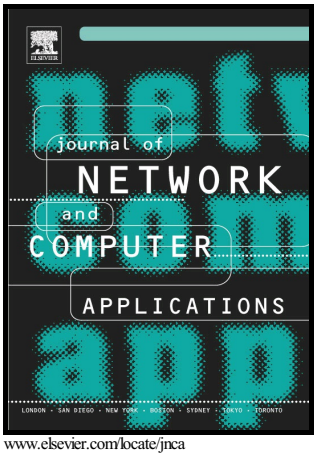
Internet of things Security: A Survey

Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30145-5
DOI: http://dx.doi.org/10.1016/j.jnca.2017.04.002
Reference: YJNCA1899

To appear in: *Journal of Network and Computer Applications*

Received date: 3 December 2016
Revised date: 14 March 2017
Accepted date: 4 April 2017

Cite this article as: Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem and Faiz Alotaibi, Internet of things Security: A Survey, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2017.04.002

Internet of things Security: A Survey

Fadele Ayotunde Alaba[a*], Mazliza Othman[a*], Ibrahim Abaker Targio Hashem[a], Faiz Alotaibi[b]

[a]Faculty of Computer Science and information Technology, University of Malaya, 50603, Kuala Lumpur, Malaysia.

[b]Faculty of Computer Science and information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia.

ayotundefadele@siswa.um.edu.my

mazliza@um.edu.my

targio@siswa.um.edu.my

gs3095@mutiara.upm.edu.my

Abstract

The Internet of things (IoT) has recently become an important research topic because it integrates various sensors and objects to communicate directly with one another without human intervention. The requirements for the large-scale deployment of the IoT are rapidly increasing with a major security concern. This study focuses on the state-of-the-art IoT security threats and vulnerabilities by conducting an extensive survey of existing works in the area of IoT security. The taxonomy of the current security threats in the contexts of application, architecture, and communication is presented. This study also compares possible security threats in the IoT. We discuss the IoT security scenario and provide an analysis of the possible attacks. Open research issues and security implementation challenges in IoT security are described as well. This study aims to serve as a useful manual of existing security threats and vulnerabilities of the IoT heterogeneous environment and proposes possible solutions for improving the IoT security architecture.

Keywords: IoT, Security, Privacy

1.0 Introduction

The Internet of things (IoT) provides an integration of various sensors and objects that can communicate directly with one another without human intervention. The “things” in the IoT include physical devices, such as sensor devices, which monitor and gather all types of data on machines and human social life (Yan, Zhang, and Vasilakos, 2014). The arrival of the IoT has led to the constant universal connection of people, objects, sensors, and services. The main objective of the IoT is to provide a network infrastructure with interoperable communication protocols and software to allow the connection and incorporation of physical/virtual sensors, personal computers (PCs), smart devices, automobiles, and items, such as fridge, dishwasher,

microwave oven, food, and medicines, anytime and on any network (Aazam, St-Hilaire, Lung, and Lambadaris, 2016). The development of smartphone technology allows countless objects to be a part of the IoT through different smartphone sensors. However, the requirements for the large-scale deployment of the IoT are rapidly increasing, which then results in a major security concern (Gu, Qiu, and Wang 2012).

Security issues, such as privacy, authorization, verification, access control, system configuration, information storage, and management, are the main challenges in an IoT environment (Jing, Vasilakos, Wan, Lu, and Qiu, 2014). For instance, IoT applications, such as smartphone and embedded devices, help provide a digital environment for global connectivity that simplifies lives by being sensitive, adaptive, and responsive to human needs. However, security is not guaranteed. The privacy of users may be compromised and the information on users may be leaked when user signal is interrupted or intercepted. To extensively adopt the IoT, this issue should be addressed to provide user confidence in terms of privacy and control of personal information (Li, Tryfonas, and Li, 2016). The development of IoT greatly depends on addressing security concerns (Sicari, Rizzardi, Grieco, and Coen-Porisini, 2015).

This study focuses on security threats and vulnerabilities in the context of the IoT and the state-of-the-art IoT security. We survey a wide range of existing works in the area of IoT security that use different techniques. We present an IoT security taxonomy based on the current security threats in the contexts of application, architecture, and communication. Possible security threats and vulnerabilities of the IoT are also compared. We propose a new security scenario for the IoT structure and provide an analysis of the possible threats and attacks to the IoT environment.

This study aims to serve as a useful manual of existing security threats and vulnerabilities of the IoT heterogeneous environment and proposes possible solutions for improving the IoT security architecture. State-of-the-art IoT security threats and vulnerabilities in terms of application deployments, such as smart environment, intelligent transportation, smart grid, and healthcare system, have been studied. The IoT security, particularly the IoT architecture, such as authentication and authorization, has also been investigated.

The most relevant work is a secure IoT architecture for smart cities that uses the black SDN proposed by Chakrabarty and Engels (2016). However, the proposed architecture does not support a full SDN implementation due to the constrained nature of the IoT nodes, which makes IoT nodes vulnerable and causes new types of threats and attacks, including node capturing, eavesdropping, and tampering. The architecture also decreases the network efficiency and leads to complicated routing. The current study proposes a possible solution to the security problem based on the weaknesses and limitations of the existing approaches in a comprehensive way. Other related works include the end-to-end (E2E) secure key-managing protocol for e-health applications by Abdmeziem and Tandjaoui (2015). The security protocol is limited to offloading heavy cryptographic primitives to third parties and does not specify the necessary trade-off between the communication overhead and the number of third parties. Flauzac, Gonzalez, and Nolot (2015) proposed a novel SDN-based security architecture for the IoT using border controllers. However, the use of border controllers has many drawbacks, such as securing both wanted and unwanted traffic and enterprise protection. These challenges were not addressed by the authors. Hernández-Ramos et al. (2015) focused on a lightweight authentication and authorization framework for constrained smart objects. Nevertheless, the proposed framework was not integrated into the constrained IoT environments for authentication, authorization, and defining some alternative methods to evaluate its suitability.

The remainder of this paper is organized as follows. Section 2 presents an overview of the IoT and the difference between IoT security and conventional wireless network security. Section 3 provides the IoT classification. Section 4 discusses the threats and vulnerabilities of the IoT. Section 5 describes the IoT security taxonomy. Section 6 provides an IoT security

scenario. Section 7 presents the discussions on possible attacks posed by the threats and vulnerabilities on the IoT. Section 8 offers future directions. Finally, Section 9 concludes the study.

2.0 Overview of IoT

The IoT has drawn attention recently because of the expansion of appliances connected to the Internet (Whitmore, Agarwal, and Da Xu, 2014 and Atzori, Iera, and Morabito, 2010). IoT simply means the interconnection of vast heterogeneous network frameworks and systems in different patterns of communication, such as human-to-human, human-to-thing, or thing-to-thing (Horrow and Anjali, 2012 and Al-fuqaha, Guizani, and Mohammadi, 2015). Moreover, the IoT is a realm where physical items are consistently integrated to form an information network with the specific end goal of providing advanced and smart services to users (Botta et al., 2016 and Da Xu, He, and Li, 2014). The connected "things" (for example, sensors or mobile devices) monitor and collect all types of environment data. They enable the collection of real-time data about properties, individuals, plants, and animals.

In the IoT model, sensor-equipped devices know how to deliver lightweight data around the physical world, authorizing cloud-based resources to extract data and make choices from the extracted data by using actuator-equipped devices (Borgia et al., 2016 and Weber, 2010), which enhance the communication among nodes. With the degree and size of the IoT components, the IoT applications have been improved using different methods, techniques, and models derived from device-driven-embedded frameworks (Mansfield-Devine, 2016). The IoT is required to address the problems related to the IoT application environments, such as real-time communication (Jutila, 2016), the presence of both sensor and actuator, and the distributed heterogeneous nature of the IoT. Different research groups have investigated the method of securing a wireless sensor network (WSN), which is a major component for developing constrained devices in the IoT (Borgia et al., 2016; Zhu, Leung, Shu, and Ngai, 2015; and Roman et al., 2011).

WSNs are ad hoc networks that are considered the major building blocks for the IoT devices. They are used for gathering data from their surrounding and delivering them to users and for accessing connected IoT devices remotely. They comprise an extensive number of small nodes that can detect, compute, and communicate with other devices (Bi, Wang, and Xu, 2016 and Frizzo-barker et al., 2016). The communication between the Internet and the sensor nodes should satisfy secrecy, trustworthiness, verification, and non-revocation (Li, Han, and Jin, 2016 and Gluhak et al., 2011). The privacy and security issues in the IoT differ from those in conventional and other wireless networks in terms of deployment and technology (Yinbiao et al., 2014). The IoT networks are deployed on low-power and lossy networks (LLN). LLNs are networks constrained by energy, memory, and processing power. Hence, lightweight encryption technology, which includes lightweight cryptographic algorithm, is used for securing the IoT environments. These aspects have not been considered for conventional and other wireless networks (Suo, Wan, Zou, and Liu, 2015).

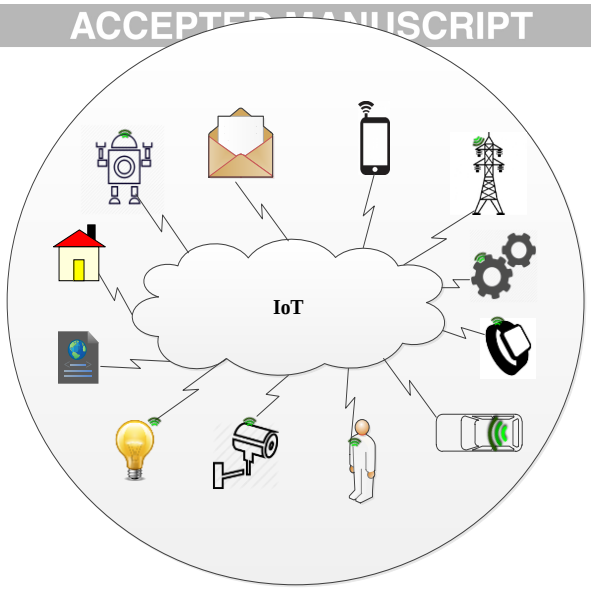


Fig 1: Landscape of IoT

2.1 IoT Security versus Conventional Security

Several key differences exist between the IoT and conventional wireless networks in terms of dealing with security and privacy. For example, the deployment of the IoT is unique compared to that of the normal Internet. The IoT devices are set up on LLNs, whereas others have extremely dynamic topologies that rely on the application. LLNs are strained by dynamism, memory, and processing power (Lu, 2014). These aspects are not considered for the standard Internet. LLNs experience great data losses due to node impersonation. For instance, in the process of data transmission, if an attacker can connect to the network using any identity, the attacker can be assumed an authentic node. In the case of smart meter applications, the readings can be manipulated by an attacker to send erroneous control messages (Lu, 2014).

The security features and requirements of both the IoT and conventional network devices are also different (Suo et al., 2015 and Yan et al., 2014). In the IoT perception layer, sensor nodes have limited computational power and low storage capacity, which make the frequency hopping communication application and public key encryption to secure the IoT devices impossible. Lightweight encryption technology, which includes lightweight cryptographic algorithm, is used for the IoT devices. The IoT network has security issues, such as man-in-the-middle and counterfeit attacks, in the network layer. Both attacks can capture from and send fake information to communicating nodes in the network (Zhao, 2013). Identity authentication and data confidentiality mechanism are used to prevent unauthorized nodes. At the application layer, data sharing is the main feature. Data sharing creates security problems in data privacy, access control, and disclosure of information (Zhang, 2015). The security requirements for the application layer include authentication, key agreement, and protection of user privacy across heterogeneous networks.

Furthermore, the communication protocols in both networks differ. Each layer in the networks has its own communication protocol. For example, IPv6 is used over low-power wireless personal area networks in the IoT perception/physical layer, whereas wireless fidelity is used in the physical layer in conventional networks. In the IoT network layer, Datagram Transport Layer Security (DTLS) is used as a communication protocol, whereas conventional network uses a transmission control protocol (TCP). Constrained Application Protocol (CoAP) is used in the IoT application layer for communication, whereas Hypertext Transport Protocol (HTTP) is used in the application layer of conventional networks (Milbourn, 2016).

In summary, the conventional security architecture is designed based on the perspective of users and not applicable for communication among machines. The security issues in both networks may be similar, but different approaches and techniques are used in handling each network security issue (Kai, 2016). In this survey, the security threats and vulnerabilities discussed are specific to the IoT devices.

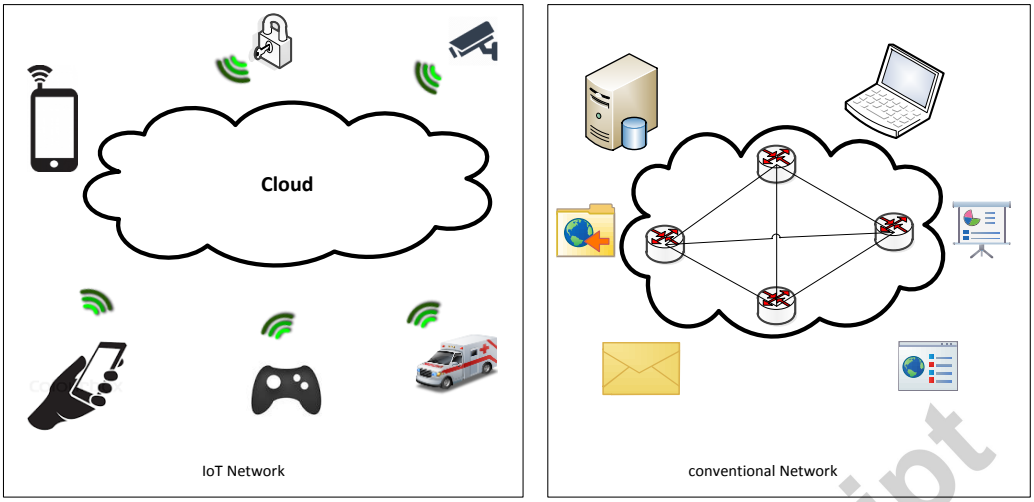


Fig 2: IoT Network vs. Conventional Network

3.0 Classification of IoT

The IoT can be classified into three layers (Zhao and Ge, 2013), namely, application, perception, and network protocol, as shown in Figure 3.

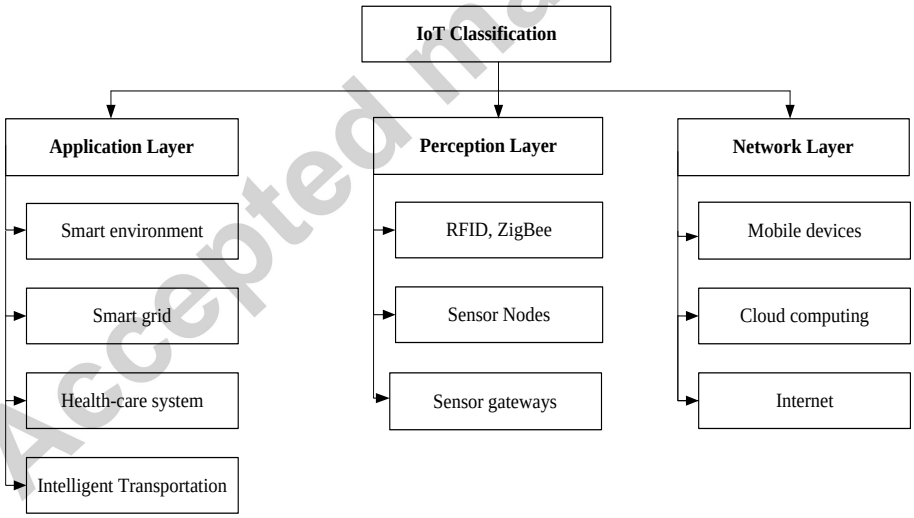


Fig 3: IoT classification

3.1 Application Layer

No universal standard for constructing the IoT application layer currently exists (Zhao and Ge, 2013). The application layer can be structured in several ways based on the service it offers. The application layer is the uppermost layer and is visible to the end user. Applications, such as smart grid, smart city, healthcare system, and intelligent transportation protocols, constitute this layer (Jing et al., 2014). An application layer protocol is distributed over multiple end systems, in which the application in one end system uses a protocol to exchange information packets with an application in another end system

(Oen, 2015 and Nolin and Olson, 2016). An application layer typically comprises a middleware, a machine-to-machine (M2M) communication protocol, cloud computing, and a service support platform. The security issues differ depending on the industry and environment (Valmohammadi, 2016).

3.1.1 Smart Environment

The integration of the IoT applications enables the conception of smart surroundings, such as smart cities. A smart environment combines the services provided by multiple shareholders and scales to support numerous users in a dependable and distributed way (Kotsev et al., 2016). They should be capable of working in both wired and wireless system environments and manage limitations, such as data access with restricted control and untrustworthy network. Numerous strategies, techniques, models, functionalities, frameworks, applications, and middleware solutions are identified with context awareness in an IoT smart environment (Ning and Liu 2015). The M2M communication among the IoT devices is thus less demanding and provides more important data that help in recognizing a situation or data (Perera, Zaslavsky, Christen, and Georgakopoulos, 2014). However, smart city devices are exposed to various threats and attacks, including smart city Denial-of-Service (DoS) attack, data manipulation, fake seismic detection, and fake flood detection (Zhu, Leung, Shu, and Ngai, 2015).

3.1.2 Smart Grid

A smart grid is an electrical grid that comprises different operational and energy measures, such as smart meters, smart appliances, renewable energy resources, and energy-efficient resources (Mahmood et al., 2016). The high demand for extended energy sources has led to the modernization of the traditional electrical distribution system that is beneficial to energy distribution. Smart grid is defined as a smart electrical distribution system that involves a wide range of electrical power functions, such as smart meters, smart machines, sustainable energy resources, and effective energy properties, which distribute energy flows from manufacturers to users in a bidirectional way. Smart grids serve as building blocks for energy management for a sustainable environment (Borgia, 2014). Smart grids are reliable, improve cost and savings, and enhance energy independence. Smart grid is vulnerable to different attacks and threats, such as customer security, physical security, trust among traditional power devices, endpoints on devices, and malicious attacks.

3.1.3 Healthcare System

The increasing cost of health maintenance and the frequency of prolonged diseases worldwide earnestly demand the reconstruction of healthcare services from the doctor facility-focused framework to an individual-focused environment, with attention on controlling the diseases and the health condition of patients (Moosavi et al., 2015). The framework is based on radio frequency technology that delivers general networking performances. E-health depends on the interrelationship of tiny nodes developed using sensing (detecting) and actuating (activating) capacities embedded inside or outside the human body (Abdmeziem and Tandjaoui, 2015). The applications are connection mindful, active, and personalized, and they depend on trusted channels for communication with connected devices. The rapid increase in the IoT services has prompted the requirement for modern approaches to handle heterogeneous devices, fluctuating availability, and data-creating behavior (Abdmeziem and Tandjaoui, 2015 and Aazam et al., 2016). Smart healthcare involves the use of smart health cards that protects the security and privacy of patients. However, smart health cards are vulnerable to threats and attacks, such as theft, loss, insider misuse, unintentional actions, hacking, internal attack, and cyber-attack (Aman and Snekkenes, 2016).

3.1.4 Intelligent Transportation

Information technology, vehicle manufacturers, and industries are a part of the IoT revolution through the creation of new types of products and systems by integrating several technologies and communication solutions, which include radio frequency identification (RFID) tags, sensors, and actuators, into newly developed systems (Kanuparthi, Karri, and Addepalli, 2013). The incorporation of detection innovations in passive RFID tags would enable completely novel functions in the IoT application domain, particularly in tracking locations and movement and monitoring temperature (Atzori, Iera, and Morabito, 2010). Dedicated Short Range Communication (DSRC) is communication system that consists of RSU and On Board Units (OBUs) with transceivers and transponders. It is mainly used for frequent data communication between vehicles-to-vehicle or vehicle-to-roadside infrastructure, for example, toll collection, and operate between the radio frequencies of 5.725 MHz and 5.875 MHz. Moreover, DSRC provides support for intelligent transport system through Electronic Fee Collection (EFC) application for toll collection. EFC is mostly used in United States and European Union countries such as Switzerland, Germany, Austria etc., (Bansal, Kenney and Rohrs, 2013).

EFC deployment in Europe is primarily based on the European DSRC 5.8 GHz technology, a standard developed by Comité Européen de Normalization (CEN) which is based on the European Telecommunications Standards Institute (ETSI) and the security standard is IEEE 1609.2. But these systems are currently incompatible in terms of technology, security, and charging principles. The tariff principle is one of the main reasons for the incompatibility in the classification parameters used and how the fee is calculated (i.e. whether it is based on network, distance or zone/congestion). For example, with respect to security, the use of different security mechanisms to protect the integrity of the data stored in OBU (Li, 2015). Hence, standardization is important in order to ensure interoperability, particularly for EFC applications, for which the European imposes a need for interoperability of systems.

Intelligent transportation deploys large scale WSNs to observe travel time online (i.e., from the starting point to the endpoint), routing decisions, queue lengths, air pollutants, traffic congestions, and noise emissions. Intelligent transportation involves traffic control, parking, and public transportation. Its ease-of-use enables different individuals to be well-informed and the secure, organized, and smooth use of intelligent transportation systems (Mishra, 2015 and Miorandi, 2012). However, intelligent transportation is also exposed to several types of threats and attacks, such as DoS, improper configurations, insecure transmission channel, congestion control, security and spectrum sharing. Table 1 compares the possible security threats in the IoT devices and the enabling communication technologies deployed in the application domain. The application domain includes smart environment, smart grid, healthcare system, and smart transportation.

Table 1: Comparison of security threat and communication channel in IoT application domain

Applications	Network communication	IoT devices	Type of Threat
Smart environment	Wi-Fi, Ultra-wideband, ZigBee, Bluetooth, LTE, LTE-A,	buildings, people	Authentication, Privacy, Eavesdropping, Authorisation
Smart grid	Wi-Fi, ZigBee, Z-Wave	Smart meters and Smart readers	Privacy, Eavesdropping, Physically attack, tampering
Health cares system	Bluetooth and ZigBee	Sensors, Smart wearable devices	Privacy, authentication authorization, DoS,
Intelligent transportation	DSRC 5.8 GHz	EFC, RSU, OBUs	Jamming, Congestion, security and spectrum sharing

3.2 Perception Layer

The perception layer involves the collection of information. This layer is classified into two sections, namely, the perception node (sensors, controllers, and so on) and the perception network that interconnects the network layer (Tsai, Lai, and Vasilakos, 2014). Data are acquired and controlled at the perception node, while control instructions for sending and controlling data are carried out at the perception network layer. Perception layer technologies include all types of sensors, such as RFID, ZigBee, sensor nodes, and sensor gateways (Jing et al., 2014).

3.2.1 RFID

RFID technology is the main revolution in the embedded communication model that facilitates the configuration of microprocessors for wireless communication. Two types of RFID tags exist, namely, active and passive (Atzori et al., 2010). Active RFID tags have their power source. They are almost the same as the lower end nodes of WSNs in terms of limited processing capability and storage. These tags provide signals to readers regardless of their distance and their battery supply is capable of providing instant communication. Active RFID devices have constrained life spans. On the contrary, passive RFID tags are not powered by battery. They use the power from the inquiry signal of the reader to establish communication from the tag to the RFID reader. They are used in many applications, such as bank cards and road toll tags. Passive RFID tags are tiny and have a virtually unconstrained life span. The major features of RFID tags are auto identification and the unique identity that includes the rapid exchange of information between tags and readers through wireless connections. The possible threats to and attacks on RFID include tracking, DoS, repudiation, spoofing, eavesdropping, data newness, accessibility, self-organization, time management, secure localization, tractability, robustness, survivability, and counterfeiting (Jing et al., 2014).

3.2.2 Sensor Nodes

A sensor node can gather and process sensory data and interconnect with other nodes in the network. Sensor nodes have the following components: (i) a controller that executes data processing and controls the performance of other parts in the node, (ii) a transceiver that transmits and receives radio frequencies, (iii) a program memory that is used for programming the device, (iv) a power source that supplies power to the nodes, and (v) hardware that is used to capture data from the environment (Wu et al., 2014). The major components of a sensor node are the sensors and actuators that are used for sensing and activating devices based on the commands sent from the nodes. The sensor node is flexible and has high latency in communication. Nonetheless, sensor nodes are vulnerable to different threats and attacks, which include node subversion, node failure, node outage, passive information gathering, false node message corruption, exhaustion, unfairness, Sybil, jamming, tampering, and collisions (Zhang, Shen, Wang, Yong, and Jiang, 2015 and Massis, 2016).

3.2.3 Sensor Gateways

Sensor gateways deal with wireless network and collective data from various distributed WSN nodes. Every gateway includes a 2.4 GHz IEEE 802.15.4 radio for communication. WSN involves the collection of dedicated transducers with a communication framework for checking and recording the conditions of any sensor device at different positions/locations. The following parameters are checked regularly: temperature, humidity, pressure, wind direction and speed, light strength, vibration strength, sound strength, power-line voltage, chemical concentrations, pollutant levels, and dynamic body functions. The wireless communication channel involves radio communication, transmitters, and receivers for the data exchange between two or more devices. This channel enhances user access, network expansion, mobility, and collaboration. Nevertheless, this channel leads to several threats and attacks, such as misconfiguration, hacking, signal lost, DoS, war dialing, protocol tunneling, man-in-the-middle attack, interruption interception, and modification fabrication (Liu et al., 2016).

Table 2 compares the IoT communication channels from a security perspective with focus on the most common technologies used in the IoT, such as RFID, sensor nodes, and sensor gateways.

Table 2: Comparison of IoT communication channel regarding security

Type of Security	RFID	Sensor nodes	Sensor gateways
Encryption	Weak	Fair	None
Authentication	Fair	Strong	Strong
Authorization	Fair	Strong	Strong
Privacy	Fair	Fair	Weak

3.3 Network Layer

The network layer provides network transmission and information security and delivers pervasive access environment to the perception layer, that is, data transmission and storage awareness. The network layer includes mobile devices, cloud computing, and the Internet (Pongle and Chavan, 2015).

3.3.1 Mobile Device

A mobile device (e.g., tablet or laptop) is a portable device with an operating system (OS) that can run applications, such as business, enterprise resource-planning, and finance applications. Most portable devices are equipped with Wi-Fi, Bluetooth, Near-Field Communication (NFC), and Global Positioning System (GPS) capabilities that allow connections to the Internet and other devices. Mobile devices can also be used to provide location-based services (Bohge and Trappe, 2013). Smartphones and personal digital assistants are suitable for users who want to utilize some of the conveniences of a traditional PC at a location where moving one would be impractical. Digital business partners can further enhance the accessible components for business users by integrating data capture devices, such as barcode, RFID, and smart card readers (Laghari and Niazi, 2016). Nevertheless, mobile devices are vulnerable to threats and attacks, such as tracking, eavesdropping, DoS, bluesnarfing, bluejacking, bluebugging alteration, corruption, and deletion (Bekara, 2014).

3.3.2 Cloud Computing

Cloud computing is Internet-based distributed computing that provides common data processing for different devices based on a set of requirements. This distributed computing is a model for enabling pervasive, suitable on-demand network access to a common pool of developing computing properties (e.g., servers, systems, storages, functions, and utilities). In the IoT, cloud computing technology has made the task of processing the large amount of data produced by communicating devices easy and provides the IoT devices with resources on-demand (Horrow and Anjali, 2012). This technology also provides high computing power, low-cost services, high performance, versatility, and openness for device accessibility (Botta et al., 2016). However, cloud users face many security threats and vulnerabilities, including identity management, dynamic change in the IoT devices (heterogeneity) that makes transmitted data inaccessible to an authentic node, data access controls, system complexity, physical security, encryption, infrastructure security, user identity, a management approach to security, and misconfiguration of software (Horrow and Anjali, 2012).

3.3.3 Internet

The Internet is the global arrangement of interconnected computers that uses the traditional Internet protocol (IP) suite (TCP/IP) to connect billions of devices globally. This arrangement consists of a network of networks, such as private, public, academic, business, and government networks, from a local to a worldwide scope that are connected by an extensive collection of electronic, wireless, and optical networking technologies (Bahtiyar and Ufuk Çağ layan, 2012). A broad range of information and services are provided by the Internet, such as the connection between hypertext files and the World Wide Web application, e-mail, communication, and distributed systems for document sharing (Islam et al., 2015). The Internet communication framework consists of hardware components and software layers that control various aspects of the framework. The Internet serves as a platform for millions of constrained devices connected to communicate and share resources (Mazlan, 2014). However, the Internet is exposed to several common security and privacy challenges, such as confidentiality, encryption, viruses, cyberbullying, hacking, identity theft, reliability, integrity, and consent (Akhunzada et al., 2016).

4.0 Threats and Vulnerabilities of the IoT

In this section, related works that focus on the threats and vulnerabilities of the IoT are discussed to explore the various types of existing security solutions for the IoT. The related works specifically focused on security solutions for the threats and vulnerabilities of the IoT architecture and their applications.

Several specific solutions for the IoT architecture and applications have been proposed in the literature (Granjal, Monteiro, and Silva, 2015 and Guo, Chen, and Tsai, 2017). A secure IoT architecture for smart cities that addresses the vulnerabilities in traditional IoT systems was proposed by Chakrabarty, Engels, and Member (2016) and Haroon et al. (2016). The architecture comprises black networks and a Key Management System (KMS) that provide confidentiality, integrity, privacy, and efficient key distribution. The aim was to deliver security services that mitigate the vulnerabilities of the IoT networks at the link and network layers, specifically for mission-critical data. The drawbacks of this approach include lack of privacy solution for defining device location and new routing challenges for the IoT nodes created by header encryption that are asleep, which leads to data loss.

Valdivieso et al. (2014) and Akhunzada et al. (2016) proposed a SDN architecture for developing the IoT applications to eliminate the inflexible security nature of traditional networks. A SDN architecture was adopted to provide a basis for developing a secure network OS that allows administrators to have a global view of possible threats to and attacks on the IoT network and provide them the privilege to control the network against the threats. Nevertheless, security, scalability, and reliability are some of the drawbacks of SDNs. The separation of the control and data planes of a SDN causes poor performance in packet processing, which in turn leads to significant problems, such as packet delay or loss and distributed DoS (DDoS) attack.

Similarly, a novel SDN-based security architecture for the IoT, also known as the SDN domain using border controllers, was proposed by Flauzac, Gonzalez, and Nolot (2015). The authors described how SDN could be used to interconnect heterogeneous IoT devices, how the security of each domain could be enhanced, and how the security rules could be distributed without compromising the security of any domain. However, the authors were not able to address the challenge of securing both wanted and unwanted traffic and enterprise protection, which are the major drawbacks of using border controllers.

Abdmeziem and Tandjaoui (2015) proposed a novel lightweight key management protocol. The protocol depends on the association of different IoT security components to set up a secure and protected communication channel for constrained nodes and wireless things. During data transmission along the channel, the protocol guarantees data confidentiality and

constrained node authentication. However, the security protocol is limited to offloading heavyweight cryptographic primitives to unwanted parties and does not specify the necessary tradeoff between the communication overhead and the number of third parties.

Hernández-Ramos et al. (2015) focused on a lightweight validation and authorization security framework for constrained smart objects. The objects/devices in the proposed security framework are compliant with the recent IoT Architectural Reference Model project presented by the EU FP7 IoT-A Project. The framework subsequently intends to propose a general security method for developing novel lightweight security protocols in the IoT. Nonetheless, the authors did not integrate the proposed framework into the constrained IoT environments for authentication, authorization, and defining alternative procedures to evaluate its correctness.

Neisse et al. (2015) proposed SecKit, a security toolkit for integrating a management framework for the IoT devices. The security toolkit aims to collect meta-models and provide a foundation for developing the IoT security engineering tools, add-ons, runtime components, and extensions to address the security, data protection, trust, and privacy requirements for the constrained IoT environment. The framework also enables and enhances cross-domain security configuration and interoperability. One drawback of this approach is that it does not provide a design analysis on how to deploy security and privacy solutions for devices operating in a dynamic environment. Another drawback is that data safety is not guaranteed as malicious attackers could easily take over the IoT actuators and send incorrect information to influence the data transmission process between connected devices.

In this survey, several specific solutions to the threats and vulnerabilities of the IoT architecture and applications are examined and discussed. However, instead of developing individual solutions for separate architecture and application scenarios, we believe that the IoT applications can be secured through adopting a universal IoT security architecture by considering the proposed IoT security solutions in this survey. To the best of our knowledge, none of the existing security techniques has the following IoT architecture properties:

- A privacy solution for defining node locations and handling new routing challenges created during the header encryption for the IoT nodes that are asleep (i.e., a secure IoT architecture that helps in addressing translations, defining location privacy, and characterizing mobility should be designed to achieve this goal)
- A simple symmetric cryptography solution to third parties at the constrained nodes for offloading
- Handling poor performance in packet processing as a result of separating the control and data planes in the SDN (i.e., the only way to improve the SDN performance is to ensure the integration of the control and data planes, so that the SDN technology can use applications, such as encryption, analysis, and traffic classification)
- Allowing the constrained nodes to dynamically set up a shared key with any wireless things with which no previous shared knowledge has been established (third parties are dedicated to supporting the constrained nodes in this process to reach this goal)
- Guaranteeing an E2E code where no entity has the knowledge of the exchanged secret apart from the constrained nodes and the wireless things

In fact, developing a generic security solution for a wide range of IoT applications and that is backward compatible with existing solutions is safer (Bonetto et al., 2012).

In the next section, our newly designed IoT security taxonomy that includes application, architecture, communication, and user is presented and elucidated.

5.0 Taxonomy of the IoT Security

The existing IoT security approaches discussed in Section 3 indicate the need to design a new security taxonomy that is simple and more specific to categorizing classes of security threats and vulnerabilities in each IoT application domain. We therefore specify the functionalities and performances of each domain on different threats and vulnerabilities and explain how security countermeasures may improve the security services in any IoT application domain.

The security information profile of the IoT devices always changes as a result of new security threats imposed on the devices. In spite of the fact that the implementation of technological solutions may react to the IoT threats and vulnerabilities, the security for the IoT is a significant management issue. The effective management of the threats related to the IoT requires a sound and thorough evaluation to mitigate known threats in the IoT environment (Covington, 2013). The taxonomy for the IoT security must provide a comprehensive analysis of the security mechanisms, including the services and the attacks, and how all of their components work to provide system developers and analysts the necessary information to design and analyze secured systems (Whitmore, Agarwal, and Da Xu, 2014).

The IoT security taxonomy presented in this survey is an effort to address several of the faults and shortcomings of previous works. Considering that our taxonomy attempts to map the existing security attacks to security services, we use the list of security services proposed by Akhunzada et al. (2016) as one of the axes of our taxonomy.

The proposed taxonomy helps build a security framework for the IoT in a heterogeneous environment. The IoT security taxonomy will definitely help in the security evaluation for the IoT, which is a critical issue (Mahalle, Babar, Prasad, and Prasad, 2010 and Babar et al., 2015). The proposed taxonomy will be used as a framework that will systematically examine some new unknown vulnerabilities and attacks in the IoT networks. This taxonomy will help security developers develop security models for constrained devices and provide a valuable information tool for security analysts.

The first step in developing our taxonomy is building a new classification of the application domain, architectural domain, communication channel, and data domain for the IoT. We then introduce a new matrix taxonomy for the IoT security that relates each classification to its appropriate components. Finally, we discuss and analyze each security component, evaluate its impact, and link it to one or more possible security countermeasures, as shown in Figure 4.

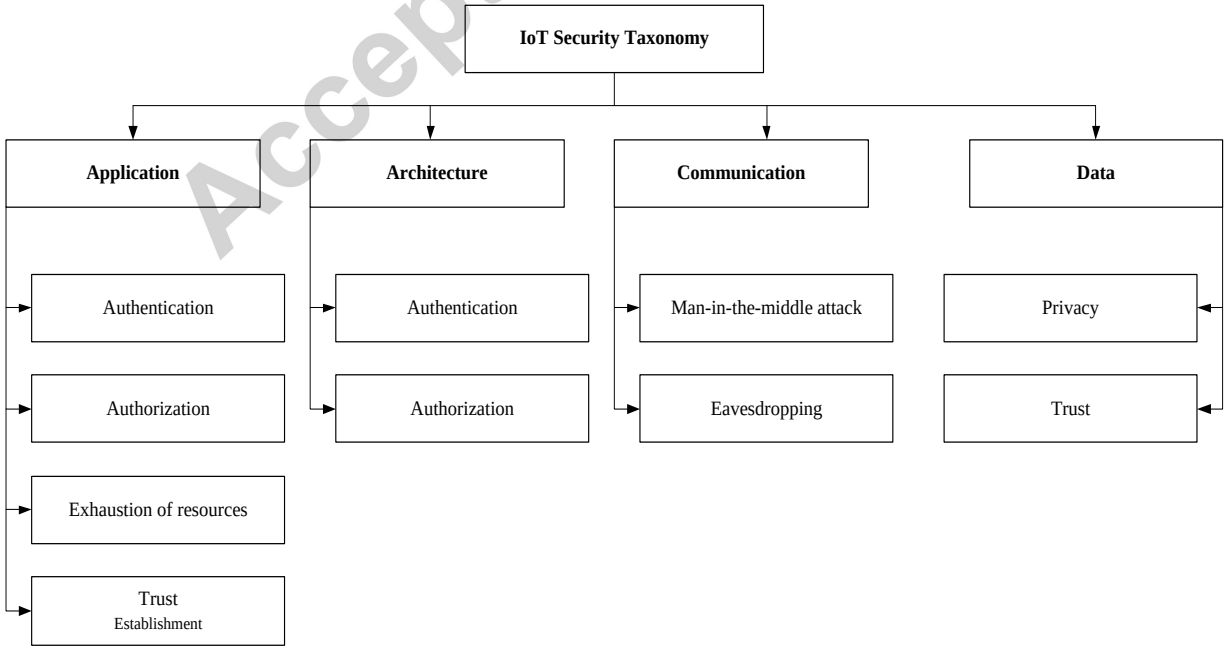


Fig 4: IoT Security Taxonomy

5.1 Application

Numerous application areas will be affected by the IoT development. Applications are categorized based on the type of network accessibility, scope, scale, heterogeneity, repeatability, and user involvement (Gubbi, Buyya, Marusic, and Palaniswami, 2013). Several security techniques exist, as shown in the IoT security taxonomy. The most commonly used security techniques that are considered with the use cases in this application domain are (i) authentication, (ii) authorization, (iii) exhaustion of resources, and (iv) trust establishment. The summary is provided in Table 3.

Table 3: Summary of different IoT security technologies

Reference	Technologies	Objectives	Advantages	Limitations	Domain
Gubbi et al. (2013)	Cloud implementation using Aneka computing platform	To determine the current IoT application trends and the requirement for merging different interdisciplinary technologies	It utilizes storage and system resources together with public (open) and private clouds. It supports the provision of resources for public clouds, such as Microsoft Azure, GoGrid clouds, and Amazon EC2.	Security and personality protection is a serious issue in hybrid clouds.	Smart environment
Yao, Chen, and Tian (2014)	Lightweight no-pairing attribute-based encryption (ABE) scheme based on elliptic curve cryptography (ECC)	To address the security and privacy problems in the IoT To reduce computation and communication overhead	ABE is applicable in cipher-text-based access control and broadcast encryption.	Poor scalability Poor flexibility in revoking attribute	Single-authority applications
Jiang, Shen, Chen, Li, and Jeong (2015)	Revised secret-sharing scheme (Shamir's secret-sharing scheme)	To achieve data scalability To reduce complex key management related to conventional cryptographic algorithms To deliver reliability feature at the data level	Scalability is achieved with Shamir's secret-sharing scheme.	It generates computational overheads that bring potential bottlenecks. Hardware failure leads to the issue of fault tolerance.	Data mining and analytics
Aazam et al. (2016)	Resource estimation and management using fog computing	To propose a probabilistic resource estimation model of customer for fogs	Fog permits real-time data delivery. Fog brings cloud properties to the edge of the basic IoT and other end nodes.	Minimum latency is difficult to achieve.	Healthcare
Bose et al. (2015)	Lightweight scheme to secure channel establishment	To regulate the amount of privacy from the fine-grained sensor information To save the	It influences the relationship between the privacy and the security of sensor datasets. It offers E2E adaptive	It can only consider a single security scenario (i.e., sensitivity).	Smart energy meter

	protection content through secure exchange of information	and improved security with minimum resource consumption.

5.1.1 Authentication

In the IoT application domain, authentication allows the integration of different IoT devices and their deployment to various smart environments, such as smart cities. A smart environment can merge different services provided by different multiple shareholders and scales to support numerous users in a dependable and distributed manner (Martín-Fernández, Caballero-Gil, and Caballero-Gil, 2016). Authentication involves validation among routing peers of connected IoT devices before exchanging the route information (known as peer authentication) and guaranteeing that the source of the route data is the connected peer devices (known as data origin authentication). This validation helps enhance the primary element in the IoT vision, which is M2M communication (Perera et al., 2014). A broad range of techniques and middleware solutions that make M2M communication easy are identified with framework responsiveness in the IoT.

Gubbi et al. (2013) focused on a common authentication scheme for the IoT between different layers and terminal nodes. The scheme is based on hashing and element extraction. The extracted element is mutually shared with the hash function to dodge any jamming attacks. This scheme essentially provides a good security solution for the authentication in the IoT. The extraction procedure comprises some irreversibility properties (which are lightweight) that guarantee the security of connected things in the IoT domain. The scheme emphasizes the authentication process among different IoT layers that send data to terminal nodes and not the reverse. The claim that the scheme would enhance data security was based only on theory and no practical proof was presented to support it.

Ndibanje et al. (2014) proposed a security analysis and authentication and access control improvements for the IoT. Their work primarily broke down current authentication and access control approaches and proposed a practical protocol for the IoT. A simple, efficient, and secure key establishment based on Elliptical Curve Cryptography (ECC) for the authentication protocol was used to improve device authentication. A Role-Based Access Control (RBAC) was also introduced for the access control policy on applications associated with the IoT network. Nevertheless, the communication overhead for the IoT sensor nodes was high, and practical experiments on the proposed security valuation were not performed.

Ye et al. (2014) introduced an efficient authentication and access control technique. Their technique was based on a general perspective of the security issues for the IoT perception layer. This technique creates a session key that is based on ECC, which improves the mutual authentication between user and sensor nodes. However, this technique only solves the authentication issues in the IoT perception layer and does not address the attribute-based access control policy among devices.

Neisse et al. (2015) proposed an identity authentication model for the capability based on access control for the IoT. A public key technique is employed in the proposed model, which is suitable for lightweight security approaches, mobile/portable devices, distributed devices, and constrained IoT devices using different communication technologies, such as Bluetooth, 4G, WiMAX, and Wi-Fi. This approach uses timestamp as part of the authentication message among communicating devices to prevent MitM attacks. The identity authentication in this approach is carried out in three sequential phases.

- Key generation phase: In this phase, a secret key that is based on the ECC-Diffie–Hellman algorithm is generated.

- Establishment phase: This phase involves establishing the device identity after generating the secret key. Identity establishment is conducted by either one-way or mutual authentication protocol.
- Implementation phase: This final phase grants access control to authenticated devices to communicate with one another.

Although the model does not prevent DoS attacks completely, it reduces the risk because resource access is granted to only one ID at a time (Mahmoud et al., 2016).

Al-turjman and Gunay (2016) introduced a lightweight authentication protocol to secure RFID tags. The perception layer of the IoT involves devices, such as RFID and sensors. These devices are constrained in nature, and their computational capability is limited. These characteristics pose a problematic issue to the application of any cryptography algorithms to guarantee the IoT network security. When the RFID is insecure, an attacker can easily gain access to the network through sniffing and reprogramming the electronic product code tag of the victim. This attack can be avoided by applying an authentication protocol on the tags. The authentication protocol safeguards the combined authentication between RFID readers and tagged items with minimum computation overhead on the devices.

5.1.2 Authorization

Authorization involves specifying access rights to resources, such as healthcare devices, related to information security and access control. E-health depends on the interrelationship of tiny nodes developed using the sensing (detecting) and actuating (activating) capacities embedded inside or outside the human body. E-health applications are connection mindful, dynamic, individual, and dependent on trust.

The data should be secure and accessible to authorized users only. In the IoT, users can be humans, machines, services, internal objects (i.e., devices within the network), and external objects (i.e., devices outside the network). For instance, sensors should not expose the collected data to an unauthorized neighboring node (Abdmeziem and Tandjaoui, 2015 and Aazam et al., 2016). One more authorization issue that must be addressed is how data is managed and controlled in a heterogeneous IoT environment. The users of the IoT should know about the data management mechanisms that will be applied and the procedure or administration, and guarantee that the data are protected all throughout the procedure (Moosavi et al., 2015).

Gaur et al. (2015) proposed ID authentication at the IoT sensor nodes. The approach was based on the one-time cipher request–reply scheme. The scheme uses a pre-shared matrix by applying a dynamic variable cipher when communication involves multiple parties. The communication parties create a random coordinate that serves as the key (i.e., password) coordinate. Every communication (messages) among parties is encrypted using a key and node ID together with a timestamp. The communicating parties communicate by authenticating the timestamps, and they could also use the timestamp to cancel a session. However, this approach is only efficient in an IoT domain where securing things is not exceptionally delicate and significant because the key can be rehashed for various coordinates. If the password is changed consistently, then the security could be enhanced for that specific IoT framework. The establishment of the pre-shared matrix needs to be secure for this work to be implemented in an extensive number of IoT devices.

5.1.3 Exhaustion of Resources

The high demand for ubiquitous resources, such as energy sources, can add to the current system resources and greatly influence the performance of different applications, which can in turn lead to resource leakages and overloading in the IoT (Borgia, 2014). Bekara (2014) indicated that resource-exhaustion vulnerability is a particular type of fault that causes the

consumption or allocation of some resources in an undefined or unnecessary manner or the incapability to release it when no longer required, which eventually causes its depletion.

Resource depletion attacks drain the energy of target IoT nodes by introducing routing loops and extending the path during packet transmission. Routing protocols are vulnerable to resource depletion attacks (Raju, 2014).

Resource exhaustion also occurs in places where an attacker transmits consistently high volumes of packets from one or more attack nodes. In this case, all the sensor nodes that are within the transmission range of the attack nodes are possible targets and their batteries are subject to intentional exhaustion. The degradation of batteries is accelerated if the packets from the attackers elicit a transmitted response time from the target nodes. This degradation occurs, for example, when the target nodes choose to forward the packet to other nodes in the WSN. Resource exhaustion attacks that are executed in this manner are more severe than other DoS attacks because more sensor nodes become unavailable at the same time and the nodes may be isolated in sub-networks that cannot communicate with one another (Botta et al., 2016).

5.1.4 Trust Establishment

A convincing trust mechanism must be available to establish trust between the IoT physical objects and events, such as interconnected WSNs, RFID-based systems, and mobile phones (Akhunzada et al., 2016). Sensitive user information that are stored in the application server can be compromised, which can subsequently lead to forging legitimate user credentials in the network. Mechanisms to verify network devices exist. However, convincing mechanisms for establishing trust in verifying network applications do not exist. Therefore, trust establishment is crucial for suitable interoperability among devices. Trust involves the preservation of user privacy, such as personal user data, by the policy and prospect of the IoT users in a flexible manner (Josang, Ismail, and Boyd, 2012). Given that the IoT devices are portable and mobile in nature, the devices can be moved physically from one owner to another; thus, trust should be established between both parties to allow the smooth movement of the devices in terms of access control and authorization. Atzori et al. (2010) introduced a model of mutual trust in the system security in the IoT by developing an item-level access-control framework. The framework establishes trust among the connected IoT devices during data transmission. The authors used key creation and token as the mechanisms for establishing trust in this model. The mechanisms guaranteed the authorization among communicating devices by assigning creation keys and tokens to the IoT devices during data transmission.

5.2 Architecture

No universally acceptable IoT architecture currently exists (Chen et al., 2011). Several research types have been conducted on the IoT architecture in different scenarios and application domains in terms of authentication and authorization. Table 4 provides a summary of existing IoT architectures and application domains.

Table 4: Different IoT security architecture types and application domains.

Reference	Architecture	Application Domain	Objectives
Valdivieso et al. (2014)	SDN Architecture	Smart environment	To eliminate the rigidity present in traditional networks.
Moosavi et al. (2015)	SEA Architecture	Healthcare	To improve the secure and efficient verification and authorization framework for IoT-based healthcare systems.
Gaur et al. (2015)	Smart City Architecture	Smart City	To ease the interaction of remote sensor systems and data with

			communication technologies.
Ramão et al. (2015)	Service-Oriented Architecture (SOA)	Smart transportation	To define secure the IoT middleware architecture services. To analyze and deliberate on the security services that can be applied to the IoT middleware.
Vucinic´ et al. (2015)	OSCAR: Object Security Architecture	Smart grid	To introduce a novel scalable security architecture for E2E security and access control in the IoT. To evaluate the architecture in constrained M2M settings.
Vishvakarma et al. (2015)	Conceptual Organizations Framework	Business organizations	To identify the two types of the IoT architectures for an organization: cloud-centric three-layered and autonomic-oriented, five-layered architectures.
Chakrabarty et al. (2016)	Black SDN Architecture	Smart City	To address the vulnerabilities in traditional IoT systems.

5.2.1 Authentication in IoT architecture

Valdivieso et al. (2014) adopted the SDN architecture that helps eliminate the rigidity in traditional networks. SDNs allow administrators to have a global perspective of the system and the ability to control the network according to the requirements of each organization. SDNs simplify network utilization and operation by lowering the total cost of organization networks by providing programmable network services. However, several security vulnerabilities exist in SDNs. The lack of sophisticated authentication and authorization mechanisms makes SDN controllers the fundamental focus of hackers because they serve both as the central point of control in the network and the possible central point of disaster. For example, if a user is not focused on the controller, the controller becomes the target of an attacker who can effortlessly compromise it by altering the user's code base. The attacker can also rescript the user's traffic control such that confidential data can be sniffed by the attacker.

Moosavi et al. (2015) proposed a type of distributed smart e-health gateway architecture for IoT-based health-care systems. This architecture type depends on the certificate-based DTLS handshake protocol, which is the basic IP security solution for the IoT. The proposed architecture utilizes both public key-based authentication and ECC primitives, such as the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Diffie–Hellman (ECDH). ECDSA employs the key exchange protocol in the DTLS handshake to provide data authentication and integrity, whereas ECDH is adopted in an unsecure communication environment for confidential data exchange. ECDH and ECDSA are more efficient in terms of securing constrained devices than an asymmetric cryptographic algorithm (RSA). This architecture type can adapt to different security challenges in general healthcare systems, such as scalability, trust, and consistency. One drawback in the proposed

architecture is DoS attacks. A sample scenario is the IoT heterogeneous medical domain where the IoT-based healthcare system functionality depends on a centralized delegated server. The server can be compromised easily in a DoS attack, which allows an attacker to access and retrieve all available stored data in the constrained medical domains. Another drawback is the issue of privacy in IoT-based healthcare applications. The techniques utilized in the proposed architecture do not support the privacy assurance re-used on constrained devices because of the security level requirements.

Ramão et al. (2015) focused on defining a type of classic security architecture for SOA-based IoT middleware systems, which provide support for the heterogeneity and interoperability of IoT devices, information management, and security. SOA-based procedures also provide the IoT applications with an identical and organized reflection of services and conversation with the IoT devices. SOA-based methods provide a uniform and controlled abstraction of services between the IoT devices and guarantee the confidentiality, integrity, and protection of communication channels. The major function of SOA is to prevent unauthorized access through the authentication features, such as trust and identity management, because that are incorporated in the architecture. However, lightweight security solution compatibility is a major challenge in SOA-based methods. Lightweight solutions, such as key management, authentication, and access control, are considered as critical issues, particularly in IoT resource-constrained environments. In addition, the authentication protocols among the IoT devices were not addressed, thus creating a room for unauthorized users to attack the communication channel.

5.2.2 Authorization in the IoT architecture

Authorization in the IoT architecture is attained by exchanging identified data between connected items. This procedure is vulnerable to eavesdropping, which can lead to a Man-in-the-Middle (MitM) attack that risks the entire IoT framework (Sezer et al., 2013 and Karlof, 2013).

Vucinic´ et al. (2015) proposed OSCAR for E2E security in the IoT. OSCAR was evaluated in two ways: (1) utilizing 802.15.4 LLN and M2M communication on two different hardware types and (2) utilizing MAC layers on a real testbed and applying the Cooja emulator. This architecture type utilizes authorization servers to grant access to users, which permits users to demand resources from the CoAP nodes. OSCAR has a security feature that supports multicasting. This feature provides authorization for E2E security. However, the drawback of this framework is the latency of ECDSA authorization, which largely affects the microcontroller unit and computation capabilities of the IoT devices. This scenario allows unauthorized users to control the entire system.

5.3 Communication

The IoT communication involves information exchange/sharing among the IoT devices or between different IoT layers. With the enormous potential of the IoT in many domains, the entire IoT communication infrastructure is inconsistent from the security perspective and vulnerable to privacy loss from the perspective of end users (Hashem et al., 2016). The IoT communication medium serves as a decision point for attackers. The possible attacks in the channel are described as follows.

5.3.1 MitM attacks

Attacks similar to MitM must be prevented to maintain data integrity during a conversation. In MitM, an attacker silently transmits and probably modifies the communication between two IoT devices that directly communicate with each other. Reliable information, such as patient health status, billing information of smart grids (SGs), or even secret keys of house doors, can be forged and altered by an attacker with MitM, thus causing serious security problems (Han et al., 2015). MitM attacks represent a genuine threat to the IoT security because they provide an attacker with the capability to seize and control a communication channel. Therefore, attackers can access sensitive data in real-time communication between nodes and obtain control over the channel. The attacker then forms a connection to the actual node and acts as an intermediary to read,

redirect, insert, and modify the traffic between the user and the authentic node. For example, an attacker may want to fake the temperature information from a monitoring device within the IoT to compel the device to overheat, which can stop the device from working. This action can cause inconvenience to the device and can also lead to physical damage and financial losses (Simko, 2016).

MitM attacks create challenges in protecting data security and privacy. The security problem in the IoT generally involves active interference by intruders on the devices (i.e., allowing unauthorized users to spy on data through the backdoor). Lightweight cryptographic protocols are considered to provide communications security for the IoT devices over a computer network as part of the DTLS. However, MitM attacks take advantage of the flaws in the authentication protocols utilized by the communicating parties (Mahmood et al., 2016).

5.3.2 Eavesdropping

Eavesdropping is an interception of information between two communicating nodes. Eavesdropping occurs on the network layer in the IoT and takes the form of data sniffing. A particular program is utilized for sniffing and recording packets from the network layer, which are subsequently listened to or read utilizing cryptographic tools for analysis and decryption. Privacy is employed as a method for providing efficient access control and security against eavesdropping during data communication (Vučinić et al., 2015). Eavesdropping also poses unique challenges to the IoT architecture, particularly when an attacker targets the communication channels to extract data from the flow information. This attack type is performed by listening directly to the message or data sniffing (Pongle and Chavan, 2015).

Thus, MitM and eavesdropping attacks in the IoT occur among dynamic sensor nodes that do not require a dedicated centralized server, unlike the conventional network where a dedicated server is employed for traffic control and monitoring (Kothmayr, Schmitt, Hu, Brnig, and Carle, 2013).

5.4 Data

The users' privacy and trust must be protected for the IoT to be fully deployed and completely accepted. Data privacy and confidentiality for business procedures are still critical issues, and finding practical solutions remain challenging (Botta, de Donato, Persico, and Pescapé, 2013). User data privacy must be guaranteed because users require maximum protection for their personal information. Trust involves the preservation of user privacy, which includes personal user data, by the policy and prospect of users in a flexible manner. Transmitting and computing trust among different nodes in a heterogeneous IoT is a challenging issue because different network nodes have different trust criteria (Eschenauer, 2012).

The security services provided by IEEE 802.15.4 are data authenticity, data confidentiality, and replay protection. The main threats to this protocol are encrypted ACK frames, NO timed frame counters, and NULL security level. When the ACK frame is unencrypted, an intruder can intercept a MAC frame and forge an ACK frame with a sequence number, which results in frame loss with no retransmission (Chakrabarty et al., 2015). Table 5 provides a summary of the existing threats within each IoT security communication layer of the IEEE 802.15.4-based protocols.

Table 5: Summary of security threats within each IoT layer

Layers	Threats
Physical	Micro-probing, tampering of hard components, jamming
Link	Collision, unfairness, exhaustion, replay, meta-data attacks
Network	Neglect, greed, homing, misdirection, traffic analysis, black holes, meta-data attacks

6.0 IoT security scenario

After a comprehensive research and survey on the security threats and vulnerabilities of the IoT as discussed in the previous sections, we know that security and privacy issues must be addressed for the IoT to be fully deployed in different domains at a large scale. The IoT environment involves different technologies and communication standards; no unified standard policy regarding security and privacy requirements currently exists (Chen et al., 2011). A well-defined security and privacy policy must be designed and deployed to guarantee confidentiality, access control, and privacy for users and items. Given the security flaws and lack of standardization in the IoT environment, we propose a conceptual type of architecture that can help mitigate the security challenges posed on items to an extent. Figure 5 shows a novel type of physical IoT security scenario architecture.

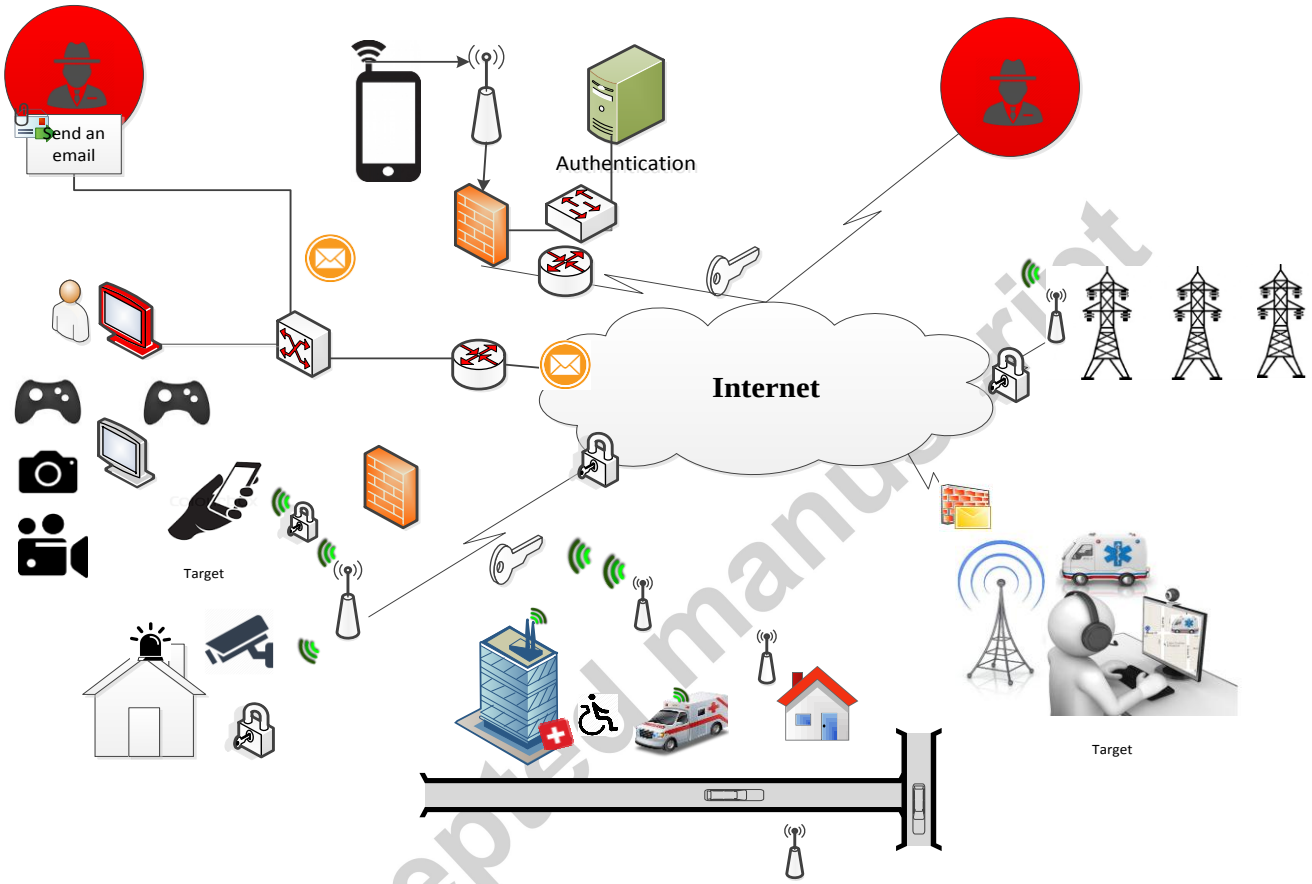


Fig 5: IoT security scenario.

Figure 5 shows an IoT security scenario where multiple devices and sensors communicate with each other in a secure environment. A virtual healthcare system is considered to illustrate the communication between different users. Suppose a user with a healthcare device is at home and must contact a hospital to ask for assistance. The user cannot go to the hospital to see the doctor in person because of his/her health condition. Thus, the user simply calls or sends an email to the hospital from home to avoid the stress of traveling to the hospital. The home and hospital network comprises multiple sensors/wireless devices as shown in Figure 5. Given the availability of wireless technologies, such as imo and Skype, that support video calls, both the user and the doctor can now make video call connections that can help the doctor assist the user.

The user mobile device and information and the hospital information that utilize different networks and devices are left open or exposed to hackers, as shown in Figure 5. Apart from the available security in current networks, the security characteristic requirements for resource-constrained devices during communication must be focused on. However, current networks cannot

inadequately satisfy the security requirements of sensitive data applications. Network and device security are two major requirements that must also be considered when designing the security architecture for constrained devices (Akhunzada et al., 2016). Individual wireless devices that are used interfaces with the Internet, collections of wireless devices, and ubiquitous systems and sensor networks are associated with new network service requirements in the IoT scenarios (Gaur et al., 2015). Therefore, a secured type of IoT architecture that satisfies the security standard of new network services must be developed.

7.0 Discussion on possible attacks posed by threats and vulnerabilities of the IoT

The IoT is a concept that evolves every day. Several technologies, which include WSNs, RFIDs, and cloud facilities, are utilized by the IoT devices. The M2M function is the main building block of the IoT paradigm (Jing et al., 2014). Moreover, the IoT paradigm is applicable in many domains, such as smart cities, healthcare, SGs, and intelligent transportation. These devices must communicate with each other and with different objects, including human beings. Every communication type must be secured in one way or another by protecting and providing users with the confidence that their information and communication channels are properly secured. However, the IoT protection is a challenging and demanding task (Kanuparthi, Karri, and Addepalli, 2013).

Security is a significant challenge that must be overcome to realize the IoT. The IoT architecture is expected to manage billions of connected items. This scenario will create many paths that can be accessed by malicious attackers because global availability and connectivity are the basic visions of the IoT. The IoT can be affected by different degrees of threats that range from hardware, network, and smart application threats that target different communication channels. Security and privacy issues must be addressed for the IoT to be deployed in different domains at a large scale (Roman, Zhou, and Lopez, 2013).

(a) Hardware threats

The IoT hardware devices include RFID tags, ZigBee, Bluetooth, and sensor nodes. The RFID tags' major features are auto identification and unique identity, which perform a rapid exchange of information between tags and readers through a wireless connection (Atzori et al., 2010). However, the possible threats and attacks on RFIDs include tracking, DoS, repudiation, spoofing, eavesdropping, and counterfeiting (Jing et al., 2014). ZigBee comprises a radio, a microcontroller, and a simple protocol. It is small in size, reliable, has limited power consumption, and inexpensive. However, these devices are vulnerable to threats and attacks, such as packet manipulation, hacking, key exchange, KillerBee, and Scapy (Lu, 2014). Bluetooth comprises a frequency-hopping spectrum that allows two devices to connect wirelessly, and it is safe and convenient. However, Bluetooth is exposed to threats and attacks, such as eavesdropping, DoS, Bluesnarfing, Bluejacking, car whisperer, and Bluebugging (Moosavi et al., 2015). The sensor node's major components are sensors and actuators that are utilized to sense and activate devices based on commands sent from the nodes; it is flexible and has high latency in communication (Zhang et al., 2015). Nevertheless, sensor nodes are exposed to different threats and attacks, such as DoS, exhaustion, unfairness, Sybil, jamming, tampering, and collisions (Massis, 2016).

(b) Network threats

The communication channels in the IoT can either be a wired or wireless medium. A wired medium involves utilizing cables, network adapters, and routers for the information exchange between two or more IoT devices. It enhances the security, reliability, and ease of use (Liu and Wang, 2010). However, a wired medium is exposed to certain threats and attacks, such as data manipulation, extortion hack, equipment hijacking, Signaling System No. 7, and malicious attacks (Perera et al., 2014). A wireless communication channel utilizes radio communication,

transmitters, and receivers for the data exchange between two or more devices (Atzori et al., 2010). It enhances the guest access and provides easier network expansion, increased mobility, and collaboration (Bandyopadhyay and Sen, 2011). Nevertheless, a wireless communication channel is vulnerable to several threats and attacks, such as misconfiguration, hacking, signal loss, DoS, war dialing, protocol tunneling, and MitM (Zhang, Shen, Wang, Yong, and Jiang, 2015).

(c) Smart Application threats

The IoT can be deployed in several smart application domains, such as smart city, SG, smart healthcare, and smart transportation. The smart city includes e-governance, street lighting, and water and waste management. In a smart city, city planning is improved for faster service delivery and economic development. However, smart city devices are open to different threats and attacks, which include smart city DoS, information manipulation, fake seismic detection, and fake flood detection (Zhu et al., 2015). SGs (i.e., smart meters and smart energy) are reliable, improve cost and savings, and enhance energy independence (Bi et al., 2016). Nevertheless, a SG is vulnerable to different attacks and threats, such as customer security, physical security, trust between traditional power devices, device endpoints, and malicious attacks (Barreto et al., 2015). Smart healthcare involves utilizing smart health cards. It improves the patients' security and privacy in terms of information details. However, smart health cards are vulnerable to threats and attacks, such as theft and loss, insider misuse, unintentional actions, hacking, internal attacks, and cyber attacks (Aman and Snekkenes 2016). Intelligent transportation involves traffic control, parking, and public transportation. It is easy to utilize, allows different users to be well-informed, and creates a new secure, organized, and smoother utilization of intelligent transportation systems. Nonetheless, intelligent transportation is exposed to several threat and attack types, such as smart city DoS, security plagues, and cyber-attacks (Jing et al., 2014).

The analysis of the possible attacks posed by threats and vulnerabilities to the IoT environment is presented in Table 6.

Table 6: Analysis of the possible attacks posed by threats and vulnerabilities to the IoT hardware, network infrastructure, and smart application environment.

Group	Features	Benefits	Threats	Vulnerability	Attacks	Confidentiality	Integrity	Authentication	Availability	Non-repudiation
Hardware										
RFID	Unique identity, Auto identification, and Unique identity	Rapid exchange of information between tags and readers through wireless connection	Tracking, DoS, Repudiation, Spoofing	Alteration, Corruption and Deletion	Eavesdropping, Counterfeiting,	-	-	-	+	-
ZigBee	Radio, Microcontroller, Simple protocol and Small size	Reliable, Low power consumption Low Cost	Packet manipulation	Hacking	Key exchange, KillerBee, and Scapy	±	+	±	+	±
	Frequency hopping spectrum	Allows two devices to connect wirelessly, very	Eavesdropping, DoS	Bluesnarfing Bluejacking	Car Whisperer, Bluebugging,	-	-	±	±	±

Bluetooth		safe and convenient								
Sensors node	Sensors and Actuators	Flexibility, Higher latency in communication	DoS, Exhaustion, Unfairness, Sybil	Flooding, Routing Protocols	Jamming, Tampering, Collisions	±	±	+	+	+
Network Infrastructure										
Wired	Cable, Network adapters, and Router	Enhanced security, Greater Reliability and Ease of use	Manipulation of data, Extortion hack	Signaling system No.7 (SS7), Hijacking of equipment	Weak Link, Malicious attacks	+	±	+	+	+
Wireless	Radio Communication, transmitters, and receivers	Enhanced guest access, Easier network expansion, Increased mobility and collaboration	Rogue access points, Misconfiguration	Hacking, Signal lost	DoS, War dialing, protocol tunneling; man-in-the-middle	±	±	±	+	+
Smart Application										
Smart City	e-governance, Street Lighting, Water and Waste Management	Better city planning, Faster delivery of service, Economic development	Smart City DoS, Manipulation of information	Fake seismic detection, fake flood detection	Mobile apps, Sensors	±	±	±	±	-
Smart grid	Smart meters, Smart Energy	Reliability, cost savings, and energy independence	Customer security, Physical security	trust between traditional power devices	End points on devices, malicious attacks	±	±	±	±	±
Healthcare	Smart health cards	improves patients security and privacy details	Theft and loss, Insider misuse, Unintentional actions	Hacking	Internal attack, cyber attack	±	±	±	-	-
Smart Transportation	Traffic control, Parking, Public Transportation	Ease-of-use	Smart City DoS	Security plagued	Cyber-attacks	-	-	±	±	±

- DoS: DoS attempts to make the IoT devices inaccessible to its intended users through temporary or indefinite interruption (Wood and Stankovic, 2012). The different types of DoS attacks that can be launched against the IoT include jamming, collision, and malicious internal attacks; the last type can create more havoc because it controls part of the infrastructure (Kasinathan et al., 2013 and Kasinathan et al., 2013).

- Eavesdropping: Eavesdropping is an electronic attack on the communication channel (i.e., wired or wireless networks) where communications are interrupted by an individual to extract data from the information flow. This attack is conducted by listening directly to the message or data sniffing (Pongle and Chavan, 2015).

- Device end-point: Smart applications on the IoT domain include smart city items (e.g., e-governance, street lighting, and water and waste management), SG items (e.g., smart meters and smart energy), smart health-care items (e.g., smart health cards), and intelligent transportation of items (e.g., traffic control, parking, and public transportation), which are physically situated in a specific domain. An active attacker can easily hack these items, extract information, and target other infrastructure that store information as alternatives to destroying these items (Porambage, et al, 2014).

- Counterfeiting attacks: Counterfeiting simply means imitation or forgery. The IoT devices, such as smart watches and smart lighting systems, are fragile and require lightweight security. However, an active attacker can easily duplicate and modify the contents of the IoT devices because of the security nature of these devices (Whitmore et al., 2015 and Ferati et al., 2016).

- MitM attack: MitM attacks create challenges in maintaining data security and privacy. Given the different attacks on the IoT devices, the security problem in the IoT involves the active interference of intruders on the devices (i.e., allowing unauthorized users to spy on data through a backdoor). Lightweight cryptographic protocols are considered to provide communication security for the IoT devices over a computer network as part of the DTLS. Nevertheless, MitM attacks take advantage of the weaknesses in the authentication protocols utilized by the communicating parties (Mahmood et al., 2016 and Maras, 2015).

8.0 Future Directions

The IoT development faces many security, trust, and infrastructure challenges. The aforementioned challenges must be addressed for the IoT to be accepted and fully deployed (Whitmore, Agarwal, and Da Xu, 2014). Most IoT devices are typically wireless (Raza, Wallgren, and Voigt, 2013), and securing these devices is essential. Security problems are fundamental in the IoT because they can occur at different layers. Different security properties, such as confidentiality, integrity, authentication, authorization, non-repudiation, availability, and privacy, must be assured for security to be guaranteed in the entire IoT system. This objective is extremely challenging due to the IoT environmental attributes (Abdmeziem and Tandjaoui, 2015).

8.1 Security-Related Challenges

This section presents several of the challenges related to security, which include secure SGs, lightweight authentication, heterogeneity, and quality of service (QoS).

8.1.1 Secure SG

Bekara (2014) proposed the SG security to examine the security issues and challenges in the IoT-based SG and describe the main security services that must be considered. However, no in-depth study has been conducted on the key security element of the SG and the secure integration of energy-aware smart homes, which makes end-users vulnerable to security threats and attacks. These threats and attacks include impersonation/identity spoofing, data tampering, and unauthorized control access when utilizing smart meters/smart appliances. Hence, an in-depth study on the key security element of SGs and an integration of a secure energy-aware smart home must be performed before deploying smart meters/smart appliances. Such study can help mitigate the vulnerability and security challenges in smart meters/smart appliances. Gupta and Garg (2015) proposed mobile IoT applications with cloud techniques, such as mobile sensor data processing engine, mobile fog, Embedded Integrated Systems (EIS), Mobile Sensor Hub (MosHub), and dynamic configuration that utilizes MosHub, to illustrate the different techniques employed in mobile IoT applications and the cloud. They discussed the similarities and comparisons

between the techniques and integrated the IoT applications utilizing mobile phones and cloud computing to form the cloud IoT. However, an increase in the quantity of sensors associated with a device or an increment in inquiry demand by GSN affects the CPU usage, memory, and energy utilization because of the nature of the IoT devices.

8.1.2 Lightweight Authentication

Yao, Chen, and Tian (2014) proposed a lightweight no-pairing Attribute-Based Encryption (ABE) scheme based on ECC to address data security and privacy issues. Their approach decreases the computation and communication overhead in the IoT. However, ABE has poor scalability and is inflexible in revoking attributes, which cannot be applied to multi-authority applications. Therefore, a lightweight multi-authority-oriented ABE and a flexible attribute revoking scheme must be developed.

Perera et al. (2014) proposed a pervasive lightweight verification mechanism for WSNs in distributed IoT applications. The DTLS scheme is adopted to conduct a security analysis on the PAuthKey to measure the security performance of WSNs. They implemented the PAuthKey protocol and demonstrated its performance capacities on the high-resource-constrained sensor nodes. However, many security threats and issues, such as access control and multicasting, have been encountered by the distributed IoT due to network heterogeneity and device mobility. Hence, an implicit certificate scheme for access control and large-scale multicasting must be developed, and security protocols that can handle issues of threats in distributed IoT network applications must be implemented.

Bose et al. (2015) and Raza et al. (2013) proposed a lightweight scheme for secure channel establishment to control the confidentiality level, evaluate a security score from the fine-grained sensor data, and preserve and protect content over a secure transmission. A lightweight security mechanism can support and measure the confidential value (i.e., affects the secrecy connection) of the sensor dataset (i.e., data in smart meters). Nevertheless, such a scheme can only consider a single security scenario (i.e., sensitivity) and how to derive sensitivity analysis and privacy degree based on multivariate data; it does not address multi-dimensional sensor data. Thus, an algorithm that can derive sensitivity analysis and privacy measure based on multivariate and multidimensional sensor data must be developed to extend the scheme to other IoT cases, especially for intelligent transportation.

8.1.3 Heterogeneity

Billions of connected devices have made the IoT heterogeneous in nature and thus more vulnerable to threats because each device has a different security measure (Srivastava and Garg, 2015). Constrained devices have inconsistencies in memory, energy consumption, and bandwidth, as well as in their mode of implementation and communication. Attaining a secure E2E communication is a challenge that mostly requires the adaptation of existing solutions or application of gateways (Bekara, 2014).

Resource estimation and management that utilize fog computing for a customer's Probabilistic Resource Estimation (PRE) model were introduced by Aazam et al. (2016) to implement well-organized, successful, and reasonable resource management for the IoT. Nevertheless, estimating the amount of resources that will be consumed by each node and determining whether the requesting nodes or devices will completely utilize the resources they requested are difficult because of the heterogeneous devices that are part of the IoT. Attaining minimum latency is also difficult with devices, such as healthcare and emergency services, because of the unreliable core network of reaching the cloud through shared resources. Hence, testing for minimum latency requires the application of the model in other research fields, such as smart cities,

medical centers, and smart homes. Moreover, Sicari et al. (2015) analyzed the available solutions identified with security (i.e., reliability, secrecy, and verification), privacy, and trust in the IoT arena. Nonetheless, the solutions provided by the authors do not properly define the privacy policies that can manage the adaptability of the IoT devices in the heterogeneous environment.

Persson and Angelsmark (2015) presented a framework called Calvin, which adopts a unified programming model to combine the IoT and the cloud. This framework attempts to develop a solution that does not allow developers to avoid heterogeneity in the IoT, but utilize it by hiding the protocol and data transport details. It also refines communication efficiency by avoiding a direct device-to-cloud client/server approach. Calvin is still in its initial phases of development due to the hybrid nature of the framework. No implementation that anticipates all security and routing properties required to make autonomous migration for an IoT distributed environment has been reported.

Li, Han, and Jin (2016) recently proposed a practical access control for sensor networks in the context of the IoT. The senders in this novel Heterogeneous SignCryption belong to the Certificate-Less Cryptography (CLC) environment, whereas the receivers belong to the Identity-Based Cryptography (IBC) environment. The main characteristic of this approach is heterogeneity. In particular, the senders and receivers belong to two different cryptographic environments. It permits a sender in the CLC environment to transmit a message to a receiver in the IBC environment. Furthermore, this approach has ciphertext authenticity that allows the shift of the computational cost of the sensor nodes to the gateway. CLC does not require the utilization of certificates. However, it still requires a trusted third party called the Key Generating Center, which is responsible for generating a partial private key that utilizes the user's identity and a master key. They also focused mainly on the computational cost and energy consumption of the sensor node.

8.1.4 QoS

The QoS design is the fundamental functionality for routing data in resource-constrained devices to allow differentiated delivery and ensure quality service. Several solutions have been provided to improve the services in constrained nodes and ensure suitable QoS for constrained devices. The solutions include adaptive edge (fog) computing solutions based on REgressive Admission Control (REAC) proposed by Jutila (2016) and Fuzzy Weighted Queueing (FWQ) with adaptive computing methods for the IoT networking at the network edges, which can be applied to optimize and control traffic flows and network resources. The FWQ control with a feedback mechanism provides properties related to system stability, short settling times, and fast response time. REAC helps in managing the E2E network performance at the network edge. However, the solutions focus on only one QoS metric (i.e., network capacity) and do not address other QoS issues, such as connectivity, reliability, and delay. The operating capacity (i.e., IEEE 802.11p) must fully support two instances of Roadside Unit (RSU) deployment to avoid network congestion. However, it only supports one RSU deployment that leads to network congestion. Therefore, solutions that address the interoperability challenges and unsolved QoS metric issues, such as connectivity, reliability, and delay, are required.

Chakrabarty et al. (2015) also proposed a black SDN to enhance secure communications by encrypting the header and payload at the network layer. This approach can mitigate a range of attacks and improve the overall lifespan and network performance of the IoT networks. Resource-constrained IoT nodes cannot support a full SDN implementation and do not address the security of the black link layer frame. The black network is an application delivery network that provides a key service method for securing all data, decreases network efficiency, and complicates routing. Therefore, sleep synchronization protocols that are appropriate for black networks are required to ensure packet delivery to all nodes and secure the black link layer frame by multiple methods. This approach allows for a fine-grained approach to securing the meta-data. These protocols

include the following: 1) replacing the meta-data fields by Grain-128a IV and a keystream, 2) the AES-EAX mode, and 3) a pre-shared IV to allow for better payload efficiency.

Homg et al. (2011) proposed an adaptive bandwidth allocation algorithm called Adaptive Weighted Fair Queue (AWFQ) for reservation protocols to support QoS in the IoT network layer. The proposed algorithm employs the queue status and priority assignment to control the bandwidth sharing of different Internet services and guarantee that a defined QoS policy is obtained for resource-constrained devices. The algorithm mainly focuses on bandwidth utilization (i.e., how network bandwidth is effectively and efficiently utilized among resource-constrained devices in a flexible, fair, and prioritized manner). Nevertheless, the bandwidth starvation on resource-constrained devices with low priority and queuing congestion was not addressed.

8.2 Trust Management

The privacy of the nodes and users in the IoT are extremely important and must be seriously considered when developing the IoT devices. Trust Management (TM) involves the preservation of user privacy, such as personal user data, by the policy and prospect of the IoT users in a flexible manner. Thus, integrating TM into the IoT RFID devices is necessary. Moreover, TM not only occurs between the readers and the RFID tags when communicating, but also between the readers and the base stations. Digital signature technology is employed in the TM domain; it is important in the trust area because it is utilized for authentication (i.e., both on the IoT devices and the data) and during data communication among different IoT applications (Jing et al., 2014). However, few research types on TM in the IoT domain have been performed.

TM attempts to solve issues related to security in a distributed environment (Gu, Wang, and Sun, 2014). Trust is a dynamic concept that can safeguard the existing IoT architecture and provide a uniform decision-making scheme for the IoT heterogeneous environment or multi-domains. Hence, Josang, Ismail, and Boyd (2012) considered TM as a possible solution to security-related issues in the IoT. Addressing and computing the trust between different networks in the heterogeneous IoT is a demanding issue because different network nodes have different trust criteria. TM provides an effective approach to assessing the trust relationships between IoT entities and helps users in careful decision-making when communicating and cooperating with each other.

Liu and Wang (2010) and Yan, Zhang, and Vasilakos (2014) concentrated on the technologies for controlling heterogeneous connected devices in the IoT. Their studies primarily focused on a heterogeneous network model, trust directing, and TM technology. Their explorations offer a direction and strategy for developing future IoT devices. However, implementing real-life solutions on TM in the IoT domain is necessary.

Chen et al. (2011) explained the complexity of trust relationship among heterogeneous entities. They analyzed the security challenges and threats imposed on the IoT based on several practicable trust-based ideas they gathered. They then proposed a type of security IoT architecture.

In contrast to Liu and Wang (2010) and Yan, Zhang, and Vasilakos (2014) who only provided several non-practicable ideas for handling trust in the IoT, Bahtiyar and Çağ layan (2012) introduced a trust model that focuses on extracting trust data and provides formal security policies for the IoT devices/entities when required. They attempted to provide a formal security policy for an entity on how to extract trust data from a secured system for service. Nevertheless, no specific network architecture has been considered in this model to properly evaluate the authentication of the parameters utilized and determine how it can be applied in the IoT.

Autonomic TM (ATM), which provides flawless benefits and supports Human–Computer Interaction (HCTI) in a reliable manner, was proposed by Yan, Zhang, and Vasilakos (2014). However, trust covers a larger extension than security. Therefore, it is complex and difficult to build, guarantee, and maintain. Disseminating and enumerating trust among different networks in a heterogeneous IoT is a challenging issue because different networks nodes have different TM criteria. Similarly, ATM is difficult to realize because the nature of the deployment, mobility, and low computation capacity of the cloud of things cannot be easily controlled. Performance improvements, such as the most effective method to make key dissemination proficient, how to implement lightweight security and preserving solutions, and how to avoid complex and energy-consuming cryptographic controls, remain as considerable threats. Hence, lightweight security and trust components that can be implemented on small items with regard to the IoT must be developed and specifically centered on preventing possible DoS or DDoS attacks.

Furthermore, Sicari et al. (2015) analyzed the obtainable solutions identified with security (i.e., reliability, secrecy, and confirmation), privacy, and trust in the IoT arena. The trust relationship between two devices will support the communication between these devices in the future. These devices can always share resources as long as they trust each other. However, they did not address the implementation of a trust negotiation tool that can handle data stream, access control, and a unified vision that concerns the assurance of security and privacy requirements in such heterogeneous environments. This approach involves different technologies and communication criteria. Therefore, well-defined privacy policies that deal with scalability and adaptable infrastructure that can manage security threats in a dynamic IoT environment must be developed.

Many studies have recently been conducted on TM for the IoT, and different trust models have been proposed (Lopez et al., 2010 and Gu et al., 2012). These trust models may be included in the TM development for the IoT. No related work that establishes a trust mechanism has been reported and remains an open issue for the IoT.

8.3 Infrastructure

This section highlights several challenges related to infrastructure, which include SDN, smart e-health, and middleware. No unified IoT infrastructure exists, which makes the IoT devices vulnerable to attacks and threats (Chen, Lai and Wang, 2011).

8.3.1 SDN

Chakrabarty, Engels, and Member (2016) proposed a secure IoT architecture for smart cities that addresses the vulnerabilities in traditional IoT systems. The four basic IoT architectural blocks to secure smart cities are a black network, trusted SDN controller, unified registry, and key management system. The IoT architectural blocks provide the following security services: confidentiality, integrity, privacy, secure routing (black packets), route availability, identity management, node authentication, authorization, availability, efficient key distribution, and secure utilization of symmetric keys by authorized devices. However, Chakrabarty and Engels did not focus on the security architecture and SDN implementation for the IoT. This scenario causes new attack types because the SDN architecture changes the IoT network's communication patterns, which requires a new approach to secure the IoT network. Encrypting the header creates routing challenges for the IoT nodes, which are often asleep. Hence, sleep synchronization protocols that are appropriate for black networks to ensure packet delivery to all nodes and a secure type of IoT architecture that can help address translations, define location privacy, and characterize mobility must be developed and designed.

Jararweh et al. (2015) proposed a comprehensive software-defined framework model (SDIoT) to improve the IoT managing procedure and provide a basic solution for threats in the conventional IoT architecture through forwarding, storing, and securing the data created from the IoT objects. This approach integrates a SDN, SDStore, and SDSec to a single software-defined control model. The SDIoT framework result accelerates and facilitates the control and management processes of the

IoT and covers and tackles the difficulties in traditional architecture. This framework also enables cloud users to utilize the cloud resources in an adequate manner by generating segments/fragments and allowing transparent information flow. Nonetheless, the issues of SDN compatibility, security, and interoperability still persist. No practical and experimental SDIoT framework exists to test different forms of the IoT topologies. Therefore, developing an SDIoT framework to investigate different types of IoT topologies that can address security issues and interoperability in the SDN is necessary.

8.3.2 Smart e-health

Moosavi et al. (2015) developed a secure and efficient type of verification architecture for IoT-based healthcare systems utilizing a type of distributed smart e-health gateway architecture. The gateway can be abused on medical sensor nodes due to its distributed nature derived from the end-user. Furthermore, can a gateway adapt to different difficulties in pervasive healthcare systems, such as scalability, security, and dependability? Abuse or privacy concerns can possibly limit the public from utilizing IoT-based health care frameworks. Traditional security and privacy mechanisms and current cryptographic solutions, secure protocols, and privacy assurance cannot be reused because the resources limit the security level requirements and framework design of IoT-based healthcare applications. Therefore, secure network infrastructures for short- or long-range communication are required to mitigate risks in the architecture.

Gaur et al. (2015) proposed custom-built services in a smart city environment by utilizing semantic web technologies and the Dempster–Shafer uncertainty theory to enable communication between WSNs and ICTs. This architecture type helps Alzheimer's patients and elderly individuals with their everyday breathing exercises by sending notifications to users when they forget or are unable to finish breathing exercises. This framework can also serve as a smart platform for individuals who live in a smart society by networking information from different smart city domains. However, the proposed architecture cannot cover a large area (i.e., it concentrates on the most vital parts of the smart city) and is yet to be tested. Thus, an architecture type that can cover an entire city without neglecting any area and perform experiments on the idea discussed must be developed.

8.3.2 Middleware

Ramão et al. (2015) discussed the advantages of implementing a type of well-defined standard security architecture for SOA-based IoT middleware and studied the current effort by different researchers. They also outlined the security facilities that can be utilized when defining the IoT security architecture to lower the security threats in SOA-based IoT middleware frameworks. SOA-based methods also provide the IoT applications with an inflexible and organized reflection of security facilities required for communication by items (i.e., IoT devices). These methods help ensure high levels of system interoperability and provide system services based on devices and utilized by applications. Nevertheless, the coexistence of SOA and resource-oriented architecture (ROA) creates a new set of traditional security demands that must be followed for resource-constrained environments to guarantee system safety. None of the aforementioned studies suggested solutions that outline all of the middleware security requirements. Hence, a security countermeasures system in the middleware architecture must be developed to protect the IoT middleware from attacks.

Furthermore, OSCAR with CoAP was proposed by Vucinic´ et al (2015). OSCAR is a middleware architecture for E2E security in the IoT. OSCAR was evaluated in two cases: 802.15.4 LLN and M2M communication in two hardware environments and MAC layers. This scheme essentially provides support for multicasting, asynchronous data communication, and caching. It handles security and authorization issues in E2E while safekeeping full data integrity with the plain DTLS approach. However, failure in the node that serves as a PAN coordinator in a beacon-enabled 802.15.4 affects the periodic transmission of beacons in the network. Existing techniques cannot derive lost keys once information is lost in the CoAP header. Zhao and Ge (2013) illustrated several IoT security issues that occur in a three-layer type of system

architecture and generated a solution coupled with the key technologies involved. Their study identified security problems in every layer of the IoT architecture, which are the perception, network, and application layers. The main equipment in the perception layer includes RFID, ZigBee, and all sensor types. Attackers can easily gain access, control, or physically harm the hardware. The IoT easily has security vulnerabilities in the network layer. Heterogeneity generally worsens the security, interoperability, and coordination of the network for different industries or environments. The security issues in the application layer are different, which makes security more complex and difficult. A unified IoT security architecture is yet to be formed. Therefore, encrypting the RFID signal through a suitable algorithm for data security is necessary. Furthermore, a precise unified authentication mechanism, E2E authentication, key agreement mechanism, Public Key Infrastructure (PKI), wireless PKI, security routing, and intrusion detection must be set up for different types of network architectures.

9.0 Conclusion

The IoT has recently emerged as an important research topic. It provides the integration of different sensors and objects to communicate specifically with each other without human interference. Moreover, the requirements for the large-scale deployment of the IoT are increasing rapidly with major security concerns. We presented a comprehensive review of the state-of-the-art IoT security threats and vulnerabilities. We classified the IoT by presenting the taxonomy of the current security threats and vulnerabilities in the context of its application, architecture, and communication. Moreover, we discussed the current state-of-the-art IoT-enabling communication technologies. We also proposed a possible solution structure of the IoT security to overcome the security issues in the IoT environment. Finally, we discussed open research issues and challenges to the IoT security. However, research in the IoT security is in its infancy and is yet to be tested (Gaur et al., 2015). The possible solutions to the discussed security threats and vulnerabilities need to be implemented/applied for the IoT to be fully adopted by users.

Acknowledgment

This paper is financially supported by the Malaysian Ministry of Education under the University of Malaya High Impact Research Grant UM.C/625/1/HIR/MoE/FCSIT/03.

References

Aazam, M., St-Hilaire, M., Lung, C.-H., and Lambadaris, I. (2016). PRE-Fog: IoT trace based probabilistic resource estimation at Fog. 2016 13th IEEE Annual Consumer Communications and Networking Conference (CCNC), 12–17.

Abdmeziem, M. R., and Tandjaoui, D. (2015). An end-to-end secure key management protocol for e-health applications. Computers and Electrical Engineering, 44, 184–197. http://doi.org/10.1016/j.compeleceng.2015.03.030

Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., and Khan, S. U. (2016). Secure and dependable software defined networks. Journal of Network and Computer Applications, 61, 199–221.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials, 17(4), 2347-2376.

Al-turjman, F., and Gunay, M. (2016). CAR Approach for the Internet of Things Approche de la CAR pour l' internet des objets. Canadian Journal of Electrical and Computer Engineering, 39(1), 11–18.

Aman, W., and Snekkenes, E. (2016). Managing security trade-offs in the Internet of Things using adaptive security. 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015, 362–368.

Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805.

Babar, S., Stango, A., Prasad, N., Sen, J., and Prasad, R. (2015). Proposed embedded security framework for Internet of Things (IoT). 2015 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, 1–5.

Bahtiyar, Š., and Ufuk Çağ layan, M. (2012). Extracting trust information from security system of a service. Journal of Network and Computer Applications, 35(1), 480–490.

Bandyopadhyay, D., and Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49–69.

Bansal, G., Kenney, J. and C. Rohrs, C. (2013). "LIMERIC: A Linear Message Rate Control Algorithm for DSRC Congestion Control", IEEE Transactions on Vehicular Technology, to appear fall 2013.

Barreto, L., Celesti, A., Villari, M., Fazio, M., and Puliafito, A. (2015). An Authentication Model for IoT Clouds. Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, 1032–1035.

Bekara, C. (2014). Security issues and challenges for the IoT-based smart grid. Procedia Computer Science, 34, 532–537.

Bi, Z., Wang, G., and Xu, L. Da. (2016). A visualization platform for internet of things in manufacturing applications. Internet Research.

Bohge, M., and Trappe, W. (2013). An authentication framework for hierarchical ad hoc sensor networks. Proceedings of the 2013 ACM Workshop on Wireless Security - WiSe '13, 79.

Bonetto, R., Bui, N., Lakkundi, V., Olivereau, A., Serbanati, A., and Rossi, M. (2012). Secure Communication for Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples. World of Wireless, Mobile and Multimedia Networks (WoW- MoM), , 2012, 2012 IEEE, 1–7.

Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. Computer Communications, 54, 1–31.

Borgia, E., Gomes, D. G., Lagesse, B., Lea, R., and Puccinelli, D. (2016). Special issue on "Internet of Things: Research challenges and Solutions ," 90, 1–4.

Bose, T., Bandyopadhyay, S., Ukil, A., Bhattacharyya, A., and Pal, A. (2015). Why not keep your personal data secure yet private in IoT: Our lightweight approach. Proceedings of the 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), (April), 1–6.

Botta, A., De Donato, W., Persico, V., and Pescapé, A. (2016). Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, 684–700.

Chakrabarty, S., Engels, D. W., and Thathapudi, S. (2015). Black SDN for the internet of things. Proceedings - 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2015, 190–198.

Chakrabarty, S., Engels, D. W., and Member, S. (2016). A Secure IoT Architecture for Smart Cities.

Chen, D., Chang, G., Jin, L., Ren, X., Li, J., and Li, F. (2011). A novel secure architecture for the Internet of things. Proceedings - 2011 5th International Conference on Genetic and Evolutionary Computing, ICGEC 2011, 311–314.

Chen, M., Lai, C.-F., and Wang, H. (2011). Mobile multimedia sensor networks: architecture and routing. EURASIP Journal on Wireless Communications and Networking, 2011(1), 159.

Covington, M. J. (2013). Threat Implications of the Internet of Things. Economics the Internet of Things between efficiency and privacy, 7(4), 69–71.

Da Xu, L., He, W., and Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), 2233-2243.

Eschenauer, L., and Gligor, V. D. (2012). A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communications Security, 41–47.

Ferati, M., Kurti, A., Vogel, B., and Raufi, B. (2016). Augmenting Requirements Gathering for People with Special Needs using IoT: A Position Paper, 48–51.

Flauzac, O., Gonzalez, C., and Nolot, F. (2015). New security architecture for IoT network. Procedia Computer Science, 52(1), 1028–1033.

Frizzo-barker, J., Chow-white, P. A., Mozafari, M., and Ha, D. (2016). International Journal of Information Management An empirical study of the rise of big data in business scholarship. International Journal of Information Management, 36(3), 403–413.

Gaur, A., Scotney, B., Parr, G., and McClean, S. (2015). Smart city architecture and its applications based on IoT. Procedia Computer Science, 52(1), 1089–1094.

Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., and Raza findralambo, T. (2011). A survey on facilities for experimental internet of things research. IEEE Communications Magazine, 49(11)

Granjal, J., Monteiro, E., and Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys and Tutorials, 17(3), 1294-1312.

Gu, L., Wang, J., and Sun, B. (2014). Trust management mechanism for Internet of Things. China Communications, 11(2), 148–156.

Gu, X., Qiu, J., and Wang, J. (2012). Research on trust model of sensor nodes in WSNs. Procedia Engineering, 29, 909–913.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.

Guo, J., Chen, R., and Tsai, J. J. (2017). A survey of trust computation models for service management in internet of things systems. Computer Communications, 97, 1-14.

Gupta, R., and Garg, R. (2015). Mobile Applications Modelling and Security Handling in Cloud-Centric Internet of Things. Proceedings - 2015 2nd IEEE International Conference on Advances in Computing and Communication Engineering, ICACCE 2015, 285–290.

Han, J., Ha, M., and Kim, D. (2015). Practical security analysis for the constrained node networks: Focusing on the DTLS protocol. Internet of Things (IOT), 2015 5th International Conference on the, 22–29.

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., … Chiroma, H. (2016). The role of big data in smart city. International Journal of Information Management, 36(5), 748–758.

Haroon, A., Shah, M. A., Asim, Y., Naeem, W., Kamran, M., and Javaid, Q. (2016). Constraints in the IoT: The World in 2020 and Beyond. Constraints, 7(11).

Hernández-Ramos, J. L., Moreno, M. V., Bernabé, J. B., Carrillo, D. G., and Skarmeta, A. F. (2015). SAFIR: Secure access framework for IoT-enabled services on smart buildings. Journal of Computer and System Sciences, 81(8), 1452–1463.

Homg, M.-F., Lee, W.-T., Lee, K.-R., and Kuo, Y.-H. (2011). An adaptive approach to weighted fair queue with QoS enhanced on IP network. TENCON 2011. Proceedings of IEEE Region 10 International Conference on Electrical and Electronic Technology, 1(1), 181–186 vol.1.

Horrow, S., and Anjali, S. (2012). Identity Management Framework for Cloud Based Internet of Things. SecurIT '12 Proceedings of the First International Conference on Security of Internet of Things, 200–203.

Islam, S. M. R., Kwak, D., Kabir, H., Hossain, M., and Kwak, K.-S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. Access, IEEE, 3, 678–708.

Jararweh, Y., Al-Ayyoub, M., Darabseh, A., Benkhelifa, E., Vouk, M., and Rindos, A. (2015). SDIoT: a software defined based internet of things framework. Journal of Ambient Intelligence and Humanized Computing, 6(4), 453–461.

Jiang, H., Shen, F., Chen, S., Li, K. C., and Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. Future Generation Computer Systems, 49, 133–141.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481–2501.

Josang, A., Ismail, R., and Boyd, C. (2012). A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2), 618–644.

Jutila, M. (2016). An Adaptive Edge Router Enabling Internet of Things. IEEE Internet of Things Journal, 4662(c), 1–1.

Kai, P. (2016). DEMO: An IDS framework for internet of things empowered by 6LoWPAN. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS '13, (October 2016), 1337–1340.

Kanuparthi, A., Karri, R., and Addepalli, S. (2013). Hardware and embedded security in the context of internet of things. Proceedings of the 2013 ACM Workshop on Security, Privacy and Dependability for Cyber Vehicles - CyCAR '13, 61–64.

Karlof, C., and Wagner, D. (2013). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Sensor Network Protocols and Applications, 2013. Proceedings of the First IEEE. 2013 IEEE International Workshop on, 1(2–3), 113–127.

Kasinathan, P., Pastrone, C., Spirito, M. A., and Vinkovits, M. (2013). Denial-of-Service detection in 6LoWPAN based Internet of Things. International Conference on Wireless and Mobile Computing, Networking and Communications, (October), 600–607.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., and Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks, 11(8), 2710–2723.

Kotsev, A., Schade, S., Craglia, M., Gerboles, M., Spinelle, L., and Signorini, M. (2016). Next generation air quality platform: Openness and interoperability for the internet of things. Sensors (Switzerland), 16(3), 1–16.

Laghari, S., and Niazi, M. A. (2016). Modeling the internet of things, self-organizing and other complex adaptive communication networks: A Cognitive Agent-based Computing approach. PLoS ONE, 11(1).

Li, F., Han, Y., and Jin, C. (2016). Practical access control for sensor networks in the context of the Internet of Things. Computer Communications, 90.

Li, S., Tryfonas, T., and Li, H. (2016). The Internet of Things: a security point of view. Internet Research, 26(2), 337–359.

Li, Y. J. (2015). An Overview of the DSRC / WAVE Technology. Eveleigh, NSW 2015, Australia.

Liu, L. and Wang, W. (2010). Internet of things: Objectives and scientific challenges. Journal of Computer Science and Technology. 26(6), 919-924.

Liu, Y., Cheng, C., Gu, T., Jiang, T., Member, S., and Li, X. (2016). Scheme for Smart Grid, 16(3), 836–842.

Lopez, J., Roman, R., Agudo, I., and Fernandez-Gago, C. (2010). Trust management systems for wireless sensor networks: Best practices. Computer Communications, 33(9), 1086–1093.

Lu, C. (2014). Overview of Security and Privacy Issues in the Internet of Things, 1–11.

Ma, H. D. (2011). Internet of things: Objectives and scientific challenges. Journal of Computer Science and Technology, 26(6), 919–924.

Mahalle, P., Babar, S., Prasad, N. R., and Prasad, R. (2010). Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges. Recent Trends in Network Security and Applications - Communications in Computer and Information Science, 89, 430–439.

Mahmood, K., Ashraf Chaudhry, S., Naqvi, H., Shon, T., and Farooq Ahmad, H. (2016). A lightweight message authentication scheme for Smart Grid communications in power sector. Computers and Electrical Engineering, 52, 114–124.

Mansfield-Devine, S. (2016). Securing the Internet of Things. Computer Fraud and Security, 2016(4), 15–20.

Maras, M.-H. (2015). Internet of Things: security and privacy implications. International Data Privacy Law, 5(2), 99–104.

Martín-Fernández, F., Caballero-Gil, P., and Caballero-Gil, C. (2016). Authentication based on non-interactive zero-knowledge proofs for the internet of things. Sensors (Switzerland), 16(1).

Massis, B. (2016). The Internet of Things and its impact on the library. New Library World, 117(3/4), 289–292.

Mazlan Abbas. (2014). Internet of Things (IoT) - We Are at the Tip of An Iceberg. inSlideShare. 978-3-642- 19156-5.

Milbourn, T. (2016). No Title. Retrieved July 15, 2016, from https://www.u-blox.com/en/blog/ip-versus-coap-iot-communications.

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497–1516.

Mishra, S. (2015). Network Security Protocol for Constrained Resource Devices in Internet of Things, 1–6.

Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., and Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 52(1), 452–459.

Ndibanje, B., Lee, H. J., and Lee, S. G. (2014). Security analysis and improvements of authentication and access control in the Internet of Things. Sensors (Basel, Switzerland), 14(8), 14786–14805.

Neisse, R., Steri, G., Fovino, I. N., and Baldini, G. (2015). SecKit: A Model-based Security Toolkit for the Internet of Things. Computers and Security, 54, 60–76.

Ning, H. S., and Liu, H. (2015). Cyber-physical-social-thinking space based science and technology framework for the Internet of Things. Science China Information Sciences, 58(3), 1–19.

Nolin, J., and Olson, N. (2016). The Internet of Things and convenience. Internet Research, 26(2), 360–376.

Oen, H. M. (2015). Interoperability at the Application Layer in the Internet of Things, (June).

Perera, C., Zaslavsky, A., Christen, P., and Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. IEEE Communications Surveys and Tutorials, 16(1), 414–454.

Persson, P., and Angelsmark, O. (2015). Calvin – Merging Cloud and IoT. Procedia Computer Science, 52(Ant), 210–217.

Pongle, P., and Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015, 0(c), 0–5.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., and Ylianttila, M. (2014). Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. IEEE Wireless Communications and Networking Conference, WCNC, 2014, 2728–2733.

Raju, C. (2014). Defending Against Resource Depletion Attacks in Wireless Sensor Networks, 3(11), 590–595.

Ramão Tiago Tiburski, Leonardo Albernaz Amaral, Everton de Matos, and F. H. (2015). T He I Mportance of B Eing, 44(0), 95–128.

Raza, S., Shafagh, H., Hewage, K., Hummen, R., and Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. IEEE Sensors Journal, 13(10), 3711–3720.

Raza, S., Wallgren, L., and Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8), 2661–2674.

Roman, R., Alcaraz, C., Lopez, J., and Sklavos, N. (2011). Key management systems for sensor networks in the context of the Internet of Things. Computers and Electrical Engineering, 37(2), 147–159.

Roman, R., Zhou, J., and Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.

Sezer, S., Scott-Hayward, S., Kaur Chouhan, P., Fraser, B., Lake, D., Systems Jim Finnegan, C., … Layout, S. (2013). Introduction: What is Software-Defined Networking? Future carrier networks are we ready for SDN? Implementation Challenges for Software-Defined Networks BACKGROUND: WHY SDN? Future Carrier Networks, 51(7), 36–43.

Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., and Coen-Porisini, A. (2016). A secure and quality-aware prototypical architecture for the Internet of Things. Information Systems, 58, 43–55.

Srivastava, P., and Garg, N. (2015). Secure and optimized data storage for IoT through cloud framework. International Conference on Computing, Communication and Automation, ICCCA 2015, 720–723.

Suo, H., Wan, J., Zou, C., and Liu, J. (2015). Security in the internet of things: A review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 3, 648–651.

Tsai, C.-W., Lai, C.-F., and Vasilakos, A. V. (2014). Future Internet of Things: open issues and challenges. Wireless Networks, 20(8), 2201–2217.

Valdivieso Caraguay, Á. L., Benito Peral, A., Barona López, L. I., and García Villalba, L. J. (2014). SDN: Evolution and opportunities in the development IoT applications. International Journal of Distributed Sensor Networks, 2014.

Valmohammadi, C. (2016). Examining the perception of Iranian organizations on Internet of Things solutions and applications. Industrial and Commercial Training, 48(2), 104–108.

Vishvakarma, N. K., James, W., and R.R.K. Sharma. (2015). Internet of Things Applications - From Research and Innovation to Market Deployment. JIMS, 15(1), 35–43.

Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., and Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. Ad Hoc Networks, 32, 3–16.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law and Security Review, 26(1), 23–30.

Whitmore, A., Agarwal, A., and Da Xu, L. (2014). The Internet of Things: A survey of topics and trends. Information Systems Frontiers, 17(2), 261–274.

Wood, A. D., and Stankovic, J. A. (2012). Denial of service in sensor networks. Computer, 35(10), 54–62.

Wu, J., Dong, M., Ota, K., Liang, L., and Zhou, Z. (2014). Securing distributed storage for Social Internet of Things using regenerating code and Blom key agreement. Peer-to-Peer Networking and Applications, 8(6), 1133–1142.

Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120–134.

Yao, X., Chen, Z., and Tian, Y. (2014). A lightweight attribute-based encryption scheme for the Internet of Things. Future Generation Computer Systems, 49, 104–112.

Ye, N., Zhu, Y., Wang, R. C., Malekian, R., and Lin, Q. M. (2014). An efficient authentication and access control scheme for perception layer of internet of things. Applied Mathematics and Information Sciences, 8(4), 1617–1624.

Yinbiao, S., Lee, K., Lanctot, P., Juanbin, F., Hao, H., Chow, B., … Qui, W. (2014). Internet of Things: Wireless Sensor Networks. International Electronic Commision, (December), 1–78.

Zhang, Y., Shen, Y., Wang, H., Yong, J., and Jiang, X. (2015). On Secure Wireless Communications for IoT Under Eavesdropper Collusion. IEEE Transactions on Automation Science and Engineering, 13(3), 1281–1293.

Zhao, K., and Ge, L. (2013). A survey on the internet of things security. Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013, 663–667.

Zhu, C., Leung, V. C. M., Shu, L., and Ngai, E. C. H. (2015). Green Internet of Things for Smart World. IEEE Access, 3, 2151–2162.

Zhu, S., Setia, S., and Jajodia, S. (2015). LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks Categories and Subject Descriptors. ACM Transactions on Sensor Networks (TOSN), 2(4), 500–528.