EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Editorial: Zero Trust based Internet of Things

Shancang Li[1]*

[1] University of the West of England, Bristol BS16 1QY, UK

Abstract

Zero trust is an emerging framework aims at enhancing the security of Internet of Things (IoT), which connects billions of smart devices. Specifically, the zero trust security shows great benefits for securing unmanaged devices that might be unable to run computational expensive cryptographic suits. This editorial will introduce the zero trust IoT (zIoT) and its application in new IoT era.

Received on 29 October 2019; accepted on 30 October 2019; published on 30 October 2019

Keywords: Zero Trust IoT, Privacy, Security

doi:10.4108/eai.5-6-2020.165168

1. Introduction

The Internet of Things (IoT) connects billions of devices to the internet and the number is still increasing, which makes it very challenging to secure the applications, data, users, and devices in the complicated system. The zero trust security has show great potentials for IoTs which follows "never trust, always verify" principle. In the past few years, the zero trust security has attracted attentions from both industry and academic. The zero trust holds the principle that every attempt to the resources in IoT should be verified before granting the access. The CISCO, VMware, Illumino, *et al.* have proposed their zero trust security solutions for IoT.

This zero trust covers a number of key pillars of IoT, including device access control, network access control, visibility & analysis, aotomatic security, data control, user control, workloads, *etc.* This issue covers topics like energy consumption of IoT and wireless sensor networks (WSNs) [1], smart devices that can detect accident [2], smart surgery system [3], and speech recognisable IoT solutions [4]. All these areas have a strong need for zero trust security architecture that includes a broad range of security controls mentioned above. On the other hand, the zero trust security architects can force the system re-verify identities, connect attempts, accesses to provide a more secure environment for protecting sensitive resources. However, the zIoT is still in its infant phase and a number of challenges need to be fixed: (1) zero trust security architecture for IoT; (2) trustworthiness of non-user IoT devices and agentless device; (3) segmentation of critical zIoT.

This issue presents the most recent research findings in abobe key research areas and details can be found in Section 2.

2. The Papers

In the paper entitled “Study on Evolutionary Approaches for Improving the Energy Efficiency of Wireless Sensor Networks Applications" [1], Balasubramanian *et al.* investigated the energy consumption in the wireless sensor networks (WSNs), one of a key components of IoT, in which evolutionary algorithms based approaches have been developed for optimising energy/time consuming process in IoT and WSNs.

In the paper entitled “A Review on Smart Helmet for Accident Detection using IOT" [2], Impana *et al.* reviewed the most recent research works in accident detection using smart IoT devices. The authors also proposed a solution based on micro controller, RF transmitter, and smart sensors, which can detailed key information to help detect accident, including images, video clips, position, *etc.*

In the paper entitled “An Intelligent Surgery Information System Using RFID for Internet of Things", Hung *et al.* proposed an intelligent surgery information system by combining HIS, PACS and LIS to assist medical personnel to import patient’s clinical records, imaging reports, inspection reports and other relevant

*Corresponding author. Email: shancang.li@ieee.org information before, during and after surgery. In this work, key procedures, such as recording, re-checking, report, presentation, *etc.*, are introduced to guarantee healthcare systems work in a a secure and smart manner [3].

In the paper entitled “A Neuro Fuzzy Classifier with Linguistic Hedges for Speech Recognition" [4], Vani *et al.* developed a fuzzy classifier model for partitioning feature space for noisy and clean speech classification. The experimental results in this work shows the proposed solution can enhance the accuracy by 5%.

3. Concluding Remarks

This editorial addressed the zero trust security in IoT and introduced four related research finding in the security and key technologies of IoT. Specifically the key solutions for accident detection, healthcare systems, are very practical in the applications of IoT. We hope this issue can help our readers open their mind in different areas of IoT.

We express our sincerely thanks to all authors and reviewers for kingly sharing their research findings and valuable comments. We would also like to thank all staff member for making this excellent issue.

References

[1] D. Lubin Balasubramanian, V. Govindasamy. (2020) *Study on Evolutionary Approaches for Improving the Energy Efficiency of Wireless Sensor Networks Applications. EAI Endorsed Transactions on Internet of Things*, 5(20):1-1.

[2] H.C. Impana, M. Hamsaveni, H.T. Chethana (2020) *A Review on Smart Helmet for Accident Detection using IOT. EAI Endorsed Transactions on Internet of Things*, 5(20):2-2.

[3] Lun-Ping Hung, Shen-Yuan Tang, Chien-Liang Chen, Shih-Yang Yang (2020) *An Intelligent Surgery Information System Using RFID for Internet of Things. EAI Endorsed Transactions on Internet of Things*, 5(20):3-3.

[4] Vani H Y, Anusuya M A (2020) *A Neuro Fuzzy Classifier with Linguistic Hedges for Speech Recognition. EAI Endorsed Transactions on Internet of Things*, 5(20):4-4.