Scientific Research Publishing

Journal of Computer and Communications, 2020, 8, 11-25
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions

Mohammad Rafsun Islam[1]*, K. M. Aktheruzzaman[2]

[1]Department of Electronics and Communication Department, East West University, Dhaka, Bangladesh
[2]Department of Electrical and Electronic Engineering, Manarat International University, Dhaka, Bangladesh
Email: *rafsun@ewubd.edu, akther@manarat.ac.bd

How to cite this paper: Islam, M.R. and Aktheruzzaman, K.M. (2020) An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. *Journal of Computer and Communications*, **8**, 11-25.
https://doi.org/10.4236/jcc.2020.84002

Received: March 7, 2020
Accepted: March 29, 2020
Published: April 2, 2020

Abstract

Internet of Things (IoT) has become a prevalent topic in the world of technology. It helps billion of devices to connect to the internet so that they can exchange data with each other. Nowadays, the IoT can be applied in anything, from cellphones, coffee makers, cars, body sensors to smart surveillance, water distribution, energy management system, and environmental monitoring. However, the rapid growth of IoT has brought new and critical threats to the security and privacy of the users. Due to the millions of insecure IoT devices, an adversary can easily break into an application to make it unstable and steal sensitive user information and data. This paper provides an overview of different kinds of cybersecurity attacks against IoT devices as well as an analysis of IoT architecture. It then discusses the security solutions we can take to protect IoT devices against different kinds of security attacks. The main goal of this research is to enhance the development of IoT research by highlighting the different kinds of security challenges that IoT is facing nowadays, and the existing security solutions we can implement to make IoT devices more secure. In this study, we analyze the security solutions of IoT in three forms: secure authentication, secure communications, and application security to find suitable security solutions for protecting IoT devices.

Keywords

Internet of Things, IoT, IoT Architecture, Cybersecurity Attacks, Security Solutions

1. Introduction

The rise of the Internet of things (IoT) is one of the inventions that have a special significance in the world of communication technology. Internet of things can be described as the internetworking of computing devices that are embedded in physical objects such as electronics, sensors, software, and network connectivity that allows these objects to gather and exchange data [1]. It consists of billions of devices that utilize wireless technologies for communication. Internet of things can be integrated into everything from minuscule to big machines, body sensors to cloud computing that consists of major types of networks, for example, distributed, grid, and vehicular networks. IoT uses sensors, processors and communication hardware to receive data from the surroundings in the physical world and then performs operations on these data [2].

IoT devices are often regarded as "smart devices" that can communicate with each other. Each IoT device has its features and functions so that it can utilize on itself or in combination with other IoT or non-IoT devices. The features include Transducer capabilities, data capabilities, Interface capabilities, and supporting capabilities. Transducer capabilities are used by every IoT device which gives them the ability to interact directly with a physical object. Data capabilities provide the ability to perform digital computing functions that involve data such as data storing and data processing [3]. IoT devices can use interface capabilities to interact with each other. Supporting capabilities include functionalities such as device management, cybersecurity, and privacy capabilities which are supported by IoT [3].

Although the advantages of IoT are indisputable, the state of its security is not strong. Since the number of commercialized IoT devices is increasing exponentially, society is getting connected with more and more IoT infrastructure which makes it more vulnerable to the weaknesses of the current IoT environment. Once humans start interacting endlessly with sensors, cars, robots, and drones through the IoT, we will encounter an increasing number of security threats that can impact our lives negatively [4]. An example of IoT hacks is Mirai Botnet. Mirai Botnet was utilized by hackers to perform brute force authentication against IP cameras [5]. Since these IP cameras used extremely common usernames and passwords and telnet which are an insecure and unencrypted protocol for communication, they got easily exposed by the Mirai Botnet [5]. Hackers used the same botnet to take possession of Liberia's Infrastructure, as well as on DYN [5]. They also attacked several popular websites such as GitHub, Twitter, Reddit, and Netflix by using Mirai botnet [5]. A lot of IoT devices nowadays use poor usernames and passwords, and insecure protocols to communicate with each other. If we do not take necessary precautions against those vulnerabilities, malicious hackers will take advantage of these poorly secured IoT devices to disrupt communications or even physically harm people. They can also misuse personal information of users and compromise other connected devices by exploiting IoT devices. IoT hacks can include the hacking of medical devices that can result in fatal consequences on the patient's health [6]. Therefore, we need to implement a strong security architecture to protect us against these dangerous IoT hacks.

There are a lot of challenges in protecting the IoT devices against malicious hackers. Firstly, a multitude of heterogeneous systems, protocols, and specifications must coexist in IoT devices. Securing all of these against an adversary will become a challenge for security administrators [7]. Secondly, a security solution that is suitable for one IoT device may not be suitable for another. Therefore, we cannot use a common security solution to secure all the IoT devices. Thirdly, IoT devices are designed, supplied, and deployed by different companies. So, it is unclear who will be responsible for securing IoT devices. Fourthly, IoT devices are lightweight that have low memories and low computational powers. Since most of the security countermeasures are based on computationally expensive algorithms and high overhead protocols, it will be very hard to implement these solutions on the IoT devices [7]. Lastly, since IoT is a distributed system, it will transmit most of its data wirelessly which makes it vulnerable to wireless security attacks such as eavesdropping, denial of service, spoofing, message injection, and jamming [4].

To overcome these security challenges, we need to come with security solutions that use low overhead protocols and inexpensive computational algorithms and can provide strong encryption and authentication to IoT devices. Adaptation and self-healing must play a key role in resolving existing and future security threats in IoT, as the next generation of IoT must be capable of dealing with unpredictable changes in the environment [7].

This study presents a general survey of different kinds of cybersecurity attacks against IoT devices as well as an analysis of IoT architecture. The paper also provides security solutions that can be implemented to make IoT more secure. This paper is organized into four different sections as follows Section 2 will provide an overview of the IoT architecture, Section 3 will describe different security vulnerabilities that exist on IoT, Section 4 will discuss how we can implement security solutions to achieve the security goal of IoT. Finally, Section 5 will conclude this paper and provide us a glimpse of our future work.

2. An Overview of IoT Architecture

The architecture of the Internet of Things can be regarded as an abstraction of several hierarchical layers [4]. The three basic layers of the Internet of Things are the physical layer, Application layer, and Network layer. The devices and technologies that are used in the Internet of Things are different since they are used to provide a variety of services. Because of the heterogeneous nature of these devices and technologies, it can be difficult to manage them. A middleware layer is also sometimes added to address this challenge to manage different types of service, shielding the details of the underlying implementation [4].

The middleware layer is usually used to gather information from the network layer and store them in the cloud and database. Apart from these functionalities, the middleware layer also delivers data processing ability [1] [4].

The IoT's four-layer architecture is used in this paper and this architecture can be extended to the actual development of applications. The design of these layers is addressed in this section to inspire their particular security needs. **Fig-**

ure 1 provides an overview of the technologies that are used in the IoT's four-layer architecture.

2.1. Physical Layer

The tasks of the physical layer are to interconnect devices, perform device identification, and provide service discovery [1] [8]. The devices can be of different types such as Arduino, Raspberry, Zigbee, etc. However, to consider them as an IoT device, they require to use communication technology which permits them to connect directly or indirectly by using the internet, for example, Arduino with an ethernet connection [8]. Furthermore, each device should have a unique tag that they can use to connect to the network successfully. For this purpose, Universally Unique identifiers (UUiD) can be used [8].

Energy and computing power usually affect the technology of the physical layer. At the same time, in a hostile environment, someone can intentionally or unintentionally destroy a sensor device which will have a direct effect on the system's performance. The main challenge for this layer is the malicious attack that interferes with data collection on the sensor and identification technology [4].

2.2. Network Layer

The network layer consists of network interfaces, communication channels,

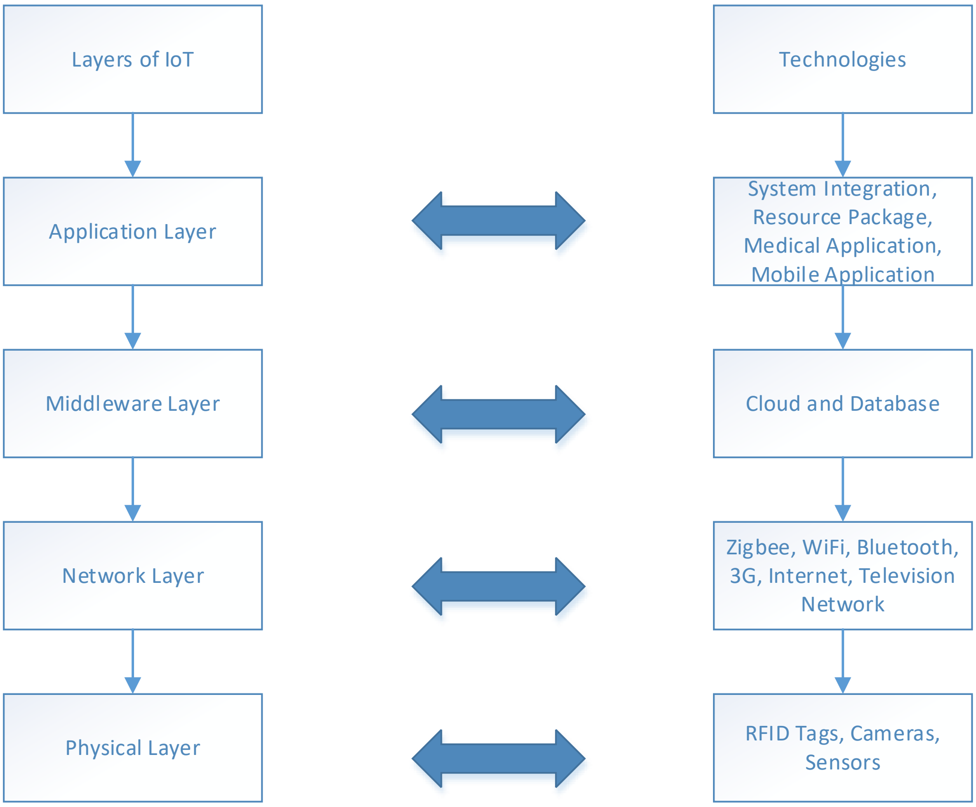
Layers of IoT
Technologies
Application Layer
System Integration, Resource Package, Medical Application, Mobile Application
Middleware Layer
Cloud and Database
Network Layer
Zigbee, WiFi, Bluetooth, 3G, Internet, Television Network
Physical Layer
RFID Tags, Cameras, Sensors

Figure 1. The architecture of IoT.

network management, information maintenance, and intelligent processing [2] [4]. Its main duty involves communication and connectivity of all the devices In the IoT system by using multiple communication protocols. The most common protocols IoT uses are the MQTT 3.1 and Constrained Application Protocol (CoAP) [8]. It is within the network layer that the information collected from the physical layer is communicated through existing communication infrastructures such as the Internet or a mobile network to any specific information processing system within the network employing Wireless Sensors or to an external network [8]. Each physical device uses wireless sensors to send its information in an IoT system. The size of these sensors is small. Since they have limited processing and computing power, their electricity consumption is low. The data received from the sensors will be processed and transmitted wirelessly to the end-user such as a human or device [2]. There are various attacks on the network layer, typically affecting work coordination and the sharing of information between devices.

2.3. Middleware Layer

The tasks of the middleware layer are to acquire data from the network layer, connect the system to the cloud and database, and operate data processing and storage [4]. The middleware layer can deliver more efficient computing and storage capabilities with the continuous development of cloud computing and IoT [1]. It also meets the requirements of the Application layer by providing APIs.

The main security attacks of this layer involve eavesdropping, injection of fraudulent packets, and non-authorized conversations. Database security and cloud security are also a concern since they can affect the quality of service in the application layer [4].

2.4. Application Layer

The application layer is responsible for ensuring the same type of service between the connected devices. Since this layer provides specific services to the end-users, it is also known as the service layer [2]. Furthermore, the application layer receives sensor/actuator data from the physical layer after the network layer converts it into a readable format. This data can then be used by the application layer to provide services or perform operations based on the data obtained.

The application layer provides storage capabilities to the collected data by storing it in a database. This layer makes it easier for these systems to connect with various types of applications outside the device-oriented network, depending on user needs, for example, Smart Home, eHealth, Smart Transportation, Smart Objects, etc. [8].

The main issue of the application layer arises when sensitive data is operated. In this layer, attackers usually target the software that is running on the IoT system. By exploiting the software, attackers can have access to sensitive data. They can also modify the data to perform malicious operations [9].

3. Cybersecurity Attacks against IoT Devices

There is much vulnerability that exists on IoT devices. Since it is simple and easy to perform cyber-attacks against IoT devices, hackers often execute them so that they can capture sensible information. Most of the IoT security threats can result in leakage of information and loss of services. These security risks can also present physical security risks which can be harmful to people.

Security vulnerabilities in IoT can open the way for many malicious hackers who want to exploit the weaknesses of IoT systems to access our personal information for their own benefits. This section will discuss the different kinds of cybersecurity attacks against IoT system. Table 1 gives different kinds of cyber security attacks against IoT Devices.

3.1. Physical Attacks against IoT Devices

Since IoT is distributed and fragmented by nature, it presents a larger attack surface and physical access to the devices. A hacker may be able to modify a node or sensor data that can put the whole sensor network on risk. Physical attacks are related to the hardware components of the IoT devices and the adversary needs to access the IoT system physically to execute his attack [9]. These attacks can harm the functionality of the IoT hardware.

Node tampering: Node tampering is a physical attack against IoT devices that can damage a sensor node. An adversary will physically replace the entire node or part of it so that he can access and modify sensitive information such as shared cryptographic keys [8].

Side channel analysis: An example of physical attack against IoT is a hacker using Side channel analysis to steal Advanced Encryption Standard (AES) secret

Table 1. Different cybersecurity attacks against IoT devices.

Classification	Security Attacks	Security Impacts
Physical Attacks	Node tempering, Side channel analysis, Radio frequency jamming	These attacks will enable hackers to modify a node or sensor data and physically harm the hardware of IoT
Network Attacks	Traffic analysis attack, Selective forwarding, Sybil attack, Sinkhole attack, Botnet attack, Hello-flood attack, Man in the middle attack	These attacks will allow hackers to have remote access and send wrong instructions to take control of IoT devices
Application Attacks	Code injection, Buffer overflow, SQL injection, Session Hijacking, Authentication and Authorization attacks	These attacks will enable hackers to steal sensitive data by providing unauthorized access to the application level of IoT
Zigbee Attacks	Eavesdropping attack, Replay attack, Packet forging attacks	These attacks will enable hackers to capture the sensitive information and Zigbee traffic
Z-Wave Attacks	Z-Wave downgrade attack, Z-Wave injection attack, Z-Wave Man in the middle attack	These attacks will allow hackers to execute security attacks against Z-Wave devices

keys used in connected street lights. Side channel analysis is a non-invasive attack involving an intruder observing power signature or Electro Magnetic radiation emitted from an integrated circuit (IC) to extract sensitive information such as secret keys [10]. Connected streetlights use AES encryption so that they can update their firmware. It also makes sure that only authorized users who know AES secret keys can securely deliver these updates. If an adversary can steal these secret keys, he will be able to hijack the streetlight network. To execute these attacks, a hacker needs to be within the proximity of the device. These types of attacks can also be used to compromise the security of bank cards, mobile devices, or medical devices.

Radio frequency jamming: An attacker can use a radio frequency jammer for blocking or jamming the wireless communication of IoT devices. It can cause IoT devices to lose network connections which will limit their abilities to communicate with the network [11].

3.2. Network Attacks against IoT Devices

These attacks are typically executed on the network level of IoT. The attackers can execute these attacks remotely and he does not have to be close to the network.

Traffic analysis attack: Traffic analysis attack is a type of network attack where an adversary can intercept and examine messages to deduce information from patterns in communication [11]. Since IoT devices have wireless characteristics, an attacker can sniff confidential information or other data from them. An attacker will try to gather network information before he tries to execute this type of attack. For that purpose, He can use sniffing applications such as port scanning applications, packet sniffers, etc.

In a traffic analysis attack, an adversary can examine the frequency and timing of IoT network packets to achieve important information. For example, an attacker can attempt to execute a timing attack on an IoT device that uses SSH for authentication. He will use the timing information to deduct passwords because SSH transmits each keystroke as a message during the interactive session.

Selective forwarding: Such attacks occur when a network node that is supposed to send the packets along the right routing path discards some of the traffic that passes through it. Various types of selective forwarding attacks exist. For one type the malicious node may drop the packets from a specific node or group of nodes selectively. It can result in a Denial of Service (Dos) attack for that specific node or group of nodes [1]. “Neglect and greed” is another type of selective forwarding attack where the subverted node skips several messages arbitrarily [1].

Sybil attack: In this attack, a malicious node which is known as Sybil node can impersonate a larger number of nodes that will enable an attacker to be in more than one place at once [12]. If a Sybil attack is executed, then it can lead to false information getting accepted by the neighboring Wireless Sensor Network (WSN) nodes. For example, in a WSN voting system, a Sybil node will be able to vote more than once which will lead to a false result [12].

Sinkhole attack: An attacker can perform a sinkhole attack against IoT devices to attract all the traffic from neighboring nodes and take control of a node inside a network [13]. This attack can lead to network congestion and an increasing amount of energy consumption by the nodes. Additionally, it can make the IoT vulnerable to denial of service attacks by dropping all the packets instead of sending them to the destination.

Botnet attack: A botnet is a collection of malware-infected internet-connected devices that enable hackers to monitor them. A botnet is used by cybercriminals to initiate botnet attacks such as data theft, unauthorized access, credential leaks, and Distributed Denial of service (DDos) attack [14].

Because of the recent developments of IoT botnets and a large number of unsecured IoT devices, hackers are turning IoT devices into a botnet army to execute botnet attacks. In botnet attack, a hacker will plant malware in IoT so that it can receive commands from command and control server to carry out malicious activities.

Hello-flood attack: Hello-flood attack can congest a network with a high number of useless unusual messages. In this attack, an attacker can cause a high number of traffic in the network by replaying a useless message that is sent by a single malicious node [15].

Man in the middle attack: Man in the middle (MITM) attacks is a type of attack where an adversary can intercept the communications between two users so that he can eavesdrop or modify the network traffics [13]. The adversary can impersonate a valid user to perform malicious activities such as stealing credentials or corrupt data.

Since a lot of IoT devices have poor security and do not implement measures against MITM attacks, they are vulnerable to it. These attacks can be executed on IoT so that an attacker can send wrong instructions to the devices and take control.

3.3. Application Attacks against IoT Devices

Application attacks enable hackers to target sensitive data of users for unauthorized access. Different types of application vulnerabilities such as buffer overflow or code injection are exploited by the adversaries so that they can gain unauthorized access to different IoT applications. Attackers can breach the application security of IoT because of any misconfiguration within the code or insecure API. Additionally, malwares such as viruses, worms, trojans, rootkits, ransomware, etc. can also target the applications running on IoT devices for unauthorized access.

Code injection: This attack exploits program errors to introduce malicious code into the system. Adversaries can use code injection attack to steal sensitive data from the users, get the full control of any system, or to spread malware [4]. Shell injection and HTML script injection are the most common types of code injection attacks. If attackers can successfully execute code injection attacks, then it can cause IoT systems to lose control and compromise the user's privacy. It can also cause a complete system shutdown of any IoT device.

Buffer overflow: In a buffer overflow attack, a program or process tries to write extra data to a fixed memory block or buffer. This attack overflows the buffer boundaries to insert malicious codes. Many programs have memory layouts or buffers to contain code and data segments. These buffers have boundaries to contain code and data. If an attacker writes a long sequence of data to a specified region that can overflow the buffer boundary, it will modify the data to execute malicious code such as encroaching into a code segment and destroy the program control flow [16]. Stack/heap-based buffer overflow, format string attack, integer error, and double free are some common types of buffer overflow attack. Buffer overflow attack is one of the most common types of application attacks against IoT devices [4]. It can help an attacker to achieve administrator privileges and execute arbitrary code to an IoT device. For example, hackers found a buffer overflow in the ZyXel NBG6716 wireless router which allowed them to take control of local networks [16].

SQL injection: SQL injection arises when an adversary submits a malicious SQL query to an unsecured field which is managed by a SQL database [9]. SQL injection is one of the most dangerous application attacks that is widespread across different kinds of systems including IoT. SQL injection can provide an attacker with privilege escalations that will grant him more access to the IoT system.

Session Hijacking: This attack can enable a hacker to reveal sensitive personal information of the users. In a Session Hijacking attack, an attacker exploits security flaws in authentication and sessions management to impersonate a real user [1].

Authentication and Authorization attacks: A lot of IoT devices have poor authentication and authorization mechanisms that allow the attackers to launch malicious attacks to remotely control a device and gain administrative privileges [15]. A common issue of the faulty authentication and authorization mechanisms is that it allows users to provide poor passwords to authenticate into a system. An attacker can easily get these passwords by using a brute force attack. In addition, if unauthorized administrative permission is given to a file and directory, an attacker can exploit this vulnerability to create attacks in different degrees and gain administrative privilege. For example, poor authentication and authorization mechanism of the smart home building can enable an attacker to perform unauthorized operations such as opening the door.

3.4. Zigbee Attacks against IoT Devices

Zigbee is a low-power, low-cost, wireless network standard that is widely used in the Internet of Things [10]. It can be found in a wide range of IoT technologies, from home security router to hospital patient monitoring systems. Because of

Zigbee's low power, low cost, and simple technology, it is often viewed as a logical choice to support IoT [13]. However, it is susceptible to different types of security attacks.

Eavesdropping attack: Since a lot of Zigbee networks do not use encryption, attackers can execute an eavesdropping attack against it. Even if Zigbee uses encryption, attackers can take advantage of unencrypted Zigbee frame information such as the Mac addresses, node addresses, and PAN ID to identify the presence of a Zigbee network [13]. Attackers can use a tool named zbdump from the KillerBee framework to perform an eavesdropping attack [14]. By using the eavesdropping attack, an adversary will be able to capture the sensitive user information such as username and password.

Replay attack: In a replay attack, a hacker will use observe data to retransmit the frames as if they were transmitted by an original user again [13]. The impact of a replay attack mainly depends on the content of the replayed data and the nature of the protocol being used. For example, an adversary can capture the traffic which is generated by a smart bulb. He can replay these packets in order to manipulate the on or off event of the smart bulb. Many ZigBee stacks that do not encrypt traffic are vulnerable to replay attacks. A hacker can use the KillerBee zbreplay tool to perform replay attacks against IoT devices that use the Zigbee network [14].

Packet forging attacks: Packet forging attacks happen when hackers try to inject their packets in the data stream to disrupt or intercept packets in a Zigbee network [13]. These forge packets can appear as normal packets. Therefore, it will be very hard to detect malicious activities that are caused by packet forging attacks.

3.5. Z-Wave Attacks against IoT Devices

Z-Wave is a popular wireless home automation protocol that is widely used by IoT devices. Millions of IoT devices such as door locks, lighting, heating systems, and home alarms embeds Z-Wave wireless chipsets. It enables smart IoT devices to connect and share control commands and data with each other [14]. Z-Wave is vulnerable to several security attacks.

Z-wave downgrade attack: Z-wave supports a strong S2 Z-wave security pairing security process. Nevertheless, a hacker can downgrade the higher S2 standard to a lower S0 security standard. As a result, it enables an attacker to steal an encryption key which can expose a device to security attacks [14].

The Z-Wave downgrade attack can trick two paired smart devices into thinking that one of them is not supporting the higher S2 standard security. Therefore, it can force both to use the older S0 security standard. All older S0 security uses a default encryption key of "0000000000000000." which can be easily sniffed by an attacker to exploit IoT devices [14].

Z-Wave injection attack: Many Z-wave devices lack basic encryption or integrity protection support. This can allow an adversary to inject arbitrary packet content or replay captured traffics so that he can manipulate Z-Wave nodes [14].

Z-Wave Man in the middle attack: In a Z-Wave Man in the middle attack, a hacker can intercept Z-Wave connections. Many Z-Wave devices do not authenticate the identity of the controller. Therefore, an adversary can intercept the inclusion process with a target device by using any Z-Wave controller which supports the CLASS_SECURITY command class [14]. It can force the victim to associate to a malicious network.

4. IoT Security Solutions

The primary goal of security mitigation is to ensure privacy, confidentiality, the protection of IoT users, infrastructures, data and devices and the availability of the services provided by an IoT infrastructure. To strengthen the security of IoT devices, we need to authenticate every communicating device on a network, maintain the confidentiality and integrity of connections between devices, encrypt the data, and store the data in a secure location. This section will discuss the security solution we can employ to protect IoT devices against security attacks. Table 2 provides different types of security solutions for securing IoT devices.

4.1. Authentication

Authentication is the method of identifying and verifying IoT users and devices so that it can provide access to authorized users and devices in the network. Since IoT consists of a vast number of interconnected and distributed devices that communicate with each other, authentication plays an important role in IoT security. It is necessary to control and properly authenticate each IoT device to make sure it is genuine and prevent unauthorized devices from accessing the network. Strong authentication can help us to mitigate several IoT security attacks such as eavesdropping attacks, replay attacks, man in the middle attacks, dictionary attacks, and brute force attacks [15].

The most common way to authenticate IoT devices is by exchanging a shared secret key between them. Therefore, symmetric algorithms such as Triple Data Encryption Algorithm (3DES or TDES) and Advanced Encryption Standard (AES) are widely used for authentication [17]. However, if an adversary can obtain the secret key, then he will be able to compromise the whole IoT system.

Table 2. Security solutions for securing IoT devices.

Classification	Security Solutions
Authentication	Symmetric algorithm, Asymmetric or Public key cryptography, Transport Layer Security (TLS), Digital Signature
Secure Communication Solutions	Virtual Private Network (VPN), Cryptographic hash functions, Private Pre Shared Key (PPSK), Firewall and IDS/IPS, End to end message secrecy
Application Security	Secure coding, Secure boot, Access Control list (ACL), Firewall and IDS, Secure software updates

Additionally, if the number of communicating devices increases, then the risk of exposing the secret key becomes significantly greater.

A better way to authenticate IoT devices is to use asymmetric or public-key cryptography. Public key cryptography can provide strong authentication for IoT [17]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is another asymmetric algorithm that can be utilized for authentication. Public key cryptography will need access to public key infrastructure (PKI). Therefore, a secure implementation of PKI Is also needed for IoT security. Secure implementation of PKI for authentication involves on-chip key pair generation which uses true random number generator to generate the key, and execution of cryptographic operations such as encryption, decryption, signing, and signature verification within a controlled environment [17]. Another method we can use for authentication is Transport layer Security (TLS). TLS can offer Transport Layer Security pre-shared key ciphersuites (TLS-PSK) that uses pre-shared keys, and TLS-DHE-RSA authentication method that uses Rivestshamir Adelman (RSA) and Diffie-Hellman (DHE) key exchange to perform authentication [15].

A digital signature can also be used to authenticate IoT devices. A digital signature that uses asymmetric cryptography can provide authenticity and integrity for IoT [17]. The authenticity and integrity can be achieved by creating a one-way hash of the secret key and encrypting the hash with the sender's private key. The recipient uses the sender's public key in order to decrypt the hash and verify the authentication and integrity of the data. Multi-factor authentication that uses bio-hashing and anonymity are other methods we can employ in order to achieve the IoT authentication's goal [15]. **Figure 2** provides a representation of the Authentication mechanisms for IoT security solutions.

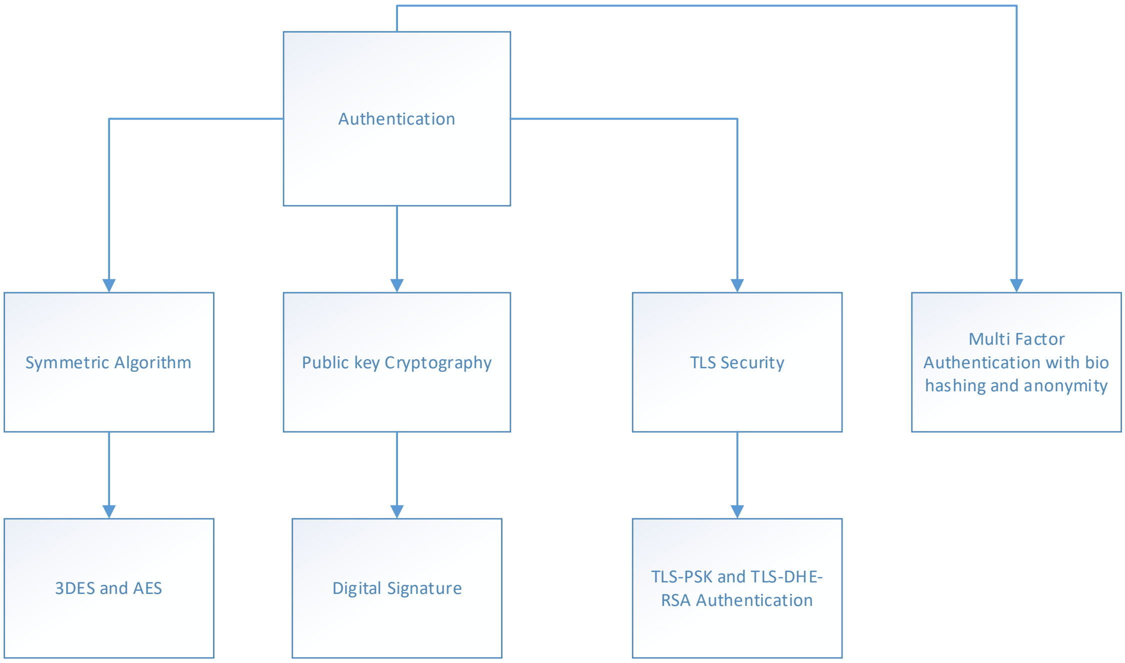

Figure 2. IoT Security solutions: authentication.

4.2. Secure Communication Solutions

IoT devices can use existing internet technologies and protocols which can supply them secure communication solutions for protecting user data. For example, IoT devices can use virtual private network (VPN) which is based on protocols like Secure Socket Layer/Transport Layer Security (SSL/TLS), Media Access Control security (MACsec), or Datagram Transport Layer Security (DTLS) to encrypt the connection which will provide better security for IoT users [17]. Cryptographic hash functions can also be used for confirming the integrity of the data. Error checking mechanisms can be introduced to mitigate the problem of tampered data [1].

Another method of securing communications between IoT devices is to use Private Pre Shared Key (PPSK) [1]. The access domain for each type of device can be easily defined by providing different unique keys. Strong password policies and periodic change of passwords should be utilized to protect communication. Moreover, technologies like firewall and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) should be employed to prevent intruders from accessing the network.

It is also important to have data confidentiality since IoT messages can be easily intercepted by an adversary by using Man in the middle tools. End to end message secrecy can be employed to achieve data confidentiality. Also, the data stored on IoT devices such as message and personal data should be protected from unauthorized entities.

4.3. Application Security

IoT applications should be secured by using various techniques. IoT devices should execute the application code securely so that it cannot be modified or corrupted and should not reveal sensitive data. Secure coding is especially important when using sensitive data like cryptographic keys or functions, payment applications, and health information [17].

IoT application can also utilize a secure boot to protect data in use and ensure that devices will only run the software authorized by its manufacturer or deploying organization. Secure boot can also guarantee that only those kernels or software which are approved by the manufacturer or trusted third party are permitted to boot on the devices [17]. Kernel and software images should be authenticated by hashes and digital signature for checking data integrity before executing them during boot time.

Access control list (ACL) should be implemented to set up policies and permissions that will decide who can access and control the IoT application [4]. This will also ensure the privacy of the data. ACL has the capability of allowing and blocking incoming and outgoing connections as well as ensuring that only authorized users can access the network.

Firewall and intrusion detection systems can also be employed to secure IoT applications. Firewall has rulesets to allow authorized connections and block malicious connections. Intrusion detection system can analyze traffic patterns to detect malicious actions so that It can report an alarm when an attack is detected [1].

Softwares that are running on IoT devices need to be regularly updated and monitored for fixing bugs and introducing new features. Secure software updates employ both digital signature verification and data integrity check to ensure that source and device code have not been altered by an adversary [17]. Digital signature verification can be achieved by signing software at the source by a trusted third party and verifying it by using a public key. Data integrity check can be achieved by using a hashing function [17].

5. Conclusion

IoT is an emerging technology that connects billions of physical devices to the internet by using existing technologies. The Internet of Things is making our lives revolutionized. Despite its rapid development, it is introducing new security threats which are enabling hackers to execute different kinds of security attacks against it. The main aim of this paper is to advance the IoT research by addressing the various types of security attacks that can be executed against IoT as well as providing solutions to make IoT environment more secure. This research would help researchers to understand the impact of security threats on IoT as well as the recent security solutions that can be implemented in IoT devices for better security. We discussed different kinds of cybersecurity attacks against IoT such as physical attacks, network attacks, application attacks, Zigbee attacks, and Z-Wave attacks on this paper. We also explored different security solutions such as authentication, secure communication solutions, and application security to protect IoT against security threats. Since IoT devices have low power and low memory, we need to implement lightweight security solutions. By reviewing the existing security solutions, we can decide which security solutions are lightweight and suitable for IoT. We believe digital signatures that use lightweight operations for signature and verification process can deliver stronger security to IoT devices. As future work, we aim to investigate the use of different kinds of lightweight protocols and cryptographic algorithms that use strong encryption and authentication to provide better security for IoT devices.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Leloglu, E. (2017) A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications*, **5**, 121-136. https://doi.org/10.4236/jcc.2017.51010

[2] Dean, A. and Agyeman, M.O. (2018) A Study of the Advances in IoT Security. *The 2nd International Symposium on Computer Science and Intelligent Control*, Vol. 15, 1-5. https://doi.org/10.1145/3284557.3284560

[3] Sethi, P. and Sarangi, S.R. (2017) Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, **2017**, Article ID: 9324035. https://doi.org/10.1155/2017/9324035

[4] Chen, K.J., Zhang, S., Li, Z.K., Zhang, Y., Deng, Q.X., Ray, S. and Jin, Y. (2018) Internet of Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*, **2**, 97-100. https://doi.org/10.1007/s41635-017-0029-7

[5] Gupta, A. (2019) The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things. Apress, Walnut. https://doi.org/10.1007/978-1-4842-4300-8

[6] Razzaq, M.A., Gill, S.H., Qureshi, M.A. and Ullah, S. (2017) Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*, **8**, 383-388. https://doi.org/10.14569/IJACSA.2017.080650

[7] Restuccia, F., D'Oro, S. and Melodla, T. (2018) Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. *IEEE Internet of Things*, **1**, 1. https://doi.org/10.1109/JIOT.2018.2846040

[8] Andrea, I., Chrysostomou, C. and Hadjichristofi, G. (2015) Internet of Things: Security Vulnerabilities and Challenges. *IEEE Symposium on Computers and Communication*, Larnaca, 6-9 July 2015, 180-187. https://doi.org/10.1109/ISCC.2015.7405513

[9] Rizvi, S., Pfeffer III, J., Kurtz, A. and Rizvi, M. (2018) Securing the Internet of Things (IoT): A Security Taxonomy for IoT. 17*th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, New York, 1-3 August 2018, 163-168. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034

[10] Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, A. (2019) IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*, **6**, 8182-8201. https://doi.org/10.1109/JIOT.2019.2935189

[11] Butun, I., Osterberg, P. and Song, H. (2019) Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. *IEEE Communications Surveys & Tutorials*, 1. https://doi.org/10.1109/COMST.2019.2953364

[12] Husamuddin, M. and Qayyum, M. (2017) Internet of Things: A Study on Security and Privacy Threats. 2*nd International Conference on Anti-Cyber Crimes*, Abha, 26-27 March 2017, 93-97. https://doi.org/10.1109/Anti-Cybercrime.2017.7905270

[13] Abdul-Ghani, H.A., Konstantas, D. and Mahyoub, M. (2017) Comprehensive IoT Attacks Survey Based on a Building-Blocked Reference Model. *International Journal of Advanced Computer Science and Applications*, **9**, 355-373. https://doi.org/10.14569/IJACSA.2018.090349

[14] Wright, J. and Cache, J. (2015) Hacking Exposed Wireless: Wireless Security Secrets and Solutions. Third Edition, McGraw Hill Education, New York.

[15] Noor Mohamad, M.B. and Hassan, W.H. (2019) Current Research on Internet of Things (IoT) Security: A Survey. *Computer Networks*, **148**, 283-294. https://doi.org/10.1016/j.comnet.2018.11.025

[16] Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K. and Fu, X. (2017) Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal*, **4**, 1899-1909. https://doi.org/10.1109/JIOT.2017.2707465

[17] Miller, L. (2016) IoT Security for Dummies. John Wiley & Sons, Chester.