The Current and Future Status of IoT Security
Challenges in Practice

Ali Ahmed H. Alyami*
College of Computer Science and Information System, Department of Information Systems, University of Najran, Saudi Arabia; ali.zamanan@gmail.com

Abstract
Objective: This study presents IoT security features, IoT security layers' challenges with application layer and network layer.
Methods/Findings: Major security concerns of IoT development are caused by heterogeneity of interconnected entities as well as incompatibility of development and communication protocols used. Authentication, integrity, and availability are compromised by such attacks as man-in-the-middle, replay, and denial of services attacks. Looking into the future, blockchain and software-defined network technologies, are promising to deliver a more secured IoT operational environment, and could, therefore, reduce associated cyber-attack instances. Application: Furthermore, IoT security solution with current IoT security arrangements incorporate trust foundation, a move towards a united design and architecture is also discussed.

Keywords: Cyber Security, Cybersecurity, Cyber-Security, Computer Security, IoT Security Futures, and IoT Security Solutions, Risk

1. Introduction

The technology domain is ever disrupted by rapid developments and innovations that come along with opportunities and threats. For every opportunity provided by any technological innovation, hackers and scammers find ways of maliciously exploiting them. Cyber-attacks have been known to It security experts since the dawn of computers and the internet. The internet became a primary playground for attackers and has been used to launch devastating attacks on individual users, small, medium and large business organizations as well as governments. The nature of attacks has grown to match technology, and the application of sophisticated tools has resulted in increased magnitude and number of cyber-attacks.

The world now relies on powerful computing technologies such as Big Data, Internet of Things, Data Analytics, Machine Learning, Artificial Intelligence, Smart Grid Systems, Cloud Computing, and Business Intelligence. All these run on highly complicated platforms that must always be tamper-proof lest attackers compromise their services and components. IoT is one of the fastest growing technologies which bring together millions of interconnected objects, services, devices and humans (things). The interconnected entities communicate by sharing data and information through a stack of rules and protocols. IoT devices use uniquely identified by both the region they are in and their IP addresses using a typical identity management system.

Radio Frequency Identification and Wireless Sensor Networks have attributed to the rapid development of

*Author for correspondence
this technology and have attributed to the development of smart cities, homes and transportation infrastructure. The RFID tagging of every device provides an identification mechanism for connected devices. WSN on the other hand has allowed the interconnected things to be wireless identifiable and communicate with the physical, cyber and digital world.

The purpose of this paper is to research on the current state and future trends of security in the Internet of Things (IoT) as the computer revolution moves with speed to interconnect millions of devices and individuals, and enabling communication between them. Section II, III, IV, and V of this paper describe the IoT security features, IoT layers’ security challenges, IoT security solutions, and future trends of IoT security respectively.

2. IoT Security Features

Security challenges in this development are either caused by technological or security problems. Security challenges are related to the functionalities and principles that must be enforced to create a securely-networked environment. Such challenges require that end-to-end security, integrity, confidentiality, authentication and authorization features be implemented. The features and privacy challenges general background is stated. Technology defined challenges are as a result of the heterogeneous and ubiquitous nature of IoT devices. They are caused by IoT features such as scalability, wireless connections, energy, and its distributed nature. IoT platforms provide security by running authorized software on all devices, running an authentication program whenever a new device (or thing) is turned on or connected to the network, and by installing necessary software updates and patches.

Security practices are anchored on the CIA-Confidentiality, Integrity, and Availability security goals. Confidentiality means that communications and transactions only reach the intended persons, and are not exposed to unauthorized attacks. Integrity refers to the security mechanisms used to preserve the authenticity of data—whether stationary or in transit. In IoT, security experts must make sure that sensors conceal information about other neighbors. To secure data, IoT users must understand how data is managed plus all the involved processes. The integrity feature is based on data exchanges between many different devices. It ensures that information is not tampered or interfered with, and is not manipulated during transmission. The availability feature is the backbone of IoT technology—connecting millions of devices. Data and connected ‘things’ must always be available to end-users. As a security requirement, every IoT device must identify and correctly authenticate other devices and users accessing them, or requesting access to their data and services. However, this is a security challenge due to the nature of entities and objects involved. Every interaction must, therefore, be mutually authenticated especially where entities are interacting for the first time. Lightweight solutions offered unique security feature and were introduced due to computational and power limitations of IoT entities. Since these solutions are meant to run on a device with varying and limited capabilities, they need to be compatible with each device’s computational capabilities.

3. IoT Security Layers’ Challenges

3.1 Application Layer

Signals in IoT are transmitted over long distances from sensor nodes to entities using wireless technologies. Disturbing waves could compromise the efficiency of wireless signals. Maliciously intended people can physically attack sensor nodes because they operate in an external environment. The limited storage and computational capacities and power consumption of IoT entities, which are inherent to the nature of network topology, expose IoT entities to many types of security attacks, threats, vulnerabilities, and risks. Replay attacks could easily be used to compromise the system’s confidentiality by spoofing, altering and replaying identity information belonging to other devices. Other attacks include node capture attacks which add another node to the network, denial of service (DoS), and timing attack which occurs
when attackers successfully analyze the time needed to encrypt IoT messages and data.

3.2 Network Layer
At the network layer of IoT, man-in-the-middle attacks are widespread. The susceptibility is caused by the nature of access mechanisms and data exchange. The communication channel easily gets compromised when attackers launch eavesdropping attacks. The introduction machine to machine communications in IoT has resulted in compatibility issues which make it difficult for traditional internet protocols to operate. Attackers, in turn, take this advantage to gain more information about users and interconnected devices and later use this information for criminal activities. Both the network and connected objects must be protected and well secured. Objects should have the ability to learn a network’s state of security and operation to protect them from any form of attack.

This creates the need for compatible protocols and useful software applications to enable objects’ automatic response to abnormal situations and network behavior. By focusing on network layer functions, different technologies such as, Device to Device (D2D) need different protocols to be operated.

3.3 Application Layer
The global community has not established any standards and policy statements that could be used to govern the development of, and interaction between IoT entities. Different systems use different authentication mechanisms making it difficult to integrate them and ensure data privacy and identity authentication. The interconnected entities share voluminous data which cause large overheads on applications used to analyze data. These overheads could negatively affect the availability of system services. The general application layer survey is mentioned.

4. IoT Security Solutions
Current IoT security solutions include trust establishment, a move towards a federated architecture, authentication measures, and security awareness. Authentication measures allow entities to authenticate themselves before they can access corporate and other entities services and data. End-to-end encryption algorithms prevent any unauthorized access, attacks, and interferences. Firewalls are used to filter traffic from external networks, therefore, allowing the use of safe resources. A federated architecture aims to solve the compatibility issues in IoT by providing a centralized unit that overcomes the heterogeneity nature of IoT entities. The general security background is stated.

5. Future IoT Security Trends
The emergence of more powerful technologies such as blockchain and software-defined networks (SDN), the likelihood of new and effective security solutions in IoT is increasingly growing. There is accelerated research on applications of blockchain technology in securing IoT. Blockchain can be used to create a mesh network which allows IoT entities to securely and reliably connect, and avoiding any chances of spoofing and impersonation. Any device that is registered with blockchain would have a unique identifier. For such devices to connect, the blockchain ids will be used as URLs while the local blockchains wallets will raise identity requests.

SDNs have empowered network operations, made them more flexible and eased network management activities. This technology can as well be leveraged to provide IoT security. SDN controllers could be configured in such a way that after correctly authenticating connected devices, and establishing a secured connection between the switch and the controller, all other switch ports are automatically blocked. SDN controllers are typical security guards who receive initial transmission flow whenever two or more devices want to communicate. It serves to ensure that devices know destinations of requested transmission flow before they can start exchanging data.

6. Conclusion
The Internet of Things is a powerful technology that interconnected millions of devices including humans across
large geographical areas. Major security concerns of this
development are caused by heterogeneity of intercon-
ected entities as well as incompatibility of development
and communication protocols used. Authentication,
integrity, and availability are compromised by such
attacks as man-in-the-middle, replay, and denial of ser-
vices attacks. Looking into the future, blockchain and
software-defined network technologies, are promising
to deliver a more secured IoT operational environment,
and could, therefore, reduce associated cyber-attack
instances.

7. Acknowledgement

This paper has been presented and discussed dur-
ing the International Conference on Communication,
Management and Information Technology- ICCMIT
2019, Vienna, Austria.

8. References

1. Dlamini MT, Eloff MM, Eloff J. H. Internet of Things:
Emerging and future scenarios from an information secu-
rity perspective. Southern Africa Telecommunication
Networks and Applications Conference; 2009. p. 1–6.
2. Yousuf T, Mahmoud R, Alouf F, Imran Z. Internet of Things
(IoT) Security: Current status, challenges, and counter-
measures. International Journal for Information Security
Research. 2015; 5(4):608–16.
3. Roman R, Zhou J, Lopez J. On the features and challenges
of security and privacy in distributed internet of things.
Computer Networks. 2013; 57(10):2266–79.
4. Rossouw S, Johan N. From Information Security to Cyber
Security. Elsevier Journal. 2012; 3(8):97–102.
5. Bello O, Zeadally S, Badra M. Network layer inter-opera-
tion of Device-to-Device communication technologies in
Internet of Things (IoT). Ad Hoc Networks. 2017; 57:52–
62.
6. Karagiannis V, Chatzimisios P, Vazquez-Gallego F,
Alonso-Zarate J. A survey on application layer protocols
for the internet of things. Transaction on IoT and Cloud
Computing. 2015; 3(1):11–17.
7. Zhang ZK, Cho MCY, Wang CW, Hsu CW, Chen CK,
Shieh S. IoT security ongoing challenges and research
opportunities. 2014 IEEE 7th International Conference
on Service-oriented Computing and Applications; 2014. p.
230–4.
8. Mohan S, Mikael A, Gedare B, Sadeghi AR, Ahmad I, Negin
S, Bruno S. Special Session: The future of IoT security.
International Conference on Embedded Software; 2018. p.
1–7.
9. Sahoo KS, Bibhudatta S, Abinas P. A secured SDN frame-
work for IoT. Conference on Man and Machine Interfacing;
2015. p. 1–4.