includes safeguarding IoT systems against hackers and employing artificial intelligence to detect anomalous behavior that could indicate an attack. However, in the IoT scenario, cybercriminals always have the upper hand because they only need to find a hole, as opposed to cybersecurity experts who must secure multiple sites. As a result, cyber attackers are increasingly relying on Artificial Intelligence (AI) to circumvent sophisticated algorithms that may overlook unusual behavior [3,4]. The advancement of IoT technology has heightened interest in AI. As a result of this advancement, several AI optimization tools can now recognise potential threats and activities in IoT cyber security applications. IoT applications are more vulnerable to vulnerabilities than traditional computer systems for a variety of reasons.

To begin with, there are numerous IoT systems available, including devices, platforms, communication channels, and protocols. Second, rather than being designed for Internet communication, IoT systems are made up of "things" that connect physical systems. Third, because users and devices are mobile, IoT systems lack clearly defined limitations and are subject to constant change. IoT systems would also pose technical risks. Finally, the limited energy supply of IoT devices makes it difficult to deploy improved security and solutions on linked devices. Lighting, heating, ventilation, air conditioning, and other services ranging from light detection, temperature, and noise to control systems are frequently managed by multiple nodes in an IoT ecosystem. All sensors and control systems communicate with one another via various networking protocols such as Bluetooth, Wi-Fi, RFID, and so on. To connect these devices to the Internet, IoT gateways are used. Each tier of the IoT ecosystem, which is comprised of many levels of protocols, services, and technology, poses privacy challenges. They can share data, limit computer resources, and connect a massive number of IoT nodes [5].

Conclusion

The rapid proliferation of IoT-based devices will undoubtedly make these networks more vulnerable to privacy challenges. Sensors, which are easily accessible IoT devices, have caused numerous security issues in IoT networks. The attacker has made all IoT devices vulnerable to connection to the software-enabled access point (SoftAP) because they have less processing power and appear to have a better signal than the current access point (AP) with the same service set identifier (SSID). This has made man-in-the-middle (MiTM) and eavesdropping attacks on Internet communications possible. Such assault scenarios have been used in IoT networks to develop IDSs and identify the risks associated with IoT devices. The concept of the Internet of Things (IoT) is centred on the methods used to communicate with a real, physical world via the Internet. Lighting, heating, ventilation, air conditioning, and other services ranging from light detection, temperature, and noise to control systems are frequently managed by multiple nodes in an IoT ecosystem. All sensors and control systems communicate with one another via various networking protocols such as Bluetooth, Wi-Fi, RFID, and so on.

References

1. Roscoe A.W and G.M. Reed. "A timed model for communicating sequential processes." *Theor Comput Sci* 58 (1988).
2. Kim, Hye Yeon and Frederick T. Sheldon. "Testing software requirements with z and statecharts applied to an embedded control systemt0t1." *Softw Qual J* 12 (2004): 231-264.
3. Yin, Yongfeng, Bin Liu and Zhen Li. "The integrated application based on real-time extended UML and improved formal method in real-time embedded software testing." *J Netw* 5 (2010): 1410.
4. Metsä, Jani, Shahar Maoz and Mika Katara. "Using aspects for testing of embedded software: experiences from two industrial case studies." *Softw Qual J* 22 (2014): 185-213.
5. Braione, Pietro, Giovanni Denaro and Andrea Mattavelli. "Software testing with code-based test generators: data and lessons learned from a case study with an industrial software component." *Softw Qual J* 22 (2014): 311-333.

***Address for Correspondence:** Esther Leuenberger, Department of Information Science, University of Melbourne, Australia, E mail: EstherLeuenberger50@gmail.com.*

Received: 07-June-2022, Manuscript No. jcsb-22-73845; **Editor assigned:** 09-June-2022, Pre QC No. P-73845; **Reviewed:** 23-June-2022, QC No. 73845; **Revised:** 28-June-2022, Manuscript No. R-73845; **Published:** 04-July-2022, DOI: 10.37421/0974-7230.2022.15.419.

How to cite this article: Leuenberger, Esther. "Cyber Security Protection by Using Internet of Things." *J Comput Sci Syst Biol* 15 (2022):419.