Computer & Robotics

Taxonomy of Threats and Attacks in IoT

Maryam Shamsadini [a], Ali Ghaffari [b,*]

[a] *Department of Computer Engineering, International Aras Branch, Islamic Azad University ,Aras, Iran*
[b] *Department of Computer Engineering, Tabriz Branch, Islamic Azad University ,Tabriz, Iran*

Received 19 May 2022; Accepted 01 June 2022

Abstract

The Internet of everything that is often known as The Internet of Things (IoT), is the next generation internet network that is created by intelligent objects with software and sensors, where machines can communicate with various machines and humans. The IoT industry does not have one clear set of security standards for developers and manufactures to build in consistent security. The data collected and stored with these devices such as name, age, health data, location and more can aid cyber-attack activity. The first step to face these threats is to classify it and determine the risk of attacks and threats according to different classes of layers. The present study discusses about various IoT attacks happening, classify them, its countermeasures and finding the most prominent attacks in IoT in different layers.

Keywords: IoT, IoT Attacks, IoT Security, Vulnerability of IoT, IoT Threats

1. Introduction

Today, the IoT is seen as a new-generation network that has advanced enough to establish the connection between the real world and the virtual world. Figure 1 visualizes the use of many IoT applications for the use of people, vehicles, houses, cities, trade and industry. As is seen, computers, smartphones, smart sockets, school services, smart grids, smart health, smart office and wearable materials are some of the IoT applications. The common feature of IoT applications is that the data collected from intelligent objects with embedded sensors are gathered and used over the network. IoT applications are increasing day by day, expanding the usage areas and making human life easier. In fact, a huge amount of personalized data collected by convenient IoT applications covering smart cities, smart environments, smart metering, security and emergency, retail sales, logistics, smart farming, smart livestock and smart health are being shared and analysed [1].

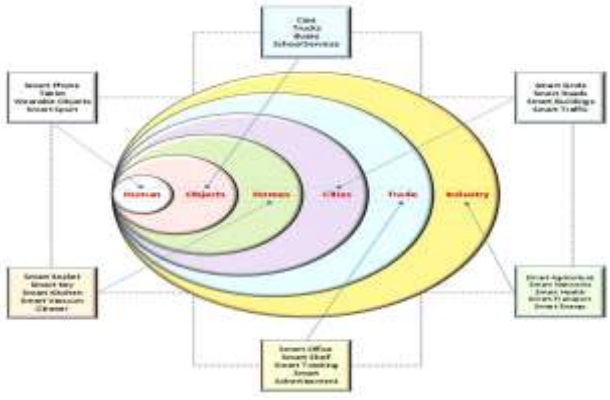

Fig 1. IoT Applications

2.IoT Architecture and Protocols

Since IoT technology is designed to apply in many sectors that are crucial, especially for national security and economy with different industry standards and specifications security issues require primary attention to minimize the attack surface and

* Corresponding Author. Email: ghaffari943@yahoo.com

prevent security issues. The architecture shown in Figure 2 is a general reference model that can be applied to different IoT application platforms including all components involved in the process of data collection, sharing and processing [3]. Based on the 7-layer protocol, we will discuss in the following issues and concerns that address the security threats of each layer.

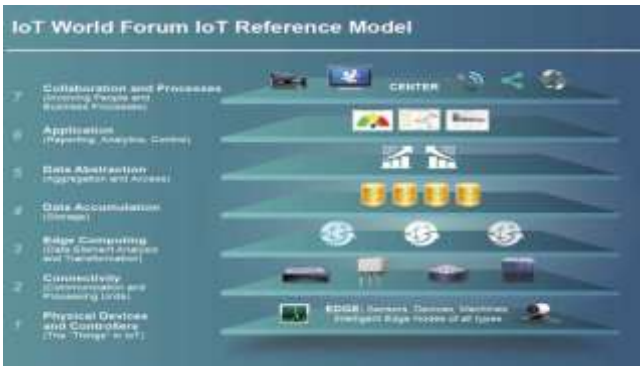

Fig 2. IoT Reference Model

3.IoT Security

TLS (Transport Layer Security) and its predecessor Secure Socket Layer (SSL) protocols are used to securely communicate by encrypting IoT data transmitted over problematic computer networks having no resource and energy shortages [4]. Meanwhile, in protocols that provide security on the transport layer, authentication is handled via symmetric key distributed by asymmetric encryption with X.509 certificates.

DTLS (Datagram Transport Layer Security) protocol has been developed to provide three main principles of security, such as UDP-based integrity, authentication and privacy, to enable the TLS protocol to work more efficiently in slow and problematic networks such as IoT [1]. The location of the DTLS protocol in the IoT architecture is shown in Figure 3. [1]

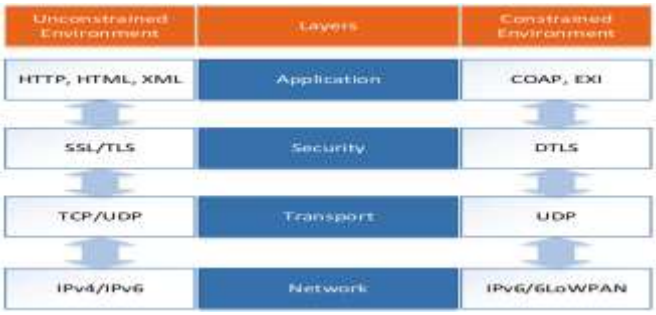

Fig 3. Position of DTLS in Protocol Stack.

As shown in Figure 3, the DTLS protocol running between the application and the network layer is an important protocol that provides end-to-end transfer security. It should be noted that, in the absence of end-to-end protection, it will be possible to gain unauthorized access and misuse of data through an object seized by the attacker. The ability of the DTLS protocol to operate in limited environments also prevents the performance application platforms including all components involved in the process of data collection, sharing and processing. DTLS consists of two layers: registration protocol and handshake. The data are shared with the client and server using the handshake protocol, while the data are encrypted with symmetric encryption keys with the registration protocol. The process of mutual authentication between the parties that will communicate with each other is handled via the exchange of the encryption algorithm and keys. The registration protocol protects application data using keys created during handshake. DTLS partitions, compresses and encrypts each outgoing message in order to generate the message verification code. Similarly, for the incoming messages, it combines, decompresses and decrypts in order to verify the message. Another important security element in ensuring IoT security is the access control. Access control mechanisms should be used to manage permissions on the use of network resources of data owners and data sharing agents on a large IoT network [6].

4.Challenges Associated with IoT Security

Most IoT devices are not designed with security in mind, and many do not have traditional operating systems or even enough memory or processing power to incorporate security features. Not only that, but IoT devices are growing in number, with over a million new devices connecting to the internet each day. The result is a significant quantity of data moving freely between devices and across network environments, remote offices, mobile workers, and public clouds with minimal visibility, making it difficult to track and secure this data.

4.1.What Are the Risks, Threats and vulnerable of IoT?

IoT devices are vulnerable to hijacking and weaponization for use in distributed denial of service (DDoS) attacks, as well as targeted code injection, and spoofing. Malware is also more easily hidden in the large volume of IoT data, and IoT devices

sometimes even come with malware already onboard. Further, some IoT devices can be remotely controlled or have their functionality disabled by bad actors. In fact, swarms of compromised IoT devices can act as swarms which could really change the game in terms of protecting against these types of attacks in table1.

Table1
IoT threats and Vulnerable

Threats and Vulnerable	Description
Convergence of IT, OT, and IoT	IoT, especially when paired with edge computing, enables the IT portion of IT/OT convergence. OT devices aren't traditionally networked technology. IoT devices, by definition, are networked computing devices with the ability to collect, transfer and analyse data.
Lack of physical hardening	Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device
Insecure data storage and transfer	Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
Lack of visibility and device management	When IT and security teams lack visibility into any part of their attack surface, they lose the ability to meet security and operational objectives, putting the business at risk. In some cases, organizations were reporting 3.3 times more incidents caused by lack of visibility into IT assets.
Botnets	A botnet is a number of Internet-connected devices, each of which runs one or more bots. Botnets can be used to perform Distributed Denial-of-Service attacks, steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control software.
Weak passcodes	Although intricate passcodes can prove to be secure for most IoT devices, one weak passcode is all it takes to open the gateway to the organization's network. Inconsistent management of passcodes throughout the workplace enables hackers to compromise the entire business network.
Insecure ecosystem interfaces	Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
AI-based attacks	AI-based attacks identify and imitate authentic user behaviour to hide threats from conventional security controls. Actions suggested: Security experts need to plan for a futuristic AI software system that can evaluate all potential threat vectors, choose the right strategy, implement effectively, and locate malware.
Ransomware	Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

4.2.Managing IoT Security Threats

Robust IoT security requires integrated solutions that are capable of providing visibility, segmentation, and seamless protection across the entire network infrastructure. Key features of such a solution include the following:

- **Complete network visibility**, which makes it possible to authenticate and classify IoT devices, as well as build and assign risk profiles to IoT device groups.
- **Segmentation of IoT devices** into policy-driven groups based on their risk profiles.
- **Monitoring, inspection, and policy enforcement based** on activity at different points within the infrastructure.
- **The ability to take automatic and immediate action** if any network devices become compromised.

5.Zero Trust is Key

Additionally, as digital innovation expands networks and there is an increased reliance on remote access, a zero trust approach is necessary to protect distributed environments, including securing IoT. With Zero Trust Access (ZTA), role based access control is a crucial component of network access management with a least access policy that gives users the minimum level of network access required for their role while removing their ability to access or see other parts of the network. ZTA also can authenticate endpoint and IoT devices to establish and maintain comprehensive management control and ensure visibility of every component attached to the network. For headless IoT devices, network access control (NAC) solutions can be relied on for discovery and access control. Using NAC policies, organizations can apply the zero-trust principles of least access to IoT devices, granting only sufficient network access to perform their role [15].

Table 2
Comparison of existing mechanisms a long description with respect to security for IoT.

Method's Name with Layer	Description	Issues Which It Address
Hashed Based Encryption in Perception layer [47]	Hash Functions are used along encryption algorithms.	It is used to check the integrity of the message.
PKI protocol in Perception Layer [49]	Base station sends message to destination and has the public key.	It does not compromise about security so, deliver message by itself.
Secure Authorization Mechanism in Perception Layer	Client - Server based System. It consists of two mechanisms; RBAC and ABAC.	Client send a request to server in order to fetch required resources. As a result, client get resources from server in a secure way.
Lightweight Cryptographic Algorithms in Perception Layer [52]	Keys are used to convert messages.	It is used to convert a message from plain text to cipher by using symmetric, asymmetric key and hash functions
Embedded Security Framework [53] in Perception Layer	It provides not only security but also secure OS, memory and run time environment.	It provides secure secondary storage, run time environment and secure memory management in order to provide security to users.
Identity Management Framework in Network Layer [54]	It has two fragments of it; identity and service and Communicate via them.	It confirms from identity module which has information of users in order to prevent the attacker.
Risk based Adaptive Framework in Network Layer [55]	Four portions an each portion do their tasks and send the responsibility to other.	It stores the information about attack so when attacks come again, remove the attacks at second portion.
SDN with IoT in Network Layer [56]	SDN is used for better performance in low cost and use less hardware resource.	All communication is occurred by SDN which provides security to both; the IoT agent and controller.
Cooperation of Nodes based Common Protocol in Network Layer [57]	Node sends information to a trust manager to prevent the network from the intruders	It works on ad hoc communication environment. It detects and prevents the intruders.
Reputation System based Mechanism in Network Layer [58]	Node maintains two data structures; the reputation table and watchdog mechanism to detect intruders.	It works on ad hoc communication environment. It prevents the intruder the reputation system.
Cluster based Intrusion Detection and Prevention System [59] in Network Layer	Detects intruder by computing trust level. Trust level depends on packet generating, sending and receiving ratio.	It detects and prevents the intruder by dividing the network into cluster.
Preference Based Privacy Protection [60] in Application Layer	Communication occurs by service provider, client and third party in secure environment.	A third party organization acts like a bridge between service provider and client. It also checks security provided by the service provider to client.

The attack is always intentional and malicious to cause damage, unlike the threat that can be intentional or unintentional. There are several security attacks in the IoT framework that can be analyzed with respect to the proposed IoT reference model.

6. Security Concern Due to Threats and Attacks at Different Layers

In this paper we will briefly describe some of the threats and attacks at different layers of the 7 layers' model architecture. And we describe each attack in the 7 layer when it occurs.

6.1. Security Concern at Perception Layer

Perception Layer is a physical layer, often called the sensor layer. It works like a human sensor e.g., eyes for watching, ears for listening, nose for sniffing etc. Actuators, Edge devices, and Sensors are used in this layer responsible for interacting with the environment, identifying objects in the environment, collecting data, processing that data into useful information, and passing it to the network layer. Since current sensor management systems and protection schemes are insufficient to protect the sensors, an attacker may use them in various ways. In general, sensor-based threats refer to passive and active malicious actions that are attempted by the manipulation of sensors for their malicious purposes. Different kinds of threats and attacks which cause serious security challenges at the perception layer are eavesdropping, battery drainages, hardware failure, malicious data injection, Sybil threat, disclosure of critical information, device compromise, node cloning, node capture, side-channel attack (SCA), tag cloning, Radio Frequency (RF) jamming, node injection, exhaustion, node outage, etc. Some of these security threats and attacks are briefly discussed below in table 4.

Table 3
Attacks at Perception layer

Attack	Description
Replay [14]	A replay attack is a more specific type of man-in-the-middle-attack, so they share some similarities. In a replay attack, a hacker intercepts your data and resends the same web request to a server, so it looks like that data is coming from your browser. When the server sends back a response, the hacker will receive it.
Micro probing [68]	This attack is applied by attaching tiny needles to the internal wiring of a chip.
Sybil and spoofing [69]	A Sybil node with a fake identity pretending to be an authorized object of the system consumes network resources, resulting in access denied to other objects.
Insecure interface [70]	Insecure implementation of the communication interface could lead to attackers access the system
Sleep deprivation [71]	This attack is made by making the devices always awake, resulting in too much energy consumption and ultimately no battery left when necessary to perform some operation
Buffer reservation [72]	The receiver contains the store for incoming packet processing, and an attacker sends the incomplete packet, which results in a denial-of-service attack.
Denial of Service [14,15]	The purpose of this attack is to overload the device with redundant packets, which make the device unusable
Eavesdropping [73]	An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices.
Man in The Middle [74]	MITM. A malicious device secretly establishes a connection between two devices and making them think they are exchanging data with each other;
Malicious Data Injection [75]	Malicious data injection attacks, which alter the values of measurements without being detected, are one potential cause of bad data and may have serious consequences. Thus, unexpected measurement values after a probe provide an indication of both bad and malicious data.
Node capture attack [76]	The attacker gains access to the key node and can extract sensitive information
Fake node or malicious node [77]	The attacker adds a node into the IoT system and tries to stop the network.
Timing attack [78]	This attack is possible when the device has low computational resources. The attacker observes the response time of the device and extracts weaknesses.
Side-Channel Attacks [79]	Side channel attacks (SCA) exploit the information leakages in the system. The leakages can be related to timing, power, electromagnetic signals, sound, light, etc.
Node cloning [80]	In a clone-node attack, the attacker can capture the physical device(s) from the IoT network by extracting their secret credential, including ID, public and private keys.
Exhaustion attack [100]	Exhaustion attacks are computer security exploits that crash, hang, or otherwise interfere with the targeted program or system. They are a form of denial-of-service attack but are different from distributed denial-of-service attacks, which involve overwhelming a network host such as a web server with requests from many locations

6.2. Security Concern at Abstraction Layer

An abstraction layer is a generalization of a conceptual model or algorithm, away from any specific implementation. These generalizations arise from broad similarities that are best encapsulated by models that express similarities present in various specific implementations. The simplification provided by a good abstraction layer allows for easy reuse by distilling a useful concept or design pattern so that situations, where it may be accurately applied, can be quickly recognized. A layer is considered to be on top of another if it depends on it. Every layer can exist without the layers above it, and requires the layers below it to function. Frequently abstraction layers can be composed into a hierarchy of abstraction levels. The OSI model comprises seven abstraction layers. Each layer of the model encapsulates and addresses a different part of the needs of digital communications, thereby reducing the complexity of the associated engineering solutions. Today's threat landscape is more dynamic than ever and represents a robust playground for financial, activist, and nationalized hackers. This is primarily driven by compute and access that is more distributed than ever. Distributed data centers, cloud instances, SaaS applications, mobile devices, remote users and even the Internet of Things (IoT) all contribute to making this a new era for information technology. This, coupled with sophisticated analytics in real time streaming data based on behavior analysis, can determine the exact nature of attacks down to even Advanced Persistent Threats (APTs), which may take months before corporate information can finally be extracted, most likely

through staging servers and taking the company's crown jewel out to an undisclosed location. Even though compute and access are at an unparalleled level of agility, many continue to incorporate traditional models to secure their assets. These traditional models consist of:

- *Fence & Gate Security* – where one or more egress points are implemented within a containment network.

- *On-Device Security* – where basic security

- functions are implemented per device.

The challenge with these options is that Fence & Gate is too static to protect distributed assets. Imagine the products, manpower and time required to implement visibility, control, and threat and data leak management for each of your data centers, cloud instances and SaaS applications via the fence & gate model. Mobile devices and remote users require on-device data-in-motion security to augment the remote control capabilities of Mobile Device Management (MDM). Mobile devices just don't have the resources to support comprehensive security on board, and even if they did, administration and logistics would be a nightmare. Implementing the above is just not viable for myriad budget, burden and sustainability reasons. The Global Security Abstraction Layer (GSAL) model is a strong candidate to address the distributed asset challenge the industry faces. With the Ubiquitous Security Abstraction Layer, disparate assets tap into a regional GSAL point-of-presence, rather than building one-off security infrastructure per application delivery point. The Security Abstraction Layer delivers visibility, control, threat and content management on a one-to-one basis between individual distributed assets and all other private or public points. This can be coupled with very sophisticated real time streaming analytics, most likely on flash matrix, and with embedded analytics can ultimately provide real time solutions to deliver world class security services across the enterprise. The benefit is that distributed data centers, cloud instances, SaaS applications, mobile assets and especially underpowered Internet-of-Things devices can benefit from consistent, robust and centrally managed security without the need for one-off infrastructure build-outs or on-device security. Moreover, the Ubiquitous Security Abstraction Layer offers single-pane visibility for all assets. This includes challenging data flow models such as visibility and security for mobile devices communicating directly with cloud instances. When considering the overwhelming trajectory of the IoT to the forecasted 50 billion over the next 6 years, especially the diversity of operating platforms and varying processing power, GSAL represents the only model that can effectively and sustainably protect such distributed assets. Moreover, it can do this by building a one-to-one relationship between the asset and the security policy. When considering the Target and Home Depot compromises for example, had they used GSAL to secure their registers along with sophisticated analytics, we are convinced they would have been protected well beyond their expectations since none of the 1200+ security products are designed to solve this problem with an abstraction layer coupled with sophisticated analytics. For the GSAL model to be effective, it is imperative that it:

1) Fulfill a broad spectrum of security functions
2) Operate with Bi-directional flows
3) Support all applications and protocols

For the Analytics model to be effective, it is imperative that it:

- Provide capturing of packet headers and not full packet structure to be able to optimize cost, capability and cycle time.

- Perform Deep Packet Inspection only on demand or an as needed basis
- Correlate every alarm coming out of a network or application sensor to be able to create a forensic case on a virtual basis similar to the one FBI does on a physical basis to solve problems.

Otherwise, every network will suffer the same limitations and challenges as today's proxy-based cloud security technologies. Proxies work with only a handful of protocols, are limited to proxy-aware applications and are most often directional, with support for either inbound or outbound communications, but not both. Proxy-based cloud security tools ultimately make delivering security more complex, since their limitations still mandate build-out of one-off traditional security infrastructure, forcing some functions to stay local while shifting other functions to one or more cloud security players. This makes for a disjointed and convoluted security platform. Use of a Ubiquitous Security Abstraction Layer will address many pain-points making security:

Simple: Though the Security Abstraction Layer itself will be a complex platform, it will significantly simplify protection of applications, assets and end-points by eliminating the need for products, their associated dependencies, implementations, management and logistics.

Agile: Even though on-demand compute or ad-hoc inter-parties' connection communications are extremely agile, securing applications and assets continues to be manual and complex. The GSAL supports multiple direct and indirect connectivity options including physical, encapsulated and obfuscated (virtual front-ending of applications over public networks). This versatility allows GSAL subscribers to utilize their existing connectivity to tap into the Abstraction Layer. This is crucial since all agility is lost with proprietary connections.
Adaptive: There is always the next big threat. Addressing the next big threat has been painful, requiring product selection, acquisition, implementation and operationalization. After all that effort, the protection offered only works for the local environment and nowhere else. Adaptive security must incorporate dynamic analytics in conjunction with traditional control and threat management approaches with real-time analysis and mitigation. This will allow security to consistently evolve with the methods hackers use.

The GSAL should also allow dynamic implementation of new and emerging security enhancements as on-demand functionalities. Once implemented, the enhanced functionalities can be applied centrally to all distributed assets.

Cloud Enabler: Moving security to an abstraction layer requires that the user experience be the same or faster than the traditional security infrastructure in use today. This means that end-to-end performance must be the same or better with communications redirected to the GSAL. This is a big obstacle to overcome, however, once this issue is addressed, it will solve the challenge of consistent performance end-to-end. Running applications today in the cloud may make them ubiquitous, but are they consistently useable from all regions?
There may be other options to address security concerns, but GSAL will undoubtedly simplify the current complex and disjointed protection and mitigation model. This is perhaps the most viable, if not the only, way to solve the security problem for the 60 billion IoT devices forecasted by 2022. We consider the Ubiquitous Security Abstraction Layer a strong candidate to be the dominant delivery method for security-as-a-utility moving into the future, especially for organizations lacking the budget, infrastructure and expertise to develop an in-house solution to the distributed compute and access problem. In fact, security products will soon represent the most expensive way for an organization to limit its security capabilities for the 3-5-year life of the product. Security via a Ubiquitous Security Abstraction Layer is the most strategic way to tame the security beast by focusing on operating security rather than managing products.

6.3 Security Concern at Network Layer

Securing the network layer is the only way to ensure your application is not flooded with attacks which could be easily blocked at that outermost layer. Common network level threats include information gathering, sniffing, spoofing and denial of service (DoS).

The popular framework developed for ensuring security at network layer is Internet Protocol Security (IPsec). As well as any other protocol above IP such as ICMP, OSPF etc. IPsec protects the entire packet presented to IP layer including higher layer headers. Gateways and networking systems assist in the routing and networking of data packets to their intended destinations. If the gateway communicates using wireless protocols, the attacker will use wireless attacks to link to the gateway or internal network. As a result, the attacker will be able to carry out further attacks, such as hello flood, sink hole, black hole, traffic analysis, worm hole, selective forwarding and RPL exploit. Some of these security threats and attacks are briefly in table 5.

The RPL protocol: A new routing protocol for IoT devices is IPv6 Routing Protocol for Low-Power and Loss Networks (RPL). According to [100], RPL is a standardized lightweight protocol that is mostly used in 6LoWPAN networks. By using an Objective Function (OF), RPL creates a Destination-Oriented Directed Acyclic Graph (DODAG) between the nodes in a 6LoWPAN network. OFs enhance routing metrics such as the Expected Transmission Count (ETX) in order to form routes in the DODAG. Both unidirectional traffic towards the DODAG root and bidirectional traffic between nodes and the root are supported by the protocol. A single 6LoWPAN network can have more than one RPL instances, and

a global DODAG can have a local RPL DODAG among several nodes. The IPv6 address of the node is used as its ID. Nodes also store their DODAG neighbors in a list and they can have one or more parents, except for the root. In addition, all nodes have a rank where it's lowest at the root. RPL comes with new ICMPv6 control messages. DODAG Information Object (DIO) messages are initially sent by the root. These messages contain information about the rank of the broadcasting node (which is the distance of the node from the backbone network), the OF, and the DODAG ID. Apart from that, DIO messages help maintaining the DODAG. If a node gets a DIO message, it determines its rank (according to the advertised rank in the received message) and the cost of getting to the sending node from itself. Each node sends these messages in intervals based on trickle timer [101]. This timer also prevents sending unnecessary DIO messages. In order for a node to join the network, it must get a DIO message or multicast a DODAG Information Solicitation (DIS) message to request a DIO message. When other devices get the DIS message, they will start broadcasting DIO messages, and the new node can join the DODAG. Then, a Destination Advertisement Object (DAO) message is sent by the new node to its parent. In some cases, parents may send DIO messages to sub-DODAG in order to request DAO messages. DAO messages are important for creating downward routes (from root to node). Nodes update their routing table when a DAO message is received. If routing tables are empty or if packets are destined for the root, the node will forward a packet up to its most preferred parent.

Table 4
Security Threats and Attacks in network Layer

Attacks	description
Hello flood	Message flooding is amongst the biggest network layer threats. By sending multiple route establishment requests to a network or node. The nodes in the network interpret a hello message as coming from within and mark it as a communication route.
Sinkhole	Sinkhole attack is the most destructive routing attacks in IoT environment. It creates the network traffic and collapses the network communication. It used different routing metrics. The metrics are fake link quality, shortest path etc. [12]
Black hole	When the attacker node drops all incoming packets, it causes the topology to change in the network, the number of control messages to increase and the attacker node to be isolated from the network in a short time. However, black hole attack can be combined with different attacks.
Traffic Analysis	The attacker analyses the traffic and saves a copy for later use in this attack. As a result, the interface can be managed using the traffic that was previously communicating with the gateway. The traffic or data that have been checked are reused in a different context [19].
Wormhole	Wormhole attack is one of the most severe attacks taking place at 6LoWPAN adaption layer of RPL network. In this type of attack, a pair of attacker nodes forms a tunnel between two nodes as if they are directly connected to each other to misguide network traffic.
Selective forwarding:	A special case of black hole attack is selective forwarding attack, where compromised node drops packets selectively, which may deteriorate the network efficiency.
RPL exploit	The Routing Protocol for Low-Power and Loss Networks (RPL), the de facto routing protocol for Internet of Things (IoT) offers little protection against various forms of routing attacks. An attacker can exploit the routing system of RPL to launch destructive and devastating attacks against an IoT network.

6.3.Security Concern at Transport Layer

Different kinds of threats and attacks which cause serious security challenges at the Transport layer are jamming, eavesdropping, false data injection, unfair access, congestion, Hello flood, DoS, DDoS, SCA, DE synchronization, MQTT exploit, session hijacking, SYQ flooding, timing attack, etc. Some of these security threats and attacks are briefly discussed below.

- **DE-synchronization:** The transmissions between two nodes allows an attacker to break actual links between them. Trying to send fabricated messages to both sides of communication, such as false flag types of messages, is an example of this type of attack. By forcing them to lose their synchronization, they will lose their ability to communicate.

- **Session hijacking:** In session hijacking, an attacker steals the session ID and pretends to be the legitimate user to take over a user's online session. The attacker can spoof the user's session ID and do anything the authorized user can do on the network once the attacker obtains it.

6.4.Security Concern at Computing Layer

This part of the IoT infrastructure supports data storage and computer remote control. If cloud servers are not properly configured, they can then lead to the server and smart devices being exploited. Different kinds of threats and attacks which cause serious security challenges at the computing layer are malicious attack, SQL injection, data integrity, virtualization, software modification, illegal access, identity theft, flooding attack in cloud, cloud malware injection, access attack, false data injection, path-based DoS, hole attack, exhaustion attack, cloud outage, signature wrapping, storage attack, etc. Some of these security threats and attacks are briefly discussed below in table 6.

Table 5
Attacks at computing layer

attack	description
Malicious Attack:	A malware attack is a common cyber-attack where malware (normally malicious software) executes unauthorized actions on the victim's system. The malicious software (a.k.a. virus) encompasses many specific types of attacks such as Ransomware, spyware, command and control, and more.
SQL injection	A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. [22].
Illegal Access	These attacks, known as social engineering, often involve some form of psychological manipulation and utilize malicious links in email, pop-ups on websites, or text messages.
Storage Attack	The main problem here is that hackers will slow down the activity of the device as they use the cloud storage resources, but it will continue to operate. This means it may seem that nothing is malicious and that the machines are probably just struggling with their processing capacity.
Access Attack	An attempt to access another user account or network device through improper means. If proper security measures are not in place, the network may be left vulnerable to intrusion.
Software modification	An IoT device can be compromised by modifying its software or firmware by using physical or remote access to take unauthorized actions. By patching or substituting code, or by making code extensions, the vulnerability can be exploited further.

6.5.Security Concern at Operation Layer

Different kinds of threats and attacks which cause serious security challenges at the operation layer are fake information, badmouthing, unauthorized access, users' privacy compromise, stealing users' critical information, MITM, secure on-boarding, firmware attack, software attack, illegal intervention, end-to-end encryption attack, interrogation attack, DoS, etc. Some of these security threats and attacks are briefly discussed below.

Illegal Intervention: Cloud services are typically provided, monitored, and managed through APIs and software user interfaces. Although, cloud service providers are engaged diligently to improve APIs and interfaces, this boom has additionally extended safety dangers related to them. Cloud specialist organizations utilize a particular structure to give APIs to developers, making their frameworks more endangered against an attacker. In 2018, the social media platform Facebook suffered a security breach that affected around 50 million users due to a flaw [23]. API flaws, particularly when linked to user interfaces, may provide the attacker a direct path to steal employee or client credentials.

Unauthorized Access: Access control is an approval system that permits authentic clients to acquire information. Multi-client access and simultaneous altering of design systems ought to be vigorous against multi-client access. When numerous clients can alter the designs of different segments of the IoT frameworks, simultaneous execution of setup changes and simultaneous altering of arrangement records effectively leads to temperamental framework status. In IoT applications, access control is important because if access is compromised, the entire IoT framework becomes susceptible to attacks.

6.6.Security Concern at Application Layer

The application layer manages the services offered to the clients. This layer serves applications such as tell health, industrial automation, smart metering, and so on. This layer has its own set of security concerns that are unique to each program. Different kinds of threats and attacks which cause serious security challenges at the application layer are briefly discussed below in table 7.

Table 6
Attacks at application layer

attack	description
Malicious code	Malicious code is code inserted in a software system or web script intended to cause undesired effects, security breaches, or damage to a system.
Software Modification	Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file.
Data tampering	Data tampering is the act of deliberately modifying (destroying, manipulating, or editing) data through unauthorized channels. Data exists in two states: in transit or at rest. In both instances, data could be intercepted and tampered with. Digital communications are all about data transmission.
Cross-site script	XSS (cross-site script) is a technique attackers use to insert malicious code into a website that is otherwise trusted. If an XSS attack is successful, the IoT system will be under the complete influence of the attacker.
Identity Thefts	IoT systems deal with plenty of personal and sensitive information. Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number,
Virus attack	The objective of these attacks is to breach the confidentiality of the system. The risk of these attacks is significantly higher for smartphones, sinks, or gateways in IoT networks. Hence, IoT applications must seriously consider mitigating viruses and malware.
Spyware attack	Installed on IoT devices without consent, spyware is an installation program that collects information. Using this type of attack, attackers are looking to gather sensitive information about users by monitoring their behaviour. Signature, behaviour, and specification-based techniques are some common approaches to spyware detection.
Code Injection	Attackers usually use the simplest or easiest way to break into a device or network. If the device is endangered to spiteful scripts and misdirection as a result of inadequate code tests, it will be the first point of entry for an attacker.
Intersection	System integrity is a critical feature of the IoT framework. When a system's integrity is compromised, there is a high risk of safety and security threats. High activity stress or irregular process conditions, network or device failures, multiple warnings, executing previously unexecuted error path code or system recovery code, or wrongly executed commands do not cause the system to crash. This necessitates extensive research.
Brute force attack	A brute force attack involves systematically trying and guessing every possible passphrase or password combination to gain access to the system. Crypto-analysts are ultimately able to identify the correct one which allows them access to the system.

7.Conclusion

Today using the IoT with smart computing devices has made lives more convenient. From the introduction of IoT into human life have all benefits from data analytics, automation, and smart devices. Nevertheless, the unprecedented growth in IoT has also been crippled with many vulnerabilities and challenges. Further, the IoT's heterogeneous design expands the attack surface and adds new challenges to an already vulnerable IoT network. The successful compromise of the system's security may have fatal consequences for users. The overall security of the device must be considered to ensure that critical vulnerabilities are mitigated. Policies and protocols must be enforced as much as possible to deter threats and attacks. The main objective of this paper was to gather all the security issues reported in IoT. The classification of those security is also performed. After collecting all those reported issues, the threats and attacks of each layer is presented.

References

[1] Krishna,R.R.;Priyadarshini,A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. Sustainability 2021, 13, 9463. https://doi.org/10.3390/su13169463

[2] Jha, A.V.; Appasani, B.; Ghazali, A.N. Performance Evaluation of Network Layer Routing Protocols on Wireless Sensor Networks. In Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 17–19 July 2019; pp. 1862–1865.

[3] Tiwary, A.; Mahato, M.; Chidar, A.; Chandrol, M.K.; Shrivastava, M.; Tripathi, M. Internet of Things (IoT): Research, architectures and applications. Int. J. Future Revolut. Comput. Sci. Commun. Eng. 2018, 4, 23–27.

[4] González-Zamar, M.D.; Abad-Segura, E.; Vázquez-Cano, E.; López-Meneses, E. IoT Technology Applications-Based Smart Cities: Research Analysis. Electronics 2020, 9, 1246.

[5] Internet of Things in Healthcare: Applications, Benefits, and Challenges. Available online: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challengeshtml (accessed on 12 April 2021).

[6] Cvar, N.; Trilar, J.; Kos, A.; Volk, M.; Stojmenova Duh, E. The Use of IoT Technology in Smart Cities and Smart Villages: Similarities, Differences, and Future Prospects. Sensors 2020, 20, 3897.

[7] Ryan, P.J.; Watson, R.B. Research Challenges for the Internet of Things: What Role Can OR Play? Systems 2017, 5, 24.

[8] Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. Wirel. Netw. 2021, 27, 2595–2613. [CrossRef]

[9] Jha, A.V.; Mishra, S.K.; Appasani, B.; Ghazali, A.N. Communication Networks for Metropolitan E-Health Applications.IEEE Potentials 2021, 40, 34–42. [CrossRef]

[10] Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. Information 2016, 7, 44. [CrossRef]

[11] Rajendran, G.; Nivash, R.S.R.; Parthy, P.P.; Balamurugan, S. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–6. [CrossRef]

[12] Chen, L.; Thombre, S.; Järvinen, K.; Lohan, E.S.; Alén-Savikko, A.; Leppäkoski, H.; Bhuiyan, M.Z.H.; Bu-Pasha, S.; Ferrara,G.N.; Honkala, S.; et al. Robustness, security and privacy in location-based services for future IoT: A survey. IEEE access 2017, 5, 8956–8977. [CrossRef]

[13] Shin, H.; Lee, H.K.; Cha, H.Y.; Heo, S.W.; Kim, H. IoT security issues and light weight block cipher. In Proceedings of the International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Okinawa, Japan, 11–13 February 2019; pp. 381–384.

[14] Gamundani, A.M. An impact review on internet of things attacks. In Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2020; pp. 114–118.[CrossRef]

[15] Kumar, N.; Madhuri, J.; Channe Gowda, M. Review on security and privacy concerns in Internet of Things. In Proceedings of the International Conference on IoT and Application (ICIOT), Nagapattinam, India, 19–20 May 2017; pp. 1–5. [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] 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]

[18] Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88. [CrossRef

[19] Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. BODYNETS 2012, 256–262. [CrossRef]

[20] Abosata, N.; Al-Rubaye, S.;Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity:A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. Sensors 2021, 21, 3654. [CrossRef]

[21] Mann,P.;Tyagi,N.;Gautam,S.;Rana A. Classification of Various Types of Attacks in IoT Environment. In Proceedings of the 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 3 November 2020;pp. 346–350. [CrossRef]

[22] Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. Comput. Sci.Rev.2020,38,10031.[CrossRef]

[23] Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. J. Netw.Comput. Appl. 2017, 84, 25–37. [CrossRef]

[24] Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion Detection Systems in the Internet of Things: A Comprehensive Investigation. Comput. Netw. 2019, 160, 165–191. [CrossRef]

[25] Kouicem, D.E.; Bouabdallah, A.; Lakhlef,H. Internet of things security: A top-down survey. Comput. Netw. 2018, 141, 199–221[CrossRef]

[26] Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. Entropy 2018, 20, 730. [CrossRef]

[27] Elazhary, H. Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. J. Netw. Comput. Appl. 2019, 128, 105–140. [CrossRef

[28] Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security.Digit. Commun. Netw. 2020, 6, 147–156. [CrossRef]

[29] Memon, R.A.; Li, J.P.; Ahmed, J.; Nazeer, M.I.; Ismail, M.; Ali, K. Cloud-based vs. blockchain-based IoT: A comparative survey and way forward. Front. Inform. Technol. Electron. Eng. 2020, 21, 563–586. [CrossRef]

[30] Tran, N.K.; Babar, M.A.; Boan, J. integrating block chain and Internet of Things systems: A systematic review on objectives and designs. J. Netw. Comput. Appl. 2020, 173, 102844. [CrossRef]

[31]]. Fersi, G. Fog computing and Internet of Things in one building block: A survey and an overview of interacting technologies.Cluster Comput.2021,1–31. [CrossRef]

[32] Atlas, H.F.; Walters, R.J.; Wills, G.B. Fog Computing and the Internet of Things: A Review. Big Data Cong. Compute. 2018, 2, 10.[CrossRef]

[33] Hamdan, S.; Ayyash, M.; Almajali, S. Edge-Computing Architectures for Internet of Things Applications: A Survey. Sensors 2020, 20, 6441. [CrossRef]

[34] Capra, M.; Peloso, R.; Masera, G.; Ruo Roch, M.; Martina, M. Edge Computing: A Survey on the Hardware Requirements in the Internet of Things World. Future Internet 2019, 11, 100. [CrossRef]

[35] Ashouri, M.; Lorig, F.; Davidsson, P.; Spalazzese, R. Edge Computing Simulators for IoT System Design: An Analysis of Qualities and Metrics. Future Internet 2019, 11, 235. [CrossRef]

[36] Amiri-Zarandi, M.; Dara, R.A.; Fraser, E. A survey of machine learning-based solutions to protect privacy in the Internet of Things. Comput. Secur. 2020, 96, 101921. [CrossRef]

[37] Adnan, A.; Muhammed, A.; Abd Ghani, A.A.; Abdullah, A.; Hakim, F. An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges. Symmetry 2021, 13, 1011. [CrossRef]

[38] Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A Survey on Security and Privacy Issues in Edge-Computing- Assisted Internet of Things. IEEE Internet Things J. 2020, 8, 4004–4022. [CrossRef]

[39] Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. IEEE Internet Things J. 2020, 7, 4682–4696. [CrossRef]

[40] Parmar, M.S.; Shah, P.P. Uplifting Blockchain Technology for Data Provenance in Supply Chain. Int. J. Adv. Sci. Technol. 2020, 29, 5922–5938. [CrossRef]

[41] Granjal, J.; Monteiro, E.; Silva, J.S. Security for the internet of things: A survey of existing protocols and open research issues.IEEE Commun. Surv. Tutor. 2015, 17, 1294–1312. [CrossRef]

[42] Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.;Maglaras,L.;Janicke, H. Blockchain technologies for the internet of things:Research issues and challenges. IEEE Internet Things J. 2018, 6, 2188–2204. [CrossRef]

[43] Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. IEEE Internet Things J. 2017, 4, 1250–1258. [CrossRef]

[44] Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies,security and privacy, and applications. IEEE Internet Things J. 2017, 4, 1125–1142. [CrossRef]

[45] Malik, M.; Dutta, M.; Granjal, J. A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. IEEE Access 2019, 7, 27443–27464. [CrossRef]

[46] Alshehri, F.; Muhammad, G. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. IEEE Access 2021, 9, 3660–3678. [CrossRef]

[47] Dodig, I.; Cafuta, D.; Kramberger, T.; Cesar, I. A Novel Software Architecture Solution with a Focus on Long-Term IoT Device Security Support. Appl. Sci. 2021, 11, 4955. [CrossRef]

[48] Capella, J.V.; Campelo, J.C.; Bonastre, A.; Ors, R. A Reference Model for Monitoring IoT WSN-Based Applications. Sensors 2016, 16, 1816. [CrossRef]

[49] Sadiku, M.N.; Tembely, M.; Musa, S.M. Home area networks: A primer. Int. J. 2017, 7, 208. [CrossRef]

[50] The OAuth 1.0 Protocol. Available online: http://tools.ietf.org/html/rfc5849

[51] Pawar, M.; Agarwal, J. A literature survey on security issues of WSN and different types of attacks in network. Indian J. Comput. Sci. Eng. 2017, 8, 80–83

[52] Eisenbarth, T.; Kumar, S. A survey of lightweight-cryptography implementations. IEEE Des. Test Comput. 2007, 24, 522–533. [CrossRef]

[53] Alotaibi, B. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. IEEE Sens. J. 2019, 19, 10953–10971. [CrossRef]

[54] Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access 2019, 7, 82721–82743.

[55] Hussain, F.;Hussain, R.;Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. IEEE Commun. Surv.Tutor. 2020, 22, 1686–1721. [CrossRef]

[56] Benkhelifa, E.; Welsh, T.; Hamouda, W. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Commun. Surv. Tutor. 2018, 20, 3496–3509. [CrossRef]

[57] Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481. [CrossRef]

[58] Yugha, R.; Chithra, S. A survey on technologies and security protocols: Reference for future generation IoT. J. Netw. Comput. Appl. 2020, 169, 102763. [CrossRef]

[59] Bhoyar, P.; Sahare, P.; Dhok, S.B.; Deshmukh, R.B. Communication technologies and security challenges for internet of things: A comprehensive review. AEU-Int. J. Electron. Commun. 2019, 99, 81–99. [CrossRef]

[60] Anthi, E.; Ahmad, S.; Rana, O.; Theodorakopoulos, G.; Burnap, P. Eclipse. IoT: A secure and adaptive hub for the Internet of Things. Comput. Secur. 2018, 78, 477–490. [CrossRef]

[61] Mauro, C.; Pallavi, K.; Rabbani, M.M.; Ranise, S. Attestation-enabled secure and scalable routing protocol for IoT networks. Ad Hoc Netw. 2020, 98, 102054. [CrossRef]

[62] Aman, M.N.; Sikdar, B.; Chua, K.C.; Ali, A. Low Power Data Integrity in IoT Systems. IEEE Internet Things J. 2018, 5, 3102–3113. [CrossRef]

[63] Gope, P.; Sikdar, B. Lightweight and Privacy-Preserving Two-factor Authentication Scheme for IoT Devices. IEEE Internet Things J. 2019, 6, 580–589. [CrossRef]

[64] Ahmed, S.; Lee, Y.; Hyun, S.; Koo, I. Feature Selection–Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning. IEEE Access 2018, 6, 27518–27529. [CrossRef]

[65] Asadullah, M.; Ullah, K. Smart home automation system using Bluetooth technology. In Proceedings of the 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies(ICIEECT), Karachi, Pakistan, 5–7 April 2017; pp. 1–6.

[66] Diaz, J.J.V.; Gonzalez, A.B.R.; Wilby, M.R. Bluetooth Traffic Monitoring Systems for Travel Time Estimation on Freeways. IEEE Trans. Intell. Transp. Syst. 2016, 17, 123–132. [CrossRef]

[67] Amendola, S.; Lodato, R.; Manzari, S.; Occhiuzzi, C.; Marrocco, G. RFID technology for IoT-based personal healthcare in smart spaces. IEEE Internet Things J. 2019, 1, 144–152. [CrossRef]

[68] Hutabarat, D.P.; Patria, D.; Budijono, S.; Saleh, R. Human tracking application in a certain closed area using RFID sensors and IP camera. In Proceedings of the 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, Indonesia, 19–20 October 2019; pp. 11–16.

[69] Zou, Y.; Xiao, J.; Han, J.; Wu, K.; Li, Y.; Ni, L.M. Grfid: A evice-free rfid-based gesture recognition system. IEEE Trans. Mob. Comput. 2017, 16, 381–393. [CrossRef]

[70] Fadel, E.; Gungor, V.C.; Nassef, L.; Akkari, N.; Malik, M.A.; Almasri, S.; Akyildiz, I.F. A survey on wireless sensor networks for smart grid. Comput. Commun. 2018, 71, 22–33. [CrossRef]

[71] Jaladi, A.R.; Khithani, K.; Pawar, P.; Malvi, K.; Sahoo, G. Environmental Monitoring Using Wireless Sensor Networks (WSN) based on IOT. Int. Res. J. Eng. Technol. 2017, 4, 1371–7378.

[72] Butun, I.; Morgera, S.D.; Sankar, R. A survey of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutor. 2019, 16, 266–282. [CrossRef]

[73] Can, O.; Sahingoz, O.K. A survey of intrusion detection systems in wireless sensor networks. In Proceedings of the 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Istanbul, Turkey, 27–29 May 2018; pp. 1–6.

[74] Drira, W.; Renault, E.; Zeghlache, D. Towards a secure social sensor network. In Proceedings of the 2013 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Shanghai, China, 18–21 December 2019; pp. 24–29.

[75] Grabovica, M.; Popic, S.; Pezer, D.; Knezevic, V. Provided security measures of enabling technologies in Internet of Things (IoT): A survey.In Proceedings of the Zooming Innovation in Consumer Electronics International Conference (ZINC), Novi Sad, Serbia, 1–2 June 2016; pp. 28–31.

[76] Yang,C.; Shao, H.R. WiFi-based indoor positioning. IEEE Commun. Mag. 2015, 53, 150–157. [CrossRef]

[77] Liu, H.H. The Quick Radio Fingerprint Collection Method for a WiFi-Based Indoor Positioning System. Mob. Netw. Appl. 2017, 22, 61–71. [CrossRef]

[78] Wenbo, Y.; Quanyu, W.; Zhenwei, G. Smart home implementation based on Internet and WiFi technology. In Proceedings of the 34th Chinese Control Conference (CCC), Hangzhou, China, 28–30 July 2015; pp. 9072–9077.

[79] Fan, Y.J.; Yin, Y.H.; Da Xu, L.; Zeng, Y.; Wu, F. IoT-based smart rehabilitation system. IEEE Trans. Ind. Inf. 2014, 10, 1568–1577

[80] Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE Access 2018, 6, 3619–3647. [CrossRef]

[81] Nunez, M. What Is 5G and How Will It Make My Life Better? Available online:https://gizmodo.com/what

[82] Global mobile Suppliers Association. The Road to 5G: Drivers, Applications, Requirements and Technical Development; Global Mobile Suppliers Association: Surrey, UK, 2015.

[83] Li, S.; Xu, L.D.; Zhao, S. 5G internet of things: A survey. J. Ind. Inf. Integr. 2018. [CrossRef]

[84] Fathy, A.; Tarrad, I.F.; Hamed, H.F.; Awad, A.I. Advanced encryption standard algorithm: Issues and implementation aspects. In Proceedings of the International Conference on Advanced Machine Learning Technologies and Applications, Cairo, Egypt,8–10 December 2012; Springer: Berlin/ Heidelberg,Germany,2012; pp. 516–523.

[85] King, J.; Awad, A.I. A distributed security mechanism for resource-constrained IoT devices. Informatica 2016,40, 133–143.

[86] Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 1978, 21, 120–126. [CrossRef]

[87] Koblitz, N. Elliptic curve cryptosystems. Math. Comput. 1987, 48, 203–209. [CrossRef]

[88] American National Standards Institute. Available online: http://www.ansi.org

[89] Institute of Electrical and Electronics Engineers. Available online: http://www.ieee.org

[90] International Organization for Standardization. Available online: https://www.iso.org/home.html

[91] Standards for Efficient Cryptography Group. Available online: http://secs.org

[92] Ravi, S.; Raghunathan, A.; Kocher, P.; Hattangady, S. Security in embedded systems: Design challenges. ACM Trans. Embedded Comput. Syst. (TECS) 2004, 3, 461–491. [CrossRef]

[93] Babar, S.; Stango, A.; Prasad, N.; Sen, J.; Prasad, R. Proposed embedded security framework for (IoT). In Proceedings of the 2nd International Conference on Wireless Communication,Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, India, 28 February–3March 2020; pp.1–5.

[94] Horrow, S.; Sardana, A. Identity management framework for cloud based Internet of things. In Proceedings of the First International Conference on Security of Internet of Things, Kollam, India, 17–19 August 2019; pp. 200–203.

[95] Abie, H.; Balasingham, I. Risk-based adaptive security for smart IoT in eHealth. In Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 24–26 February 2012; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2012;pp. 269–275.

[96] Robertazzi,T.G.Software-Defined Networking. In Introduction to Computer Networking; Springer International Publishing: Cham, Switzerland, 2017; pp. 81–87.

[97] Al Shyheim, F.; Jose, M.; Singh, A.V. Software defined network as solution to overcome security challenges in IoT. In Proceedings of the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 491–496.

[98] Buchegger,S.;Le Boudec, J.Y. Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Lausanne, Switzerland, 9–11 June 2002; ACM: New York, NY, USA, 2002; pp. 226–236.

[99] Michiardi, P.; Molva, R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced Communications and Multimedia Security; Springer: Boston, MA, USA, 2002; pp. 107–121.

[100] Winter T, Thurber P, Brandt A, Hui J, et al. Rpl: Ipv6 routing protocol for low-power and loss networks. RFC, 6550:1–157, 2012

[101] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko. The Trickle algorithm https: //www. rfc-editor.org/rfc/rfc6206.txt, 2011.