AJSP
المجلة العربية للنشر العلمي
العدد الثالث عشر
تاريخ الإصدار: 2 – 11 – 2019
www.ajsp.net
ISSN: 2663-5798

"Survey on IoT Security"

Name of the researcher:

Samaher Saleh Alghamdi

Faculty of Computing and Information Technology /King Abdul Aziz University

Abstract:

IoT is a rising field that is expected to dominate the world in the coming years. The number of devices connected to each other is expected to reach 20.4 billion by 2020 [24]. While IoT devices are becoming dominant presences in every home, office, hospital, etc., the lack of security may result in disaster. Security in IoT is very important and critical because for the IoT, the lack of security is not limited to the loss of information or personal data but may even become life-threatening. The heterogenous nature of IoT systems, which often involves devices with constrained power and computational limitations, make finding security solutions for IoT very challenging [25]. In this survey paper, we discuss IoT security from different aspects, outline IoT security requirements and measures for three-layer IoT architecture, present up-to-date security solutions, and highlight future research directions

1 Introduction

The term Internet of Things (IoT) was first used in 1999 by Kevin Ashton [11]. Since then, IoT has gradually become more common, and now is involved in every part of our life. IoT is defined as a set of devices (things) that are able to collect data from the environment and share it with other devices in real time [10]. IoT expanded the known concept of the Internet, which connects people to each other, to connecting devices to the Internet, which means communication is not limited to human-to-human, but also includes device-to-device and device-to-human [1], [3]. In IoT, the presence of humans is not as important as in the Internet, as the devices collect the data themselves, processing, analyzing, and making decisions [10]. These smart devices are able to play the role of humans and reduce our presence or participation, thus making our lives easier and more comfortable.

IoT is a rising field that is expected to soon dominate the world. Studies indicate that IoT will spread quickly in the coming years, so the number of connected devices will reach 20.4 billion by 2020 [24]. IoT has applications in many areas, such as smart cities, smart homes, smart grids, smart health, etc. [10].

While IoT devices have begun to invade every home, office, hospital, etc., the lack of security may result in disaster. Security in IoT is very important and critical because in case of IoT the lack of security is not limited to the loss of information or personal data, but it may go beyond and become also life-threatening. For example, in the case of hacking smart houses, the hacker can monitor the house and the user's activities, such as eating or leaving [10], control the settings of the camera, and give control to others [8]. Also, by hacking the smart home lock, the hacker can trespass into the home without alerting the house members, and maybe steal or threaten their lives [9]. Moreover, in the area of smart health, Implantable Medical Devices (IMD), which are implanted in patients' bodies to monitor and follow their health conditions, may be hacked. Several breakthroughs have been identified in IMDs, such as insulin pumps, pacemakers, and ICDs where, for example, a hacker can change the dose of medicine or drain the battery of the device [10].

For the above reasons, IoT security is very crucial and should be considered seriously. Although much research has been conducted to find the best security solutions since IoT began, this research is still ongoing. The heterogenous nature of IoT systems which often involves devices with constrained power and computational limitations, make finding security solutions for IoT very challenging [25].

In this survey paper, we discuss IoT security from different aspects. The paper is organized as follows: In section 2, we introduce IoT architectures; section 3 explains the difference between IT security and IoT security, including the factors that make IoT security a challenge. In section 4, we present IoT security requirements. In section 5, we discuss the security threats in each of the three layers of three-layer IoT architecture and then define the security measures for each layer in section 6. Section 7 presents up-to-date IoT security solutions. In section 8, we highlight the direction of IoT security research. Finally, section 9 concludes the paper.

2 IoT Architectures

In spite of all research attempts to create a unified IoT architecture, to this point there is no specific unified architecture for IoT systems [1], [2]. The most-commonly researched IoT architecture is the three-layer architecture, comprised of the Perception layer, Network layer, and Applications layer [2], [6]. These three layers are connected, and each one has specific functionality and security issues. Figure 1 visualizes the three-layer IoT architecture.

ISSN: 2663-5798

1. **Perception layer:** This is the bottom layer of IoT architecture. It is also called the Sensor layer [3], [6] or physical layer [2]. The main goal of this layer is detecting and collecting data and information from the surrounding environment using sensor devices and actuators, then processing this collected information to be sent to the Network layer [2], [3], [6].
2. **Network layer:** This is the middle layer of IoT architecture. This layer takes the processed data received from the Perception layer and transmits it to IoT hubs, applications, and devices using integrated networks. In this layer, several devices, such as hubs, Internet gateways, switching and cloud computing platforms, etc., are integrated with different existing communication technologies, such as WiFi, LTE, Bluetooth, 3G etc. [3], [6].
3. **Application layer:** This is the top layer of IoT architecture. It receives data from the Network layer and provides or delivers to the user the basic functionality for which the IoT system was designed [4], [6].

Moreover, researchers have introduced some other IoT architectures. In [6], a four-layer SoA-based architecture was discussed that involved a new layer, called the service or middleware layer, added between the network layer and application layer. This service layer is responsible for storing, analyzing, and processing the data received from the network layer [2]. Also, a five-layer architecture exists in which a new layer called the business layer is added on top of the application layer [2], [6]. Because the three-layer architecture is common, this paper survey will focus on this architecture.

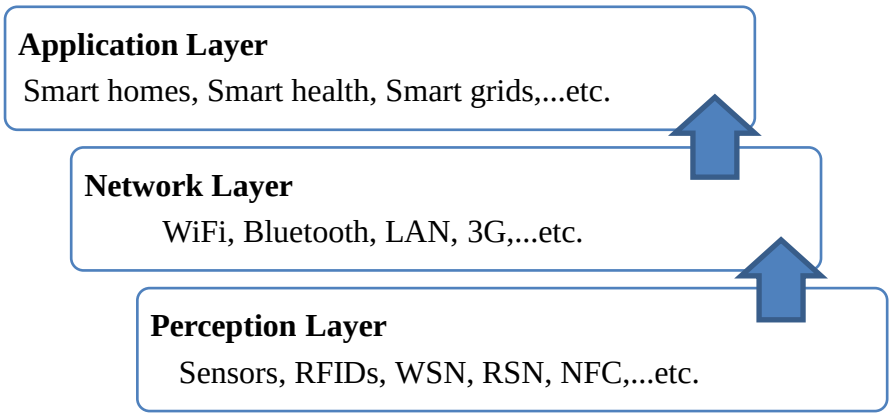

Fig.1. Three-layer IoT Architecture Based on [5], [7], [25]

3 Security in IoT

IoT security is very difficult to achieve. In this section, we mainly address why IoT security is very challenging. This section consists of two main parts: first, we identify the key differences between Internet security and IoT security; second, we present the factors that makes IoT security very challenging and outline basic characteristics of IoT security solutions.

3.1 IT Security vs. IoT Security

One of the differences between traditional Internet security and IoT security is that the parties in communication are different. The Internet is designed to connect humans with computers, but IoT expands this concept to add interconnections between devices and devices, or what is called machine-to-machine communication (M2M) [3], [10]. Naturally, when the communication circle expands, the protection requirements become more complex.

IoT users are unable to add any security software to IoT devices in order to secure and protect them, unlike the case in IT, in which they can install security software. Therefore, IoT devices must be designed to be secure from the beginning, i.e., designed with Built-in-Security [4].

Moreover, IoT devices, such as sensors, are usually located in open areas, so the proposed security solutions for IT devices in closed areas do not work well. Also, since IoT devices are often physically unavailable, it is hard to overcome any security issues. For example, when an attack happens, people cannot get to the IoT devices to reset or stop them. In the case of IT security, people can reset their PC or reinstall the system [4].

IoT devices have limitations in computational power, battery, and memory, which is not the case in IT. Therefore, IoT security solutions should be lightweight algorithmic solutions. Finding the right algorithm that meets these limitations and provides high security is a challenge [3], [4], [10].

3.2 Factors Makes Achieving IoT Security Challenge

The key factor that make the IoT security very challenging is its ubiquitous and heterogenous nature. Many devices with different technologies are integrated into IoT. Further, these devices often connect

in heterogenous environments with dynamic natures where devices connect to different devices from time to time [4]. IoT devices often have constraints in power, computation, and resources, which imposes many restrictions on security solutions [3]. Therefore, any security solution cannot be applied to constrained IoT devices, and specific solutions should be designed.

While IoT integrates many heterogenous technology, every technology has its own security issues that in turn affects the security in IoT [4]. For example, RFID, which is a basic unit in IoT systems, has many security issues, such as eavesdropping, that must be considered to secure IoT systems [25]. Similarly, the TCP, WAN, and IPSec communication technologies that are used in the transport layer can present security threats to IoT systems [25].

Based on the above, the main characteristics of IoT security solutions are summarized as follows [25]:

- Lightweight
- Lower computational and power consumption
- Requires low memory

4 IoT Security Requirements

Since achieving security in IoT is a big challenge, due to the reasons discussed in section 3, it is necessary to define and determine the key features and aspects that should be present in secure IoT systems. In general, there are three essential keys of security, i.e., the CIA triad, that should be applied and satisfied by secure IoT: Confidentiality, Integrity, and Availability [4]. Below is a brief description of these security principles.

1. **Confidentiality** means the IoT system must be able to keep, preserve, and secure a user's private and sensitive information from unnotarized access [3], [4], [6]. Confidentiality in IoT doesn't mean only securing data from other users, but also from all other devices [3].
2. **Integrity** means the IoT system must be able to protect data and information from any changes through intended or unintended interventions during transmission and delivery [3], [4], [6].
3. **Availability** means the IoT system and data must be available and reachable for the user at any requested time, even during harmful situations [3], [4], [6].

While many researchers agree on these three security principles in IoT [3], [4], [6], [7], [9], some researchers [3], [5], [6] have introduced more aspects to be considered in IoT security of which the most important are:

4. **Identification and Authentication** which mean the ability of an IoT system to identify authorized and unauthorized devices or applications, prevent unauthorized ones from connecting to the system, and authenticate authorized ones using different techniques [3], [6].

In general, what it is important is designing a secure and solid system that is fortified against all expected attacks and threats, able to maintain the integrity of the data and the privacy of the user and has the capability of performing the task for which it was designed without any errors or problems. Also, in case the system is attacked, it should be designed to be able to recover to its normal functionality quickly with the least amount of losses in data, devices, and users.

5 Security Threats in Each Layer

In section 2, we presented the structure of three-layer IoT systems and detailed the functionality of each layer. Each layer in IoT is subject to different attacks or risks, although some attacks are not exclusive to a specific layer and may appear in any layer, such as Denial of Service Attack (DoS) [3]. In this section, we present in detail the common potential threats and attacks in each layer of the three-layer IoT architecture.

5.1 Perception Layer

The perception layer is responsible for collecting information and data using technologies like RFID, WSN, sensors, etc. The security of the perception layer is often difficult and complicated [4]. In the perception layer, the risk is not limited to cyber-attacks, as physical attacks are also possible. The sensors that read data are often found in open areas, exposing them to the risk of the physical manipulation of hardware components by attackers, which in turn affects the system and its outputs [3]. In addition, limitations in computing, power, and storage in this layer increase the risk of being attacked [3]. Also, the signals transmitted between the sensors can be easily destroyed [3]. The perception layer is vulnerable to the following attacks:

- **Node Capture Attack:** This is a physical attack in which the attacker captures a node and controls it physically. The attacker might change or replace the capture node or manipulate the hardware components of the node or the IoT device. In this case, the attacker can get important and sensitive data from the captured node, such as routing tables, radio key, group communication key, etc. Also, the attacker can inject false data in the captured node, which in turn leads to the transmission of erroneous data in the system and affects the correctness of the IoT application's provided services [1], [3], [4], [6].
- **Malicious Code Injection Attack:** Like Node Capture attack, this is also a physical attack. The attacker adds a node to the IoT system with malicious code or data in its memory. By injecting malicious code, the attackers can not only force the system to do specific functions, but also can get full control of the whole system [1], [4], [6].
- **Denial of Service Attack (DoS):** This is a prevalent attack that can happen in all IoT layers. The attacker makes the service unavailable by draining the system's resources [1], [3], [4], [6], [7].
- **Replay Attack:** In this attack, the attacker uses valid identification information that was received previously by the destination host. Using this valid identification information, the attacker can get the trust of the system and can use a malicious node to send a package to the destination host [1], [3], [6].
- **Side Channel Attack (SCA):** In this attack, the attacker gets the encryption key by analyzing the IoT system's physical implementation. Attackers usually exploit leaks in time consumption, electromagnetic radiation, or power consumption to get the encryption key. The timing attack is a type of SCA attack in which the attacker gets information by analyzing the execution time of the encryption algorithm [1], [6].
- **Sleep Deprivation Attack:** In this kind of attack, the attacker exploits the limitations of IoT devices. IoT devices are designed to enter sleep mode to decrease power consumption. The attacker get access to these devices and changes their sleeping procedures to make them awake all the time. Therefore, after a while, these devices consume all their energy and turn off; as result, the system becomes unavailable [6], [7].
- **Data Eavesdropping and Inference:** Since communication in IoT systems is through wireless communication channels, it is possible that sent data be eavesdropped by attackers. Also, the

attacker could send interference data or signals to distort the original data, so it becomes inaccurate [6], [7].

- **Routing Threats:** Some routing threats can be performed by an attacker by making routing loops, shortening or extending the source path, generating error massages, partitioning the network, or increasing the delay of sending packets from source to destination [1], [4], [6], [12].

5.2 Network Layer

The network layer is vulnerable to many of the usual attacks that were mentioned in section 5.1, such as DoS attacks and eavesdropping attacks, that violate the integrity, confidentiality, and privacy of data [1]. Some common security attacks in the network layer are:

- **Man-in-the-Middle Attack:** In this attack, the attacker uses malicious nodes or devices between two devices or nodes in the IoT system to intercept and eavesdrop on communication between them and get needed information. This attack is established only on the communication protocols used by IoT systems. By this attack, the privacy, confidentiality, and integrity of data are violated [6].
- **Sybil Attacks:** In this attack, a Sybil node or device can forge a different identity in IoT system. Since the node has different identity, it can send false data to all other devices in the network and get accepted by them [6].
- **Sinkhole Attack:** The attacker makes a malicious node or device attractive by pretending that it has a distinctive specification, such as computational power, that makes the other nodes select this node as the forwarding node to route their data. Therefore, the attacker can collect data before it is delivered to the IoT system. This attack violates confidentiality and can lead to other attacks, such as a DoS attack [6], [7].

5.3 Application Layer

The application layer is vulnerable to the following attacks:

- **Phishing Attack:** In this attack, the attacker exploits the user's opening of phishing emails or websites and obtains the user’s credentials and sensitive information [6], [7].

- **Malicious viruses, worms, or scripts:** The attacker spreads malicious viruses or worms into IoT applications in order to obtain, destroy, or change a user's sensitive information. Malicious scripts are similar; whenever the user runs a script, the attacker gets access to the user's information [6].

6 Security Measures for Each Layer

As we showed in the previous section, each layer in an IoT system is vulnerable to many different attacks that can put the IoT system at risk. Each attack can be prevented using different techniques. The authors in [7] presented a security architecture for three-layer IoT architecture and showed possible policies and mechanisms that can be applied to each layer to achieve security requirements. Figure 2 shows IoT security architecture.

A brief description of these policies and mechanisms in terms of the security measurements of each layer follows [7]:

6.1 Perception Layer

The security of the perception layer includes:

1. **Authentication:** Using cartographic algorithms, such as Hash algorithms, and access control policies ensures the security of the layer and its resistance to many attacks, such as side-channel attacks [7].
2. **Data Privacy:** Data privacy can be compromised when data is collected or transmitted to the next layer. Applying symmetric or asymmetric encryption algorithms, such as RSA, DSA, DES, and BLOWFISH, will stop and prevent any unauthorized access to data and ensure privacy. Regarding the privacy of sensitive data or information, such as a user's personal information or location, applying a K-anonymity approach will protect and secure the data [7].
3. **Risk Assessment:** This is a very important policy for IoT security. Risk Assessment prevents the system from any possible attacks or threats by identifying new possible attacks to the system and providing the best securing strategies. A Dynamic Risk Assessment is an example of a risk assessment method for IoT [7].

4. **Intrusion Detection:** It is important for a system to be able to detect any intrusion and take appropriate actions to stop this intrusion and protect the system. For example, if an intrusion is detected, a kill-command is automatically sent from the RFID reader to the RFID tag to prevent access to the data [7].

6.2 Network Layer

The security of the network layer includes:

1. **Authentication:** Proper point-to-point (P2P) encryption and authentication mechanisms will prevent any illegal access to the sensor nodes [7].
2. **Routing Security:** Routing security is ensured by providing multiple paths for routing, so in the case of an error, the system can keep working, even with failure [7].
3. **Data Privacy:** Data privacy can be achieved by monitoring the system to detect any intrusions and then applying data integrity methods to ensure the integrity of the data [7].

6.3 Application Layer

The security of the application layer includes:

1. **Authentication:** The authentication process can be achieved by using integrated identity identifications. The authentication process in this layer is the same as the other layers, except that in the application layer the authentications are performed by the cooperation of some certain services, which means the user can select the information that is shared with services [7].
2. **Intrusion Detection:** Different techniques could be used for intrusion detection, like the data mining approach and anomaly detection [7].
3. **Risk Assessment:** Risk Assessment is a sufficient mechanism. It helps in the assessment and improvement of current security policies [7].
4. **Data Security:** Data can be protected from stealing and phishing attacks by applying different encryption mechanisms. Also, malicious virus, worms, and scripts could be prevented using up-to-date anti-spyware, anti-malware, and firewall software [7].

ISSN: 2663-5798

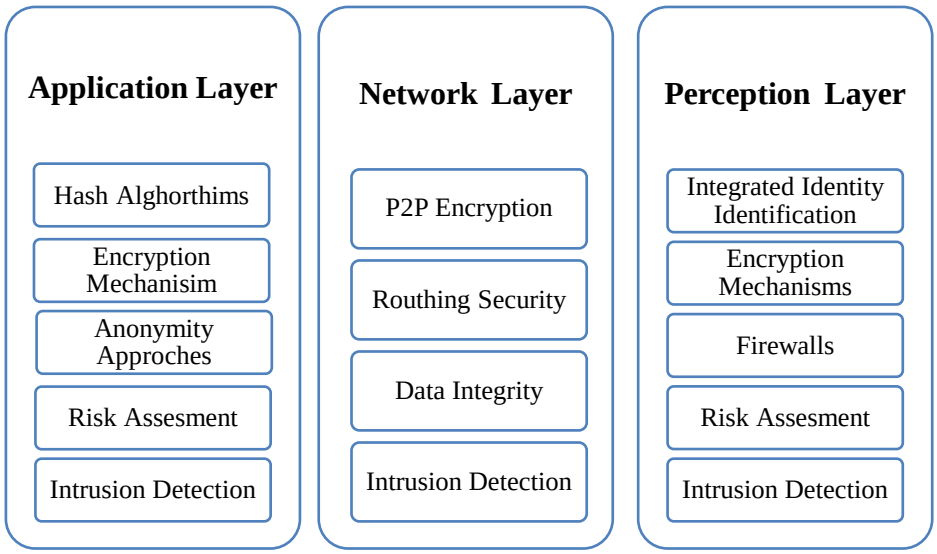

Fig.2. IoT Security Architecture Based on [7]

While different mechanisms could be applied to enforce security in each layer, adding all these solutions together is not enough to achieve security in IoT systems. As a matter of fact, in designing IoT security solutions, the system as a whole should be considered. One way to improve the security of IoT is designing security solutions for across-layer usage, which will reinforce cooperation, integration, and interoperability between IoT layers [4].

7 IoT Proposed Security Solutions

In the previous sections, we discussed in detail security requirements and measurements in IoT by considering all possible threats and attacks to which IoT systems are exposed. In this section, we present up-to-date existing solutions (from 2015 to 2017) for IoT security issues and highlight their contributions to IoT security. We discuss these solutions from two perspectives: first, we present existing solutions in general that fulfill the IoT security requirements; second, we present security solutions specific to the IoT applications of smart health and smart cities. A summary of these solutions is presented in Table 1.

7.1 General IoT Solutions

A Datagram Transport Layer Security (DTLS) based security architecture was proposed by Lessa dos Santos et al. in [13]. The proposed architecture allows constrained devices to communicate with Internet devices using DTLS with mutual authentication. To allow this communication, the authors proposed a third part device called Internet of Things Security Support Provider (IoTSSP), which is

responsible for: (1) controlling both the cryptographic keys and certificates of constrained devices, (2) analyzing Internet device's certificate, and (3) authenticating both the Internet and the constrained devices, thus establishing a secure session, and transferring it to the constrained device. Along with IoTSSP, two mechanisms have been proposed: (1) Optional Handshaking Delegation mechanism, which assigns to IoTSSP the DTLS handshaking process; (2) Transfer of Session mechanism, which is an extension of DTLS that is responsible for transferring the secure communication to the constrained device. This proposed architecture lowers the risk of Denial Service Attacks [13]. Also, this solution addresses all security requirements: confidentiality, integrity, availability, and authenticity [5].

Salman et al. in [14] proposed for heterogenous IoT an Identity-Based Authentication scheme using Software Defined Networking (SDN). The scheme architecture consists of three parts: (1) things, (2) gateway, and (3) controller. Each set of IoT devices (things) has a controller who has a full knowledge of its devices and has access to central data. The message must go through three phases for authentication. In the first phase, the gateway obtains an authentication certificate from the controller. Then, in the second phase, IoT devices (things) register themselves in the gateway. The third phase is the authentication phase, in which things request authentication from the gateways. This proposed solution shows that the scheme is invulnerable to man-in-the-middle attacks, replay attacks, and masquerade attacks [14].

A scalable security solution with symmetric keys (S3K) was implemented by Raza et al. [15]. They provided a lightweight, feasible, and scalable key management architecture for DTLS protocol in constrained IoT devices. The main idea of S3K is to initiate shared keys only between resource constrained devices and trusted anchor. A trusted anchor is a third-party used by a constrained device and client when they want to initiate a trusted relationship. A client initiates a trusted relationship with the resource constrained device by asking for a key from the trusted anchor. Then, the client obtains a public or a secret key from trusted anchor that then transferred to the resource constrained device. This solution ensures the key's integrity, confidentiality, and is immune to DoS attacks and battery drain attacks [15].

To control the access of data in IoT, an extended Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was proposed by Oualha and Nguyen [16]. A CP-ABE schemes provides flexible and powerful access control solution; however, it consumes more energy, so it cannot be used with resource-

constrained IoT devices. The authors proposed a solution to overcome the energy consumption in previous CP-ABE encryption algorithms by using an extension scheme with pre-computational techniques that lower energy consumption, which is a desirable in IoT devices. The proposed extension scheme was proven to be secure and can resist the birthday attack [16].

Khemissa and Tandjaoui [17] presented a lightweight mutual authentication solution for IoT systems that uses Wireless Sensor Networks (WSN). This authentication scheme ensures secure interconnection between the sensor node and remote user by using: nonces, exclusive or operations, and Keyed-Hash message authentication (HMAC). A successful mutual authentication between the sensor node and remote user requires before data transmission to a remote user, then a session key is established to grantee the secure communication. The scheme was proven to be energy efficient and invulnerable to DoS attacks, replay attacks, and sensor node impersonation attacks. Moreover, the design of the scheme accounts for the following security features: mutual authentication, data integrity, identity protection, and key establishments [17].

Shi et al. [18] developed a lightweight authentication protocol for Radio Frequency IDentification (RFID) systems. Their protocol encrypts all messages between the tag and the reader using CRC function, and randomizes all sessions using a pseudorandom number generator. The proposed protocol is suitable for EPCglobal Class-1Gen-2 tags, which exploit its on-chip CRC function. This protocol requires low computation and storage, which make it a feasible solution for passive tags. This protocol ensures the forward security, privacy, and confidentiality of RFID systems. Also, it is resistant to eavesdropping, tracing attacks, replay attacks, spoofing, and de-synchronized attacks [18].

One recent idea that addresses IoT security in a novel way was presented by Barbosa et al. Position paper [26]. These researchers suggested a unified IoT architecture called SAFETHINGS that enables data privacy and security in IoT systems by design. They suggested a fixable architecture that can handle IoT heterogeneity while integrating communication, storage, processing, and security of data in IoT systems from the beginning. SAFETHINGS architecture is meant to be modular in order to allow different approaches and different techniques for data privacy and security to integrate and cooperate to provide the needed level of data security [26].

This suggested architecture consists of three simple concepts: data cleaning, data blending, and data exchanging. The cleaners are responsible for data privacy and security, the blenders for data analysis,

and the exchangers for exchanging the data. The data exchangers are in the middle, between the cleaners and blenders, and are responsible for the data flow between them. The novelty of this work is that each component has it is own predefined working logic that permits different implementations to integrate both legacy and new applications. Three entities are involved in the SAFETHINGS workflow: producers, consumers, and resource providers. These entities can be applications, users, or things. The workflow of a SAFETHINGS-based application is: a row of data is produced by the producer, which then goes to the SAFETHINGS cleaner, which generates protected data using filtering, encryption, or converting the data into anonymous data. After that, the protected data goes to the SAFETHINGS exchanger, which allows consumers or the SAFETHINGS blender to get access to the data. Then, the blender or a chain of blenders process the data and generate an aggregated knowledge to the consumer or back again to the exchanger [26].

This is a very recent proposal, so the extent to which it is possible to implement or apply is still not clear. As a concept, it is a good and innovative solution because it has the advantages of different solutions for different challenges and integrates them together, which in turn may lead to powerful systems that are strongly protected. However, an open question is whether this unified architecture can always be used with different applications and different security and privacy requirements.

7.2 Application-Specific Solutions

In this section, we highlight some of the up-to-date solutions for IoT security in certain applications. Specifically, we address some of the latest solutions in the healthcare and smart homes domains.

1. Healthcare Domain

Joshitta and Arockiam [20] proposed a secure device authentication scheme with key agreement for constrained medical devices. The authentication process goes through three phases: Registration phase, Login phase, and Authentication phase. The Registration phase includes the registration of the patient and the medical device. The identities of the medical device and the patient are checked in the Login phase before starting the Authentication phase. Only successful verifications start the Authentication phase. The authentication mechanism uses a Neeva one-way hash function and the Electronic Product Code (EPC) of the medical device. The authors compared their scheme with similar

schemes in terms of security features fulfillment and attack vulnerability, which showed the novelty of the presented scheme. The presented authentication mechanism provides security requirements such as data integrity, privacy, protection, and forward security, and is immune to several attacks, such as DoS attacks, man-in-the middle attacks, eavesdropping, etc. [20].

Fan et al. [21] presented another security solution for medical devices. The authors addressed the security and privacy of medical data and proposed a secure RFID protocol for medical systems. By ensuring tag anonymity, the privacy of patients' medical data achieved. This protocol is lightweight, has low resource consumption, and provides mutual authentication and forward security. More importantly, it is resistant to DoS attacks, replay attacks, and synchronization attacks [21].

2. Smart Homes Domain

Kumar et al. [22] implemented a secure scheme for smart home environments. This scheme is lightweight and provides secure session key establishment which make it a feasible solution for constrained smart devices in the home environment. Each device or sensor should establish mutual authentication and a secure session key before getting involved in a home's network. This scheme allows new devices to join the home's network easily and securely, and can be used in different contexts in a home, such as a light system, smart energy system, appliance control system, etc. A hash function and a symmetric key cartography are used in this scheme. The scheme was proven to be resistant to masquerade attacks, message-forgery attacks, replay attacks, known-key attacks, DoS attacks, and device compromised attacks. Also, it showed confidentiality, integrity, and freshness of messages [22].

Ashibani and Mahmoud [23] proposed an Identity-Based Signcryption (IBS) scheme for smart home communication. Their proposed singcryption scheme was based on Identity based cryptography (IBC) and uses short keys, which gives a low-cost scheme suitable for constrained devices in smart home environments. IBS has four steps: (1) system initialization, (2) registration, (3) singcryption, and (4) unsignryption. During the authentication process, the scheme does not require access to third-party devices, which is only required during the updating of secret keys or registration. This scheme provides authentication, integrity, and confidentiality for data transmitting, and is resistant against several attacks, such as replay attacks [23].

Table 1. Summary of discussed IoT security solutions

Year & Reference	Proposed Security Solution	Remark	Resistant Against	Domain
2015 [13]	A DTLS-based security architecture	Using IoTSSP, mutual authentication	DoS attack	General
2016 [14]	Identity-based authentication scheme	Based on SDN	Man-in-the-middle attack, replay attack, masquerade attack	General
2016 [15]	S3K: scalable solution with symmetric keys-DTLS key establishment	Lightweight solution	DoS attack, battery drain attack	General
2016 [16]	Lightweight Attribute-Based Encryption	Access control, extension to CP-ABE	Birthday attack	General
2016 [17]	A novel authentication scheme for heterogeneous WSNs	Mutual authentication, key establishment, energy efficient	DoS attack, replay attack, rensor node impersonation attack	WSNs
	A lightweight authentication protocol for RFIDs	Using CRC function for encryption		

2017 [18]			Eavesdropping, tracing attack, replay attack, spoofing and de-synchronized attacks	RFIDs
2017 [26] (position paper)	SAFETHINGS: data security by design in the IoT	Unified IoT architecture, modular architecture	-	General
2017 [20]	Device authentication mechanism for IoT enabled healthcare system	Using EPC of medical devices	DoS attack, man-in-the middle attack, eavesdropping	Healthcare
2017 [21]	Lightweight RFID protocol for medical privacy protection	Mutual authentication	DoS attack, replay attack, synchronization attack	RFIDs in healthcare
2016 [22]	Lightweight and secure session-key establishment	Mutual authentication	Masquerade attack,	Smart homes

	scheme in smart home environments		message-forgery attack, replay attack, known-key attack, DoS attack, device compromised attack	
2017 [23]	Efficient and secure scheme for smart home communication using identity-based signcryption	Based on Identity Based Cryptography (IBC)	Replay attack	Smart Homes

8 Discussion and Future Research Directions

Security in IoT is not an easy job. It is a difficult and complex challenge. From the time of IoT's emergence, much research and many solutions have been published in IoT security in attempts to close the gaps in IoT systems' security and achieve the desired security requirements to make IoT useful and practical. Despite the many existing solutions for securing IoT systems in terms of devices, data, and communications, it is expected that the increasing number of connected devices and widespread use of IoT applications will cause new problems and reveal security gaps in previous solutions. Therefore, there is a need for new solutions to suit the fast pace of evolution and change in IoT. In this section, we discuss some open issues in IoT security that can be addressed by future research.

IoT applications vary, and new applications are expected to appear in the coming years. In view of applications from smart homes, smart grids, smart transportation, smart health, etc., it observes that

every application domain requires or needs different security requirements. For example, in smart health data, privacy is more important, while data authenticity is more important in smart cities. Hence, application-specific security solutions are needed for each specific application domain [24].

IoT physical devices are vulnerable to many threats and attacks that can affect IoT services. Thus, designing anti-theft policies should be considered. Not only that, but it is necessary to introduce policies to deal with IoT systems in the event of any attack. For example, if it is discovered that a device is stolen, it should be immediately blocked from the system to protect the rest of the devices and maintain data privacy [24].

While the number of IoT devices is growing and expected to grow more, a delay in communication between devices is expected, due to the heavy traffic. The current communication technology is 4G, with speeds ranging from 2 to 1000Mbps. Using 5G protocol for communication between IoT devices could solve the delay, since it provides speeds between 10 and 800Gbps. Also, 5G is expected to support both IPv4 and IPv6. Considering the security of the 5G protocol in IoT could be a direction for future research [3].

The lack of architecture standards is still a huge issue in IoT that affects IoT security. There is a need for unified architecture standards, including data standards, wireless protocols, and technologies, to allow the integration and communication of different devices while achieving high security [3], [8].

In this work, we highlighted the most recent research in IoT security. While there is much research on IoT security that addresses the availability, integrity, authenticity, and confidentiality of IoT, some issues in IoT security are still open and not fully addressed, such as huge data security, energy consumption, energy efficiency, software and hardware security, and scalability [5].

9 Conclusion

IoT is one of the most important emerging technologies. It has started to dominate our lives and become present everywhere. This field is expected to grow significantly in the upcoming years. The security of IoT systems is essential and important to consider from the beginning of systems design. The lack of security in IoT systems allows unauthorized people to access data, violate the privacy of

others, play with data, and damage it [25]. As the number of connected devices increases, the challenge to protect and secure them also increases.

This paper can be considered as an entry point to the subject of IoT security. It could serve as an appropriate reference for new researchers in this field, giving a comprehensive view of security in IoT, including IoT security requirements, possible threats, current security solutions, and future research directions.

References

K. Zhao and L. Ge, "A Survey on the Internet of Things Security," *2013 Ninth International Conference on Computational Intelligence and Security*, Leshan, 2013, pp. 663-667.

P. Sethi and S. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1-25, 2017.

R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 336-341.

M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and Future challenges," in *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1-1.

A. Oracevic, S. Dilek and S. Ozdemir, "Security in internet of things: A survey," *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, Marrakech, 2017, pp. 1-6.

J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

M. U.Farooq, M. Waseem, A. Khairi and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1-6, 2015.

S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," *2016 Future Technologies Conference (FTC)*, San Francisco, CA, 2016, pp. 731-738.

M. Abdur, S. Habib, M. Ali and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017.

Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

K. Ashton, "That 'Internet of Things' Thing - 2009-06-22 - Page 1 – RFID Journal", *Rfidjournal.com*, 2018. [Online]. Available: http://www.rfidjournal.com/articles/view?4986. [Accessed: 11- Mar- 2018].

P. P. Lokulwar and H. R. Deshmukh, "Threat analysis and attacks modelling in routing towards IoT," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017, pp. 721-726.

G. Lessa dos Santos, V. T. Guimarães, G. da Cunha Rodrigues, L. Z. Granville and L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things," *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, 2015, pp. 809-815.

O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," *2016 IEEE Symposium on Computers and Communication (ISCC)*, Messina, 2016, pp. 1109-1111.

S. Raza, L. Seitz, D. Sitenkov and G. Selander, "S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things," in *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1270-1280, July 2016.

N. Oualha and K. T. Nguyen, "Lightweight Attribute-Based Encryption for the Internet of Things," *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, Waikoloa, HI, 2016, pp. 1-6.

H. Khemissa and D. Tandjaoui, "A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of Internet of Things," *2016 Wireless Telecommunications Symposium (WTS)*, London, 2016, pp. 1-6.

Z. Shi, J. Chen, S. Chen and S. Ren, "A lightweight RFID authentication protocol with confidentiality and anonymity," *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Chongqing, 2017, pp. 1631-1634.

M. Barbosa *et al*., "SAFETHINGS: Data Security by Design in the IoT," *2017 13th European Dependable Computing Conference (EDCC)*, Geneva, 2017, pp. 117-120.

R. S. M. Joshitta and L. Arockiam, "Device authentication mechanism for IoT enabled healthcare system," *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, Chennai, 2017, pp. 1-6.

K. Fan, W. Jiang, H. Li and Y. Yang, "Lightweight RFID Protocol for Medical Privacy Protection in IoT," in *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1-1.

P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila and M. Sain, "Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments," in *IEEE Sensors Journal*, vol. 16, no. 1, pp. 254-264, Jan.1, 2016.23

Y. Ashibani and Q. H. Mahmoud, "An efficient and secure scheme for smart home communication using identity-based signcryption," *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, San Diego, CA, USA, 2017, pp. 1-7.

"Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", *Gartner.com*, 2017. [Online]. Available: https://www.gartner.com/newsroom/id/3598917. [Accessed: 11- Mar- 2018].

A. Punia, D. Gupta and S. Jaiswal, "A perspective on available security techniques in IoT," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, 2017, pp. 1553-1559.

M. Barbosa *et al*., "SAFETHINGS: Data Security by Design in the IoT," *2017 13th European Dependable Computing Conference (EDCC)*, Geneva, 2017, pp. 117-120.