Future Generation Computer Systems 82 (2018) 395–411

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

IoT security: Review, blockchain solutions, and open challenges

Minhaj Ahmad Khan [a,*], Khaled Salah [b]

[a] Bahauddin Zakariya University Multan, Pakistan
[b] Khalifa University of Science, Technology & Research, Sharjah, United Arab Emirates

HIGHLIGHTS

- IoT is a promising disruptive technology with incredible growth, impact and potential.
- A review of emerging topics related to Internet of Things (IoT) security and Blockchain is presented.
- A mapping of the major security issues for IoT to possible solutions is tabulated.
- Blockchain technology and its robust solutions for challenging and critical IoT security problems are reviewed.
- A parametric analysis of the state-of-the-art IoT security issues and solutions is described.

ARTICLE INFO

Article history:
Received 17 July 2017
Received in revised form 2 November 2017
Accepted 12 November 2017
Available online 26 November 2017

Keywords:
IoT security
Blockchain
IoT protocols
Network security
Data security

ABSTRACT

With the advent of smart homes, smart cities, and smart everything, the Internet of Things (IoT) has emerged as an area of incredible impact, potential, and growth, with Cisco Inc. predicting to have 50 billion connected devices by 2020. However, most of these IoT devices are easy to hack and compromise. Typically, these IoT devices are limited in compute, storage, and network capacity, and therefore they are more vulnerable to attacks than other endpoint devices such as smartphones, tablets, or computers.

In this paper, we present and survey major security issues for IoT. We review and categorize popular security issues with regard to the IoT layered architecture, in addition to protocols used for networking, communication, and management. We outline security requirements for IoT along with the existing attacks, threats, and state-of-the-art solutions. Furthermore, we tabulate and map IoT security problems against existing solutions found in the literature. More importantly, we discuss, how blockchain, which is the underlying technology for bitcoin, can be a key enabler to solve many IoT security problems. The paper also identifies open research problems and challenges for IoT security.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

With the rapid growth of smart devices and high speed networks, the Internet of Things (IoT) has gained wide acceptance and popularity as the main standard for low-power lossy networks (LLNs) having constrained resources. It represents a network where "things" or embedded devices having sensors are interconnected through a private or a public network [1,2]. The devices in IoT can be controlled remotely to perform the desired functionality. The information sharing among the devices then takes place through the network which employs the standard protocols of communication. The smart connected devices or "things" range from simple wearable accessories to large machines, each containing sensor chips. For instance, the Lenovo smart shoes contain chips which provide support of tracking and analyzing fitness data [3]. Similarly, the electrical appliances including washing machines, and refrigerators can be controlled remotely through IoT. The security cameras installed for surveillance of a location can be monitored remotely anywhere in the world.

Apart from the personal use, IoT serves the community needs as well. Various smart devices which perform diverse functionalities such as monitoring surgery in hospitals, detecting weather conditions, providing tracking and connectivity in automobiles, and identification of animals using biochips are already serving the community specific needs [4]. The data collected through these devices may be processed in real-time to improve efficiency of the entire system.

The future significance of IoT is evident due to its application in everyday life. It continues to grow rapidly due to evolution of hardware techniques such as improving bandwidth by incorporating cognitive radio based networks to address underutilization

* Corresponding author.
E-mail addresses: mik@bzu.edu.pk (M.A. Khan), khaled.salah@kustar.ac.ae (K. Salah).

https://doi.org/10.1016/j.future.2017.11.022
0167-739X/© 2017 Elsevier B.V. All rights reserved.

of frequency spectrum [5,6]. In the literature, the Wireless Sensor Networks (WSNs) and Machine-to-Machine (M2M) or Cyber-Physical Systems (CPS) have now evolved as integral components for the broader term IoT. Consequently, the security problems related to WSN, M2M, or CPS continue to arise in the context of IoT with the IP protocol being the main standard for connectivity. The entire deployment architecture therefore needs to be secured from attacks which may hinder the services provided by IoT as well as may pose threat to privacy, integrity or confidentiality of data. Since the IoT paradigm represents a collection of interconnected networks, and heterogeneous devices, it inherits the conventional security issues related to the computer networks. The constrained resources pose further challenges to IoT security since the small devices or things containing sensors have limited power and memory. Consequently, the security solutions need to be adapted to the constrained architectures.

There has been a tremendous effort in recent years to cope with security issues in the IoT paradigm. Some of these approaches target security issues at a specific layer, whereas, other approaches aim at providing end-to-end security for IoT. A recent survey by Alaba et al. [7] categorizes security issues in terms of application, architecture, communication, and data. This proposed taxonomy for IoT security is different from the conventional layered architecture. The threats on IoT are then discussed for hardware, network, and application components. Similarly, another survey by Granjal et al. [8] discusses and analyzes security issues for the protocols defined for IoT. The security analyses presented in [9–11] discuss and compare different key management systems and cyrptographic algorithms. Similarly, the authors in [12–14] target a comparative evaluation of intrusion detection systems. An analysis of security issues for fog computing is presented in [15,16]. A survey by Sicari et al. [17] discusses contributions providing confidentiality, security, access control and privacy for IoT along with the security for middleware. The authors discuss trust management, authentication, privacy issues, data security, network security, and intrusion detection systems. For edge computing based paradigms including mobile cloud computing, mobile edge computing and fog computing, the identity and authentication, access control systems, network security, trust management, fault tolerance and implementation of forensics are surveyed in [18].

A survey of privacy preserving mechanisms for IoT is given in [19]. The author describes the secure multi-party computations to be enforced for preserving privacy of IoT users. The mechanisms of credit checking and attribute based access control are described to be effective solutions for privacy preserving in IoT. Zhou et al. [20] discuss different security threats and their possible countermeasures for cloud-based IoT. The authors describe identity and location privacy, node compromising, layer removing or adding, and key management threats for IoT using clouds. Another survey by Zhang et al. [21] discusses major IoT security issues in terms of unique identification of objects, authentication and authorization, privacy, the need for lightweight cryptographic procedures, malware, and software vulnerabilities. The IOT-a project [22] describes a reference architecture for IoT whose compliance requires implementation for trust, privacy, and security. The trust model is expected to provide data integrity and confidentiality while making end-to-end communication possible through an authentication mechanism. Moreover, to avoid improper usage of data, the privacy model requires defining access policies and mechanisms for encrypting and decrypting data. The security aspect incorporates three layers corresponding to the services, communication, and application. Similarly, the Open Web Application Security Project (OWASP) [23] describes top 10 vulnerabilities for the IoT architecture. These vulnerabilities include insecure interfaces of entities of the IoT architecture, inappropriate security configuration, physical security and insecure software/firmware.

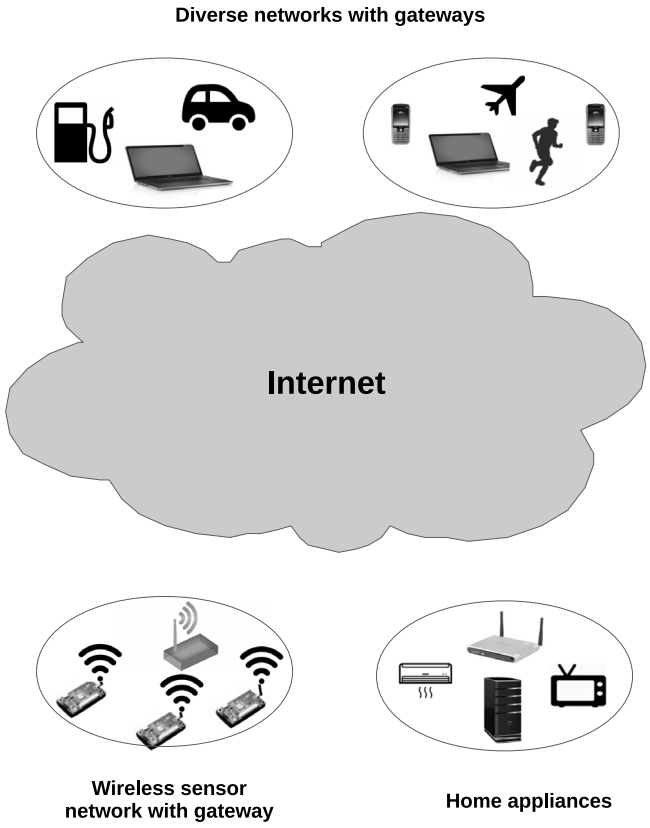

Fig. 1. An overview of IoT elements.

In sharp contrast to the survey articles found in the literature, our main contributions in this article can be summarized as follows:

- A parametric analysis of security threats and their mapping to possible solutions for IoT.
- Taxonomy and categorization of IoT security issues with respect to its layers, and the countermeasures used to address these issues.
- Discussion of basic characteristics of the blockchain based security solutions and analysis of their effectiveness for securing IoT.
- Future directions highlighting possible solutions for open IoT security problems.

The rest of the paper is organized as follows. Section 2 delineates the IoT architecture and the security challenges being faced at each layer of the protocol stack deployed by IoT. Section 3 categorizes the main security issues, whereas, Section 4 analyzes and describes a mapping of the solutions proposed. Various solutions related to blockchain security are discussed and analyzed in Section 5. In Section 6, we discuss the research challenges posing main hindrance to IoT security and their possible solutions before concluding the paper in Section 7.

2. IoT architecture and security challenges

A typical IoT deployment contains heterogeneous devices with embedded sensors interconnected through a network, as shown in Fig. 1. The devices in IoT are uniquely identifiable and are mostly characterized by low power, small memory and limited processing capability. The gateways are deployed to connect IoT devices to the outside world for remote provision of data and services to IoT users.

Download English Version:

https://daneshyari.com/en/article/6873216

Download Persian Version:

https://daneshyari.com/article/6873216

Daneshyari.com