



Article

IoT Privacy and Security: Challenges and Solutions

Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh and Muhannad Quwaider

Special Issue

Fog Computing for Intelligent IoT Applications

Edited by

Assoc. Prof. Dr. Vlado Stankovski and Prof. Dr. Marko Bajec



Article

IoT Privacy and Security: Challenges and Solutions

Lo'ai Tawalbeh ^{1,*}, Fadi Muheidat ² , Mais Tawalbeh ³ and Muhannad Quwaider ³¹ Department of Computing and Cyber Security, Texas A&M University, San Antonio, TX 78224, USA² School of Computer Science & Engineering (CSE), California State University, San Bernardino, CA 92407, USA; Fadi.muheidat@csusb.edu³ Department of Computer Engineering, Jordan University of Science and Technology, Irbid 22110, Jordan; matawalbeh18@cit.just.edu.jo (M.T.); mqquwaider@just.edu.jo (M.Q.)

* Correspondence: Ltawalbeh@tamusa.edu

Received: 10 May 2020; Accepted: 10 June 2020; Published: 15 June 2020



Abstract: Privacy and security are among the significant challenges of the Internet of Things (IoT). Improper device updates, lack of efficient and robust security protocols, user unawareness, and famous active device monitoring are among the challenges that IoT is facing. In this work, we are exploring the background of IoT systems and security measures, and identifying (a) different security and privacy issues, (b) approaches used to secure the components of IoT-based environments and systems, (c) existing security solutions, and (d) the best privacy models necessary and suitable for different layers of IoT driven applications. In this work, we proposed a new IoT layered model: generic and stretched with the privacy and security components and layers identification. The proposed cloud/edge supported IoT system is implemented and evaluated. The lower layer represented by the IoT nodes generated from the Amazon Web Service (AWS) as Virtual Machines. The middle layer (edge) implemented as a Raspberry Pi 4 hardware kit with support of the Greengrass Edge Environment in AWS. We used the cloud-enabled IoT environment in AWS to implement the top layer (the cloud). The security protocols and critical management sessions were between each of these layers to ensure the privacy of the users' information. We implemented security certificates to allow data transfer between the layers of the proposed cloud/edge enabled IoT model. Not only is the proposed system model eliminating possible security vulnerabilities, but it also can be used along with the best security techniques to countermeasure the cybersecurity threats facing each one of the layers; cloud, edge, and IoT.

Keywords: Internet of Things; security policy; cloud computing; edge computing; privacy

1. Introduction

The Internet of Things (IoT) refers to a concept of connected objects and devices of all types over the Internet wired or wireless. The popularity of IoT or the Internet of Things has increased rapidly, as these technologies are used for various purposes, including communication, transportation, education, and business development. IoT introduced the hyperconnectivity concept, which means organizations and individuals can communicate with each other from remote locations effortlessly. Kevin Ashton invented the term 'IoT' in the year 1999 for promoting the Radio Frequency Identification (RFID) concept, which includes embedded sensors and actuators. However, the original idea was introduced in the 1960s. During that period, the idea was called pervasive computing or embedded Internet. Ashton presented the IoT concept to improve supply chain activities. However, diverse functionalities of IoT has helped it to gain strong popularity in the summer of 2010. The Chinese government gave strategic priority on IoT by introducing a five-year plan. About 26.66 billion IoT devices exist in the current world [1]. The mass explosion started in 2011 with the introduction of home automation, wearable devices, and smart energy meters. The rapid explosion of IoT has benefitted

organizations and in various ways improved market research and business strategies. Similarly, IoT has improved the lifestyle of individuals by introducing automated services. However, such an uncontrolled explosion has increased privacy and security challenges.

The unconscious use, not changing passwords, and the lack of device updates have increased cybersecurity risks and access to malicious applications to the IoT systems' sensitive data. Such inappropriate security practices increase the chances of a data breach and other threats. Most of the security professionals consider IoT as the vulnerable point for cyber attacks due to weak security protocols and policies. Even though several security mechanisms were developed to protect IoT devices from cyber attacks, security guidelines are not appropriately documented [2]. Thereby, end-users could not utilize protective measures to avert data attacks. Hackers developed different kinds of malware to infect the IoT devices since the eve of 2008. They designed various phishing techniques to provoke the employees or individuals to share sensitive data [3]. Therefore, corporate workstations and personal devices often face privacy violations due to high-profile attacks. If device manufacturers and security experts assess the cyber threats accurately, they can develop an efficient protective mechanism to prevent or neutralize cyber threats.

IoT enabled devices have been used in industrial applications and for multiple business purposes [4]. The apps help these businesses to attain a competitive edge over their competitors. However, due to the excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services. It is essential to have professionals to overcome these threat concerns and develop comprehensive security measures and policies to protect their business assets and ensure services continuity and stability. For example, smart kitchen home IoT enabled appliances connected to the local network can be a source of the breach for hackers to get access to the business and/or personally sensitive data or to manipulate and interrupt the business workflow.

Every day new technologies emerge, or changes are made to existing ones. Consider the latest advances in the 5G network, for example. 5G is expected to play an essential role in the IoT systems and applications. It is getting the researchers' attention and curiosity about the possible security and privacy risks, with its high frequency and bandwidth. Yet, the short wavelength imposes a change in the infrastructure, hence the need for more base stations to cover the same area covered by other wireless technology. This new structure imposes more threats, such as fake base stations. It is essential to understand the security risks and potential solutions.

In this work, we aim to provide an overview of the IoT applications, benefits, and potential risks. Additionally, to build a framework to study and further develop best security practices by either implementing and analyzing current existing schemes or developing new ones. Based on the findings, we provide recommendations to avoid such risks and to remedy the possible security vulnerabilities. This work will guide regulatory agencies to continue enforcing policies, educating end-users and entities, and stakeholders involved in IoT to develop and apply more appropriate security and privacy measures.

We built our model using Amazon Web Service (AWS) as proof of concept, which later translated to actual physical systems of sensors nodes mimicking general IoT structure. By making the system, we can deploy and study different security approaches by building real sceneries and benchmarks.

We adopted a narrative review methodology to explore the history and background of the IoT systems, their security and privacy issues, and the corresponding countermeasures. We proposed our own view of the generic and stretched IoT model and its privacy and security concerns. We built and studied a cloud/edge supported IoT model consisted of a virtual machine (sensors), and edge node (Raspberry Pi), and cloud services (AWS). This setup was designed to evaluate the model we proposed in the following sections in this paper. Our work does not provide details on the different IoT applications (smart health, smart cities, supply chain, transportations, etc.); their features, advantages, and challenges, or the possible security risks or threats among these applications. The literature is rich

with such content. In this work, we preferred to have a general overview with proof of concept and lay the ground for further analysis and investigations.

The rest of this paper organized as follows: the next section presents a literature review followed by IoT security and privacy challenges. In Section 4, we discuss the future of the Internet of Things. Section 5 presents the proposed cloud/edge supported IoT layered models: generic and stretched with the privacy and security components and layers identification. This section also shows the implementation of the proposed model using AWS cloud and edge environments and Raspberry Pi 4 kit. Section 6 concludes this work.

2. Literature Review

The authors in [5] stated that there are various challenges, such as jamming and spoofing attacks and other unauthorized access, which have compromised the integrity of the user's data. There are potential solutions that can help the individual to implement various security measures that can help to secure their IoT devices. According to [6], various privacy threats have emerged in the present time, and they can penetrate IoT Technologies and their integrated network. It is not easy to manage the security of IoT devices in businesses and organizations. The organizations must deploy monitoring and scanning tools for all the IoT devices that could detect any kind of threats related to privacy and try to mitigate the risk of being breached. Traffic interceptors and analyzers help identify and investigate various cyber threats.

There are various studies as well as services that have been conducted on the current trends in IoT security [7]. Multiple services have presented some of the challenges or attack vectors to various IoT devices and their guards. Various simulation tools, modelers, and the availability of numerous platforms that can confirm this security protocol can also help in producing the protocol related to novel IoT security. It is fair to say that there has been rapid progress in terms of research related to IoT security and various simulation tools as well as modelers have supported this research. If the IoT devices failed, then the issues will be severe.

The authors in [8] believe that, despite the enormous benefits the users are getting from the Internet of Things, there are challenges that come along with it that need to be looked at. Cybersecurity and privacy risks are the primary concerns that have been cited. These two are posing a massive predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet, requiring novel security solutions. On the other hand, it is important to emphasize the standards and basic principles of the IoT Cyber Security Framework when it comes to implementing the IoT security system. According to [9], one of the most important measures to consider is the termination of a contract consisting of different devices with different communication protocols. The difference in protocols hinder separate service contracts from implementation and are fundamental elements that must be present in the cybersecurity structure of every Internet of Things. He demonstrated that to ensure the reliability of the IoT framework in the cybersecurity arena, some small steps need to be taken to help mitigate the challenges of IoT cybersecurity. In addition, the authors in [9] showed that scalability is also an essential measure of the success of the cybersecurity Internet of Things framework. Analysts said the IoT environment needs to be scalable enough to handle a billion Internet-related and cybersecurity challenges. In addition, the magazine showed that the IoT cybersecurity environment should also support testability, such as integration testing, component testing, system testing, and compliance testing, effectively reducing challenges and risks.

In the same context, the authors in [10] described some of the current IoT cybersecurity solutions. Some basic security measures are implemented by the supplier, and state that it is not profitable for the supplier to produce high-quality solutions. In the case of cybersecurity of the Internet of Things, companies are unlikely to develop the right solution.

Moreover, the authors in [11] describe the currently embedded mobile and cyber-physical systems as ubiquitous, from industrial control systems, modern vehicles to critical infrastructure. Current trends and initiatives, such as Industry 4.0 and the Internet of Things (IoT), promise innovative business models and new user experiences through strong connectivity and the effective use of new generations of embedded devices. These systems generate, process, and exchange large amounts of relevant data. Security and confidential beliefs that make cyber attacks an attractive target for the Internet of Things system cause physical harm and disrupt people's lives. Cybersecurity and privacy are important because they can pose a threat. The complexity of these systems and the potential impact of cyber attacks pose new threats to related industrial IoT systems. Possible solutions to security and privacy challenges are general security frameworks for industrial IoT systems. Current IoT systems have not improved enough to secure the desired functions.

Therefore, there has been extreme significance in the study and research of various security issues in IoT. One of the main objectives in terms of IoT security is to provide privacy, confidentiality, and to ensure that every user can get better protection, infrastructures, and a guarantee to the availability of various services offered by the ecosystem of IoT. Therefore, the research in various IoT security is gaining necessary momentum with the help of different simulation tools as well as multiple computational platforms [12].

3. IoT Security and Privacy Challenges

IoT brought users huge benefits; however, some challenges come along with it. Cybersecurity and privacy risks are the primary concerns of the researchers and security specialists cited. These two are posing a considerable predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This vulnerability is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet requiring novel security solutions [13].

Of all the challenges that are known, none of them has a more significant influence on IoT adaptation, such as security and privacy. It is, however, unfortunate that the users do not often have the required acknowledgment of the security impacts until the time when a breach has occurred, causing massive damages such as loss of crucial data. With the ongoing security breaches which have compromised the privacy of users, the appetite of the consumers for poor security is now declining. In a recent review conducted regarding privacy and security, consumer-grade Internet of Things did not do well. There were a lot of vulnerabilities in modern automotive systems.

3.1. Security

The IoT is diverse from traditional computers and computing devices, makes it more vulnerable to security challenges in different ways [14]:

- Many devices in the Internet of Things are designed for deployment on a massive scale. An excellent example of this is sensors.
- Usually, the deployment of IoT comprises of a set of alike or nearly identical appliances that bear similar characteristics. This similarity amplifies the magnitude of any vulnerability in the security that may significantly affect many of them.
- Similarly, many institutions have come up with guides for risk assessment conduction. This step means that the probable number of links interconnected between the IoT devices is unprecedented. It is also clear that many of these devices can establish connections and communicate with other devices automatically in an irregular way. These call for consideration of the accessible tools, techniques, and tactics which are related to the security of IoT.

Even with the issue of security in the sector of information and technology not being new, IoT implementation has presented unique challenges that need to be addressed. The consumers are required to trust the Internet of Things devices and the services are very secure from weaknesses,

particularly as this technology continues becoming more passive and incorporated in our everyday lives. With weakly protected IoT gadgets and services, this is one of the very significant avenues used for cyber attacks as well as the exposure of the data of users by leaving data streams not protected adequately.

The nature of the interconnection of the IoT devices means if a device is poorly secured and connected it has the potential of affecting the security and the resilience on the Internet internationally. This behavior is simply brought about by the challenge of the vast employment of homogenous devices of IoT. Besides the capability of some devices to be able to mechanically bond with other devices, it means that the users and the developers of IoT all have an obligation of ensuring that they are not exposing the other users as well as the Internet itself to potential harm. A shared approach required in developing an effective and appropriate solution to the challenges is currently witnessed in the IoT [14].

When it comes to authentication, for instance, IoT faces various vulnerabilities, which remain one of the most significant issues in the provision of security in many applications. The authentication used is limited in how it protects only one threat, such as Denial of Service (DoS) or replay attacks. Information security is one of the significant vulnerable areas in the authentication of IoT due to the prevalence of applications which are risky due to their natural multiplicity of data collection in the IoT environment. If we can, for instance, take an example of contactless credit cards. These cards are capable of permitting card numbers and names to be read without the authentication of IoT; this makes it possible for hackers to be able to purchase goods by using a bank account number of the cardholder and their identity.

One of the most prevalent attacks in the IoT is the man in the middle, where the third-party hijack communication channel is aimed at spoofing identities of the palpable nodes which are involved in network exchange. Man in the middle attack effectively makes the bank server recognize the transaction being done as a valid event since the adversary does not have to know the identity of the supposed victim [15].

3.2. Privacy

The perspective of the usefulness of the IoT is dependent on how well it can respect the privacy choices of people. Concerns regarding the privacy and the potential harms that come along with IoT might be significant in holding back the full adoption of IoT. It is essential to know that the rights of privacy and user privacy respect are fundamental in ensuring users' confidence and self-assurance in the Internet of Things, the connected device, and related services offered. A lot of work is being undertaken to ensure that IoT is redefining the privacy issues such things as the increase of surveillance and tracking. The reason for the privacy concerns is because of the omnipresent intelligence integrated artifacts where the sampling process and the information distribution in the IoT may be done nearly in any place. The ubiquitous connectivity via the Internet access is also an essential factor that helps in understanding this problem because unless there is a unique mechanism put in place, then it will be decidedly more comfortable to access the personal information from any corner of the world [16].

3.3. Interoperability

A fragmented environment of proprietary IoT technical implementation is known to inhibit value for users. Even though full interoperability is not always feasible across products and services, the users may not like buying products and services where there is no flexibility and concerns over dealer lock-in. Poorly planned IoT gadgets might mean that there will be a negative consequence for the networking resources that they connect to [17].

Cryptography is another essential aspect that has been used for many years to provide defense against security loopholes in many applications [9]. An effective defensive mechanism against the attacks perpetrated is not possible using one security application. It, therefore, requires different layers of security against the threats to the authentication of IoT.

By the development of more advanced security features and building these features into products, hacks may be evaded. This evasion is because the users will buy products that already have proper security features preventing vulnerabilities. Cybersecurity frameworks are some of the measures put forward to ensure that IoT is secure [18].

Moreover, some several factors and concerns might have an impact on compromising the efforts to secure the Internet of Things devices; these include:

- Occasional update: usually, IoT manufacturers update security patches quarterly. The OS versions and security patches are also upgraded similarly [19]. Therefore, hackers get sufficient time to crack the security protocols and steal sensitive data.
- Embedded passwords: IoT devices store embedded passwords, which helps the support technicians to troubleshoot OS problems or install necessary updates remotely. However, hackers could utilize the feature for penetrating device security.
- Automation: often, enterprises and end-users utilize the automation property of IoT systems for gathering data or simplifying business activities. However, if the malicious sites are not specified, integrated AI can access such sources, which will allow threats to enter into the system.
- Remote access: IoT devices utilize various network protocols for remote access like Wi-Fi, ZigBee, and Z-Wave. Usually, specific restrictions are not mentioned, which can be used to prevent cybercriminals. Therefore, hackers could quickly establish a malicious connection through these remote access protocols.
- Wide variety of third-party applications: several software applications are available on the Internet, which can be used by organizations to perform specific operations. However, the authenticity of these applications could not be identified easily. If end-users and employees install or access such applications, the threat agents will automatically enter into the system and corrupt the embedded database.
- Improper device authentication: most of the IoT applications do not use authentication services to restrict or limit network threats. Thereby, attackers enter through the door and threaten privacy.
- Weak Device monitoring: usually, all the IoT manufacturers configure unique device identifiers to monitor and track devices. However, some manufacturers do not maintain security policy. Therefore, tracking suspicious online activities become quite tricky.

4. Future of the Internet of Things

Currently, objects and systems are empowered with network connectivity and have the computing power to communicate with similar connected devices and machines [20]. Expanding the network capabilities to all possible physical locations will make our life more efficient and help us save time and money. However, connecting to the Internet also means to communicate with potential cyber threats. Internet-enabled products become a target for cybercriminals. The expansion of the IoT market increases the number of potential risks, which can affect productivity and the safety of the devices and hence our privacy. Reports highlight the frequencies of data breaches have increased drastically since 2015; 60% in the USA only [21]. Another survey conducted in Japan, Canada, the UK, Australia, the USA, and France discovered that 63% of the IoT consumers think these devices are creepy due to improper security. Research findings also highlighted that 90% of consumers are not confident regarding IoT cybersecurity [22].

Current research explored various innovative techniques to mitigate cyber attacks and increase privacy solutions. Some of the solutions identified through the research are listed below;

Deploying encryption techniques: enforcing strong and updated encryption techniques can increase cybersecurity. The encryption protocol implemented in both the cloud and device environments [23]. Thus, hackers could not understand the unreadable protected data formats and misuse it.

Constant research regarding emerging threats: the security risks are assessed regularly. Organizations and device manufacturers developed various teams for security research. Such teams

analyze the impact of IoT threats and develop accurate control measures through continuous testing and evaluation [23].

Increase the updates frequency: the device manufacturers should develop small patches rather than substantial updates. Such a strategy can reduce the complexity of patch installation. Besides, frequent updates will help the users to avert cyber threats resources from diverse sources [24].

Deploy robust device monitoring tools: most of the recent research proposed to implement robust device monitoring techniques so those suspicious activities can be tracked and controlled easily. Many IT organizations introduced professional device monitoring tools to detect threats. Such tools are quite useful for risk assessment, which assists the organizations in developing sophisticated control mechanisms.

Develop documented user guidelines to increase security awareness: most of the data breaches and IoT attacks happen due to a lack of user awareness. Usually, IoT security measures and guidelines are not mentioned while users purchase these devices. If device manufacturers specify the potential IoT threats clearly, users can avoid these issues. Organizations can also design effective training programs to enhance security consciousness. Such programs guide users to develop strong passwords to update them regularly. Besides, users are instructed to update security patches regularly. The users also taught and requested to avoid spam emails, third-party applications, or sources, which can compromise IoT security [25].

Everybody is looking forward to the fate of IoT and what it is holding for the future. There will be more than 30 billion IoT devices by 2025. Earlier on, people were aware of the IoT project, but they discarded the idea by looking at how the idea looked complex and challenging to implement. However, after the development of technology, it is now dawning on people that this was not impossible as the level of IoT development is scaling new heights day by day. In 2020 and beyond, for instance, intelligent thermostats and smart lighting are a few examples of how IoT is being used not only in the preservation of energy but also in the reduction of the bills and this contributes to the great reason why many people are choosing IoT devices [26].

A lot of cities will become smart. In the development of cities, there will be completely new horizons with the use of IoT. There will be better management of traffic; the roads will be free from congestion, the cities will benefit from reduced pollution, security will be of high standards all this by the implementation of IoT to a large scale.

Healthcare services are becoming much costlier, with the number of chronic diseases on the rise. We are approaching a time where primary healthcare would be complicated to get for many individuals, especially as people are becoming more prone to diseases. However, even though the technology is not capable of stopping the population from aging, it can help in making healthcare easier on the pocket in terms of accessibility [27]. For instance, by moving routine medical checks from the hospital to the patient's home, this will be a massive relief to the patients. Real-time monitoring using devices connected to the Internet of Things is one of the ways that will help save the lives of many patients. On-time alerts are very critical in the instances of life-threatening circumstances, as many medical IoT devices will continue to be connected to gather vital data for real-time tracking. The quality of life of the patients will be significantly improved.

5. Proposed IoT Layered Models

In this work, we propose a new view of the IoT models: generic and stretched with the privacy and security components and layers identification and separation. We built a cloud/edge supported IoT system to implement the proposed IoT models. Therefore, in this work we first introduce the generic and stretched models, then describe our experimental setup and implementation environment (layered model implementation), and then present and discuss the results and findings.

5.1. Generic IoT Layers and Data Fusion Model

The generic architecture of the IoT model, from the authors' perspective, not sure if there are any similar thoughts in literature, as shown in Figure 1, consists of a device, cloud, and end-user layers. The device layer consists of a pool of wireless Internet-enabled sensor devices, data acquisition circuitry, and communication protocols to send data to local or remote storage for further processing. These devices allow the user to collect data in real-time with different acquisition frequencies. The cloud layer hosts the data collected from the sensors for further processing, noise removal, feature extraction, and data massaging. This data is later fed into a decision support system that runs complex data analysis and artificial intelligence to provide a decision regarding the person's health. The end-user layer, consisting of the receiving user, could be in different forms. Of concern is smart devices, where security and privacy challenges exist. Within the boundaries of these three layers, a list of sublayers or modules added to ensure the robustness of the decision support system. To ensure data is sent and processed promptly to provide a critical decision that cannot wait until the data is sent to the cloud, we introduce an edge computing capability that can make such smart decision, and at the same time save a copy of the data and send it to the cloud layer for processing and long-term storage. On certain occasions, we need to send commands or instructions to some wearables devices to update their acquisition rate or functionality, and this will require another protocol and security procedures.

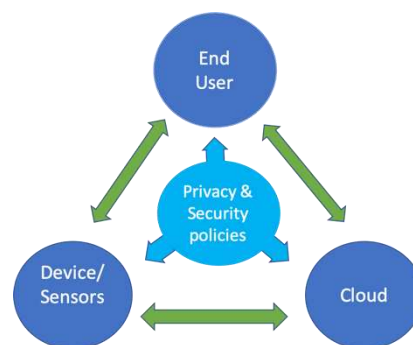


Figure 1. Internet of Things (IoT) generic model with privacy and security policies.

Figure 2 shows the stretched version of the generic model. We can see the addition of the new layers; edge and fog. Both layers can overcome the latency issues from the reliance on cloud layer services and are able to make decisions faster. Edge computing occurs on the devices to which the sensors are attached to or physically close. They provide a real-time decision and control to the data sources, and at the same time, communicate with other layers to transfer the data for fusion, storing, and analytics. The fog computing layer moves the edge computing activities to more powerful computing resources that are connected to the local area network and physically more distant from the sensors and data sources [28]. These added benefits create more security and privacy challenges.

5.2. Security and Privacy Policies

Cloud-based services are often considered as the essential infrastructure of the IoT that provides support for data storage, data processing, and data sharing [29]. Hackers and attackers are targeting IoT computing devices and nodes that store or communicate sensitive data. For example, patient information and electronic medical records make the healthcare system a valuable target for hackers. Each layer of the IoT model introduces security challenges and, at the same time, a possibility to enforce security and privacy standards and protocols. For example, in the device layer, the sensor's data is sent to the edge, fog, and then to the cloud, a need for authorization and certificates that trust specific servers to minimize these attacks. Firmware security and hardware address authenticating and more, however, this comes at the cost of the power consumption, as some of the wireless enabled devices such as wearables are battery run. Such security measures need to be revisited to accomplish both security

and power constraints. On the cloud layer, security measures need to ensure the network protocol between the edge and fog nodes and occasionally from sensors. Message passing protocol, point to point encryption, and certificates all provide less data spying and logging. In the data processing and end-user level, we need to ensure that the long-term data storage and real-time data processing are protected from SQL injections, sniffing, and phishing scripting attacks, providing the service certificate is updated and complies with the HIPPA standards (in health systems) [30]. Data fusion can introduce another access to the hackers to identify the user, hence privacy breach. Since the IoT devices can join and leave the network of sensors and data sources, this adds more complication to the standard methods of security measures, hence the need for new intelligent and adaptable security measures [31].

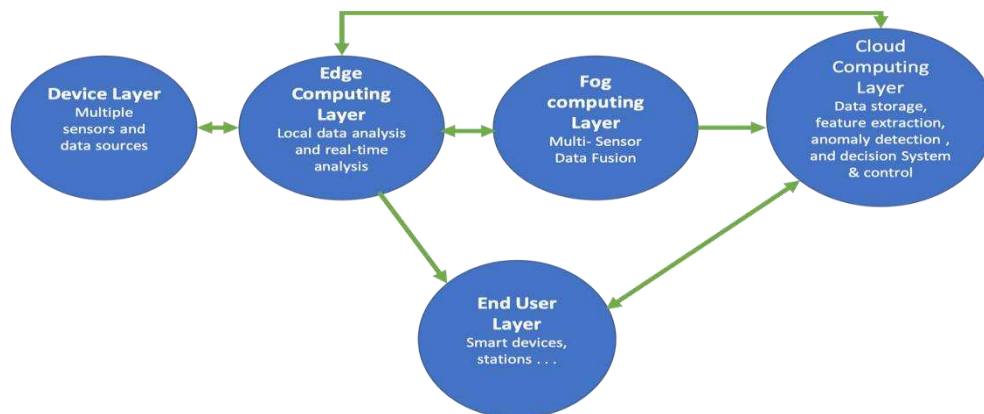


Figure 2. IoT stretched model.

5.3. Implementation of the Proposed Layered Cloud-Edge-IoT Model

Our approach is to ensure security measures set before deploying the IoT enabled devices into the secured network and ensure they can securely communicate and share data, to protect the privacy of data through encryption. Figure 3 below shows the abstraction of hardware, software, and communication model. The model consists of AWS cloud as master cloud, Raspberry Pi 4 as Edge Node, and Virtual Machines as IoT devices. The system we created with an AWS paid account to have full access to the resources provided by AWS, including certificate and encryption keys, authorization, and authentication [32].

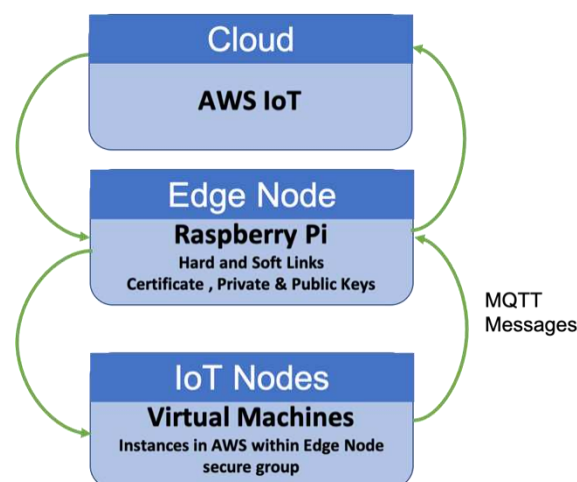


Figure 3. The proposed system model.

From the AWS available resources, we utilized the AWS Identity and Access Management (IAM) web service. It allowed us to control the user's access by initializing an IAM account (user account) for each user. For security reasons, we did not use the AWS Root account but initiated an IAM user with administrative permissions. To configure the Raspberry Pi as the Edge node (AWS Greengrass Core), the AWS Greengrass Core interacts directly with the cloud and works locally [32]. Raspberry Pi was configured by adding Linux hard and soft link protection features [33]. To make the connection between the AWS and the Raspberry. We utilized AWS Greengrass Core to create a group with a core device, and all other IoT devices to allow them to communicate with the edge.

We need certificates to authenticate all devices with the AWS. We generated certificates, private and public keys to make a secure connection with the edge and the AWS. The core certificates were generated by the AWS once we created the Greengrass group, as shown in Figure 4 below. We downloaded the generated files into the Raspberry Pi and started the Greengrass Core.

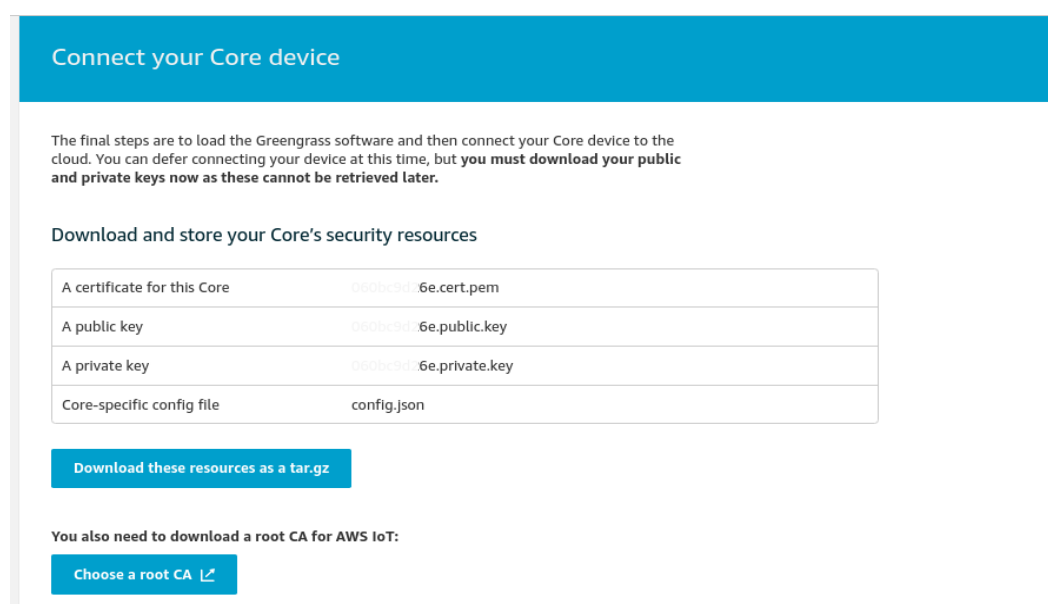


Figure 4. Certificate, private and public keys.

5.4. Discussion and Analysis

We made a simple scenario by making two IoT enabled devices to communicate with each other through our edge. The IoT devices were configured as virtual machines, created in AWS, and added to the Greengrass core, as shown in Figure 5 below. During the creation, a specific certificate, public and private keys are generated for each device to authenticate them with the AWS and with the Greengrass Core device. The communication between these two devices was done through a secure mechanism using the MQTT protocol called a message broker [34]. Finally, Figure 6 shows both IoT nodes and Edge node communicated successfully and data exchanges completed at specific times.

The following are main points to observe about our AWS working environment and our implemented model:

- In the general model, the IoT devices connect with each other or with the cloud through AWS IoT Core.
- In our model we added the edge concept by utilizing the Greengrass IoT core concept in AWS, and represent it using Pi, so we can imagine it as an added mediator between the IoT devices and the AWS IoT Core then the cloud.
- Each device needs its certificate, private key, and CA Root certificate (this is the AWS IoT certificate). There are different types of the CA Root certificate depending on the IoT device types.

- Each device needs a policy, this policy determines which operations this device can perform (connect/receive/publish/subscribe, etc.).

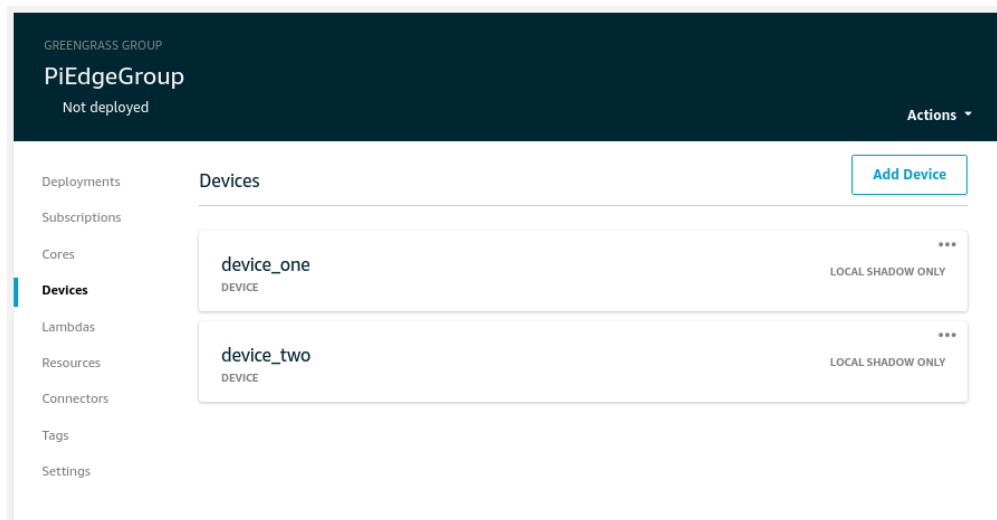


Figure 5. IoT-enabled nodes.

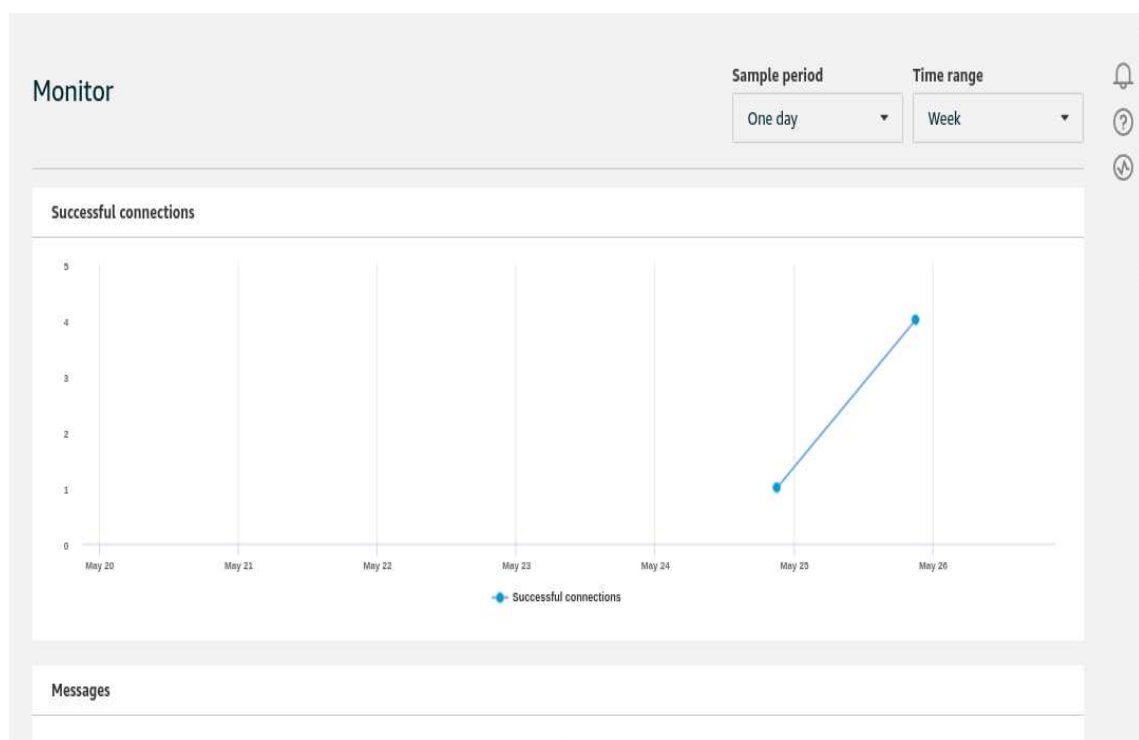


Figure 6. Successful communication and data exchange between nodes. The x-axis represents days of the month, and the y-axis the number of connections.

Therefore, we created a device, policy, and certificate. Then we attached the policy to the certificate, then attached the certificate to the device. A default policy is shown Figure 7 below:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:*",
      "Resource": "*"
    }
  ]
}
```

Figure 7. Default device policy in Amazon Web Service (AWS).

- The default policy implies the device can perform all actions (Action: iot: *) from and to all other devices (Resource: *).
- In our model, we created a modified policy to handle the added Greengrass layer.
- Additionally, action: greengrass: * means the device in the Greengrass group can perform all actions from and to other devices in the same Greengrass group (Resource: *).


The modified policy for our model is shown in Figure 8. In our scenario, the communication is done using the MQTT protocol which is a machine to machine protocol. MQTT is used because it is lightweight (small size messages and need low power), so it is suitable for a constrained environment (sensors as an example in the real applications).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Subscribe",
        "iot:Connect",
        "iot:Receive"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "greengrass:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Figure 8. Modified device policy to include the edge layer in the proposed model.

Moreover, it is important to know that the IoT devices in the AWS are emulated as MQTT clients (if it is virtual—as it is in our scenario), and the MQTT clients communicate through an MQTT Topic. The connection can be imagined as a secure channel between the clients, it is created, then clients can subscribe to it, and other clients publish messages to it.

Now, the setup process for the Raspberry Pi includes installing JAVA JDK8, the Greengrass files, in addition to a suitable Core software (depending on the used device—in our case, it is a Raspberry Pi 4). All these files were transferred to the Raspberry Pi 4 as shown in Figure 9 below.



```

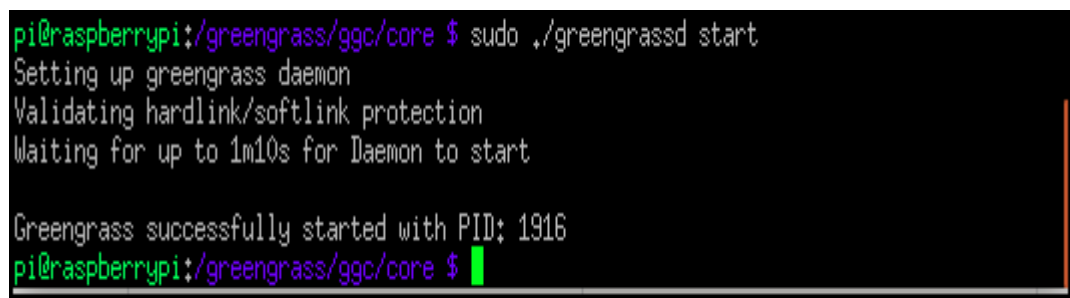
maisat@maisat-Inspiron-3537:~/Downloads$ scp greengrass-linux-armv7l-1.10.1.tar.gz pi@192.168.8.139:/home/pi
pi@192.168.8.139's password:
greengrass-linux-armv7l-1.10.1.tar.gz      100% 33MB  3.6MB/s  00:09
maisat@maisat-Inspiron-3537:~/Downloads$ scp 060bc9d26e-setup.tar.gz pi@192.168.8.139:/home/pi
pi@192.168.8.139's password:
060bc9d26e-setup.tar.gz                  100% 2842  23.2KB/s  00:00
maisat@maisat-Inspiron-3537:~/Downloads$

```

Figure 9. The Raspberry Pi 4 kit setup.

After the transfer of necessary files to the Raspberry Pi 4, we needed to extract them and make some changes on some configuration files, to match the generated certificates and keys.

Finally, we started the Greengrass core device. Figure 10 below shows that our Raspberry device successfully worked as an Edge.



```

pi@raspberrypi:/greengrass/ggc/core $ sudo ./greengrassd start
Setting up greengrass daemon
Validating hardlink/softlink protection
Waiting for up to 1m10s for Daemon to start

Greengrass successfully started with PID: 1916
pi@raspberrypi:/greengrass/ggc/core $

```

Figure 10. Running Greengrass successfully on the Raspberry Pi 4 kit.

After setting up the environment and making sure it is ready, we created an MQTT topic in our scenario and named it (my/topic). Then, we created a device to be subscribed in my/topic and created another device to be a publisher to my/topic. All devices can perform all actions with all other devices (default policy), and all messages are exchanged successfully. Figure 11 shows the different types of messages exchange in one day. The connection time is affected by many factors including the network latency and the used platform.

The proposed IoT model showed that we could ensure privacy and security measures set before we allowed the IoT enabled device or node to communicate or share its data. Upon successful implementation and configuration, we are sure that our assets are protected. The described model in this paper can be used to provide secure IoT environments and systems with fog/edge computing layers and sensors fusion. Many real-life applications can utilize this model, such as healthcare, military, disaster recovery, and many others [35]. Let us consider the healthcare case; for example, by using the proposed policy-based model, the users will have the ability to trust their healthcare provider to allow them a safeguard so that they know they are looked after. Healthcare companies invest in wearables with the belief they will help improve workforce productivity, cut absenteeism, and reduce healthcare costs. Another significant factor in wearable devices is the conviction that it can give people who are disabled. For example, a person with special needs will be able to input commands and text, say, by just moving a finger up and down. A final method, but not limited to, is the number of security users that could apply to their accounts. For example, people could restrict who can view

their social media posts or policies that explain the importance of more security to add to their account (i.e., two-factor authentication) [36].

While the IoT applications (healthcare in this case) developers try to do the best for their customers, there are still some loopholes that tend to fall through. One of the disadvantages would be the way the user's data is stored and how third parties handle it. It mostly relies on the provider itself to ensure that they set guidelines and propose a policy that will keep them in the right with the vendors and with their users. That same thing goes for the confidentiality of the customers. Most of the time, third parties (such as the insurance companies) can receive user's information if they "consent" to it, and then from there, it could be dangerous to determine whether or not it is reliable.

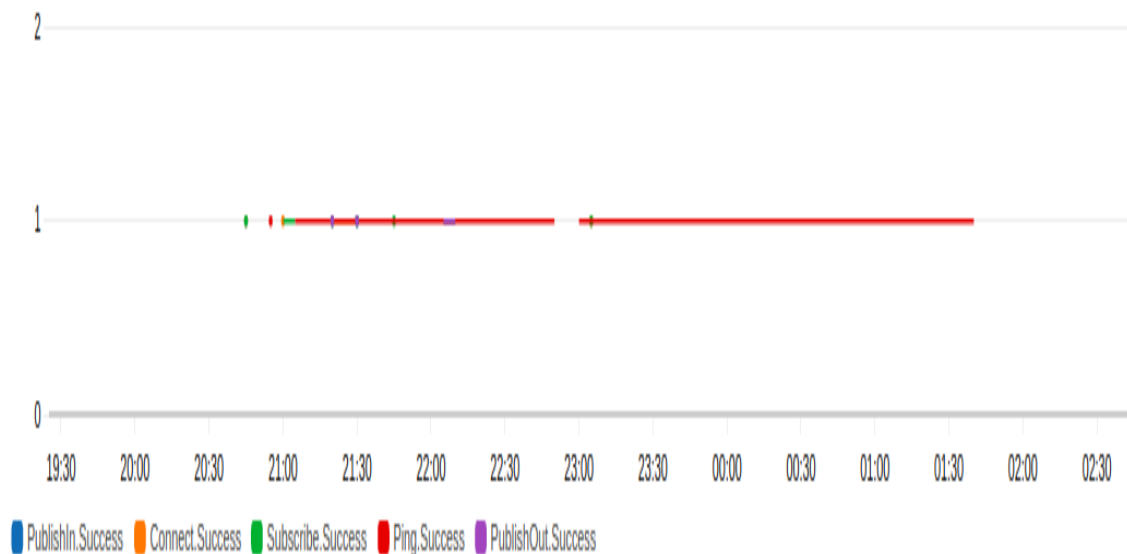


Figure 11. Successfully exchanged messages of different types: PublishOut.Success, PublishIn.Success, Connect.Success, Ping.Success, Subscribe.Success. The x-axis represents hours of the day, and the y-axis one day.

6. Conclusions

IoT devices and applications are playing an essential role in our modern life. We can see IoT devices almost everywhere from our homes, offices, shopping centers, schools, airports, and many other places to provide us with secure and on-demand services.

The IoT devices support the collaboration with the stakeholders and help in understanding the business requirements and outcomes. Additionally, IoT-based analytics and data processing can enhance the productivity and efficiency of industrial infrastructures.

Moreover, IoT systems are implementing different types of useful technological advances in various sectors. Many vendors and companies adopt a vast amount of policies to protect their connected devices from malicious attacks. With more of these devices being connected to our private networks and the Internet as well, more privacy and security concerns being reported. We read and hear that our coffee machine is spying on our talks; our smart doorbell is sending our guest photos to government agencies. Many real-life examples emphasize the severity of the security vulnerabilities associated with using IoT devices.

In this work, we proposed new IoT layered models: generic and stretched with the privacy and security components and layers identification. The proposed cloud/edge supported IoT system was implemented and evaluated. The lower layer is represented by the IoT nodes generated from the Amazon Web Service (AWS) as Virtual Machines. The middle layer (Edge) implemented as a Raspberry Pi 4 hardware kit with support of the Greengrass Edge Environment in AWS. The top layer, which is the cloud, is implemented using the Cloud-enabled IoT environment in AWS. The security protocols

and critical management sessions were between each of these layers to ensure the privacy of the users' information. We implemented security certificates to allow data transfer between the layers of the proposed Cloud/Edge enabled IoT model.

In future work, more studies should be performed on cryptographic security methods that are much more capable of operating on resource constrained IoT devices (Light Weight Crypto). It will help in ensuring that users with different experiences can steadily use and set up IoT systems despite the insufficient consumer interfaces available with many of these IoT devices. Moreover, there is an urgent need to standardize the data collection and sharing procedures done by the IoT devices connected to the Internet. Such standards will reduce the number of unpredicted vulnerabilities and associated attacks on non-homogeneous platforms.

We study the benefits and risks associated with the IoT. With all numerous benefits, risks can be exploited to harm end-users by allowing unauthorized access to sensitive private data, enabling attacks to the systems, and creating risks to personal safety. With the IoT enabled devices delivered to the market, we need to ship them with proper security measures that impact their usability, operation, and integration with existing systems. We are hoping with the help of researchers to build a dynamic security framework to mitigate, not necessarily eliminate, the security and privacy risks, and be smart enough to adapt to changes in the new communication technologies and different application deployment scenarios.

Author Contributions: Conceptualization, L.T.; methodology, F.M.; validation, M.T., formal analysis, M.Q.; investigation, F.M.; resources, L.T.; data curation, M.T.; writing—original draft preparation, L.T.; writing—review and editing, F.M.; visualization, F.M.; supervision, L.T.; project administration, L.T.; funding acquisition, L.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research funded by the Expanded Chancellor Research Initiative grant (CRI) awarded to Texas A&M University-San Antonio, TX, USA. Grant number 2019.

Acknowledgments: The authors would like to thank the Chancellor of the Texas A&M University system for supporting this research through the Chancellor Research Initiative (CRI) grant.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Khvoynitskaya, S. The History and Future of the Internet of Things. 2020. Available online: <https://www.itransition.com/blog/iot-history> (accessed on 25 March 2020).
2. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *78*, 544–546. [\[CrossRef\]](#)
3. Monther, A.A.; Tawalbeh, L. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 2088–8708.
4. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1636–1675. [\[CrossRef\]](#)
5. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. *IEEE Wirel. Commun.* **2018**, *25*, 53–59. [\[CrossRef\]](#)
6. Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30.
7. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
8. Leloglu, E. A review of security concerns in Internet of Things. *J. Comput. Commun.* **2016**, *5*, 121–136. [\[CrossRef\]](#)
9. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. *Future Internet* **2017**, *9*, 27. [\[CrossRef\]](#)
10. Ali, S.; Bosche, A.; Ford, F. *Cybersecurity Is the Key to Unlocking Demand in the Internet of Things*; Bain and Company: Boston, MA, USA, 2018.

11. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
12. Izzat, A.; Chuck, E.; Lo'ai, T. *The NICE Cyber Security Framework, Cyber Security Management*; Springer: Basel, Switzerland, 2020; ISBN 978-3-030-41987-5.
13. Tawalbeh, L.A.; Tawalbeh, H. Lightweight crypto and security. In *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*; Wiley: West Sussex, UK, 2017; pp. 243–261.
14. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [\[CrossRef\]](#)
15. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. Available online: <https://ieeexplore.ieee.org/abstract/document/7442758> (accessed on 10 April 2020). [\[CrossRef\]](#)
16. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [\[CrossRef\]](#)
17. Zaldivar, D.; Tawalbeh, L.; Muheidat, F. Investigating the Security Threats on Networked Medical Devices. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6 January 2020; pp. 0488–0493.
18. Tawalbeh, L.A.; Somani, T.F. More secure Internet of Things using robust encryption algorithms against side-channel attacks. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. [\[CrossRef\]](#)
19. Dalipi, F.; Yayilgan, S.Y. Security and privacy considerations for IoT application on smart grids: Survey and research challenges. In Proceedings of the in Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 63–68.
20. Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016; pp. 172–175.
21. Culbert, D. Personal Data Breaches and Securing IoT Devices. 2020. Available online: <https://betanews.com/2019/08/13/securing-iot-devices/> (accessed on 15 September 2019).
22. Gemalto. Securing the IoT-Building Trust in IoT Devices and Data. 2020. Available online: <https://www.gemalto.com/https://www.gemalto.com/iot/iot-security> (accessed on 17 February 2020).
23. He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the Evolutionary Computation (CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021.
24. Al Shuhaimi, F.; Jose, M.; Singh, A.V. Software-defined network as a solution to overcome security challenges in IoT. In Proceedings of the Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 491–496.
25. Estrada, D.; Tawalbeh, L.; Vinaja, R. How Secure Having IoT Devices in Our Home. *J. Inf. Secur.* **2020**, *11*. [\[CrossRef\]](#)
26. Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. 2016. Available online: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7406686> (accessed on 4 April 2020).
27. Tawalbeh, M.; Quwaider, M.; Tawalbeh, L.A. Authorization Model for IoT Healthcare Systems: Case Study. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 337–342. [\[CrossRef\]](#)
28. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Comput. Secur.* **2018**, *74*, 340–354. [\[CrossRef\]](#)
29. Singh, J.; Thomas, F.J.-M.; Pasquier, J.B.; Ko, H.; Eysers, D.M. Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet Things J.* **2016**, *3*, 269–284. [\[CrossRef\]](#)
30. The HIPAA Privacy Rule. Available online: <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (accessed on 19 October 2019).

31. Thierer, A.D. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. 2015. Available online: <http://jolt.richmond.edu/v21i2/article6.pdf> (accessed on 6 March 2020).
32. Available online: <https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html> (accessed on 17 March 2020).
33. Available online: <https://www.tecmint.com/protect-hard-and-symbolic-links-in-centos-rhel/> (accessed on 26 May 2020).
34. Available online: <https://docs.aws.amazon.com/iot/latest/developerguide/iot-message-broker.html> (accessed on 25 May 2020).
35. Sethi, P.; Sarangi, S. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, 1–25. [CrossRef]
36. Liyanage, M.; Braeken, A.; Kumar, P.; Ylianttila, M. *IoT Security: Advances in Authentication*; John Wiley & Sons: West Sussex, UK, 2020.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).