Academic Journal of Nawroz University (AJNU), Vol.10, No.4, 2021

https://doi.org/10.25007/ajnu.v10n4a1245

A Review on Security and Privacy Issues in IoT Devices

[1] Reben Mohammed Saleem Kurda, [2] Umran Abdullah Haje, [3] Mohammed Hussein Abdulla, [4] Zhwan Mohammed Khalid

[1] Department of Information System Engineering Techniques,, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Iraq

[2,3,4] Department of Computer Science, College of Basic Education, University of Raparin, Ranya, Sulaymanaiha, Iraq

ABSTRACT

In everyday lives, the Internet of Things (IoT) has been used in everywhere. It is used for the monitoring and documentation of environmental improvements, fire safety and even other useful roles in our homes, hospitals and the outdoors. IoT-enabled devices that are linked to the internet transmit and receive a large amount of essential data over the network. This provides an opportunity for attackers to infiltrate IoT networks and obtain sensitive data. However, the risk of a loss of privacy and security could outweigh any of these benefits. Many tests have been carried out in order to solve these concerns and find a safer way to minimize or remove the effect of IoT technologies on privacy and security practices in order to protect them. The issue with IoT devices is that they have small output modules, making it impossible to adapt current protection methods to them. This constraint necessitates the presentation of lightweight algorithms that enable IoT devices. In this article, investigated the context and identify different safety, protection, and approaches for securing components of IoT-based ecosystems and systems, as well as evolving security solutions. In addition, several proposed algorithms and authentication methods in IoT were discussed in order to avoid various types of attacks while keeping the limitations of the IoT framework in mind. Also discuss some hardware security in IoT devices.

Keywords: Internet of things, IoT privacy, IoT security, IoT technology, hardware security, IoT attacks.

1. Introduction

The Internet of Things (IoT) is a collection of 'things' that are embedded into the internet and use computers, software, cameras, and drives to collect and exchange data. The IoT systems provide sensors and the computing ability to be used in multiple settings. Figure 1 shows some IoT technologies, such as home automation, smart cities, smart grids, healthcare and medical networks, connected cars, and so on. IoT devices can produce interpret and take action knowledge about actions of individuals [1]. IoT apps offer resources that contribute tremendously to the lives of users, because of the privacy and protection of the person, they can cost enormously. Since IoT vendors do not have a strict security feature, safety specialists have cautioned against the possible risks of a large number of risky web-based devices [2].

The first IoT botnet in December 2013 discovered by researchers from Proof Point, in one of the security companies. Evidence notes that about 25 percent of botnet consisted of things other than computers such as smart tv, baby surveillance and other home gadgets. A Manchester-focused domain name service provider based in New Hampshire, has recently had service failures due to what seemed to be a well-coordinated attack [3].

Fig. 1. Internet of thing Applications

Data protection and security continue to be enormous problems for IoT applications that pose a whole new level of online user privacy concerns. That's how they can also monitor user behaviors, not just gather personal details, such as user names and phone number (e.g., where you are in your house and what your customers had for lunch). After the never-ending range of information concerning significant infringements in records, customers are hesitant for good reason to put so much personal information on public or private clouds [4].

New inventions or modifications to old technology are created every day. Take for example the new developments in the 5G network [8]. In IoT networks and implementations, 5G is supposed to play an important role. The researchers are attracted with their high frequency and bandwidth by the potential risk of protection and privacy. However, the short wavelength requires a shift in the grid, which is why more base stations have to cover the same field with wireless technology. This new structure presents additional challenges, including fake base stations security threats and possible solutions must be understood [9].

This work provides an overview of IoT implementations, advantages and possible threats. In addition, provide a mechanism to review and improve best practices for protection through the implementation and analysis of existing systems or the creation of new ones. On the basis of these results, suggest that these threats be avoided and the security flaws be corrected. The aim is to direct regulatory authorities in the development and application of more adequate protection, privacy controls, training of end-users and IoT stakeholders.

The IoT protection and privacy topics are discussed in four areas in this survey article. The rest of this article explained as the following. The first section introduced IoTs. Section two describes the IoT architecture. Challenges in IoT security and privacy discussed in section three. In the fourth section limitations of IoT device determined. In the fifth section types of IoT attacks are discussed. In the six section regarding hardware security in IoT devices. Discussion in the section seven. Lastly, conclusion is presented.

2. Internet of Things

IoT is a Physical device or items are connected to the internet so they may interact and communicate with one other and with their users, allowing the user to monitor or control them remotely. IoT is used at the three layers; a very important role is played by every layer. Figure 2 shows the IoT layers architecture, as well as the technologies and protocols they utilize to do their tasks [10].

The ability to translate the capabilities of cell network and information transmission into today's most used computing devices has transformed IoT into new dimensions using information technologies [11]. The IoT is primarily concerned with enhancing the interconnection between individuals and things, as well as important or critical data related to them on the Internet [11, 12]. As a result, there are so many questions around authentication and management of access [13].

In addition, IoT gives people, objects, and things themselves a whole new means of communicating [14]. The Internet of Things is going to reinvent the fate of the Internet in order to make the lives of people so smoke-free that wireless communicate with everyone else [15]. Now one day, these intelligent objects are attacked by a bad-intention hacker, who then undermines the safety of these computers so that IoT can spread the danger further beyond the internet [16]. As shows in figure 2, the IoT comprises usually of three layers: perception, network and an application layer, each layer has its own security challenges and countermeasures. This plays an essential part in IoT. All these layers perform particular duties and need to be integrated for the correct functioning of IoT. With the increasing number of devices linked to IoT, security concerns and assaults on each layer may be increasingly likely. Security attack taxonomy in IoT was designed to better identify distinct IoT safety concerns and to include stronger security solutions [17-19].

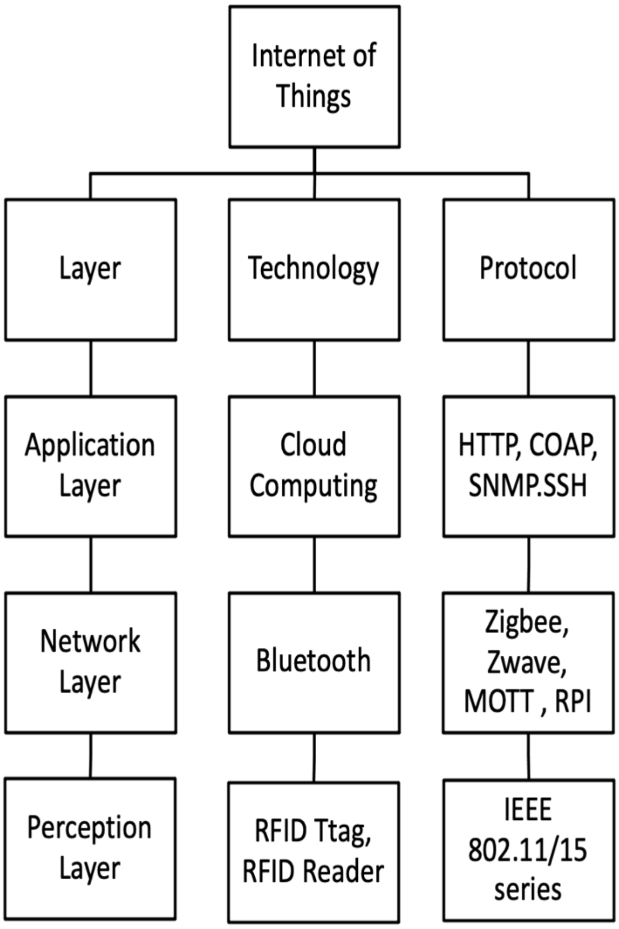

Fig. 2 Architecture of IoT [10]

Several IoT security problems and challenges have been released. The IoT structured networking protocols and cross-counter processes were studied by Granjal et al. [5] where necessary in the area of the IoT protection, the key issues found in 7 categories, were identified.

By Sicari et al. [6] authentication, Access control, private ness, con- Finance, safe middleware, mobile security and compliance policies, With the main research challenges And the latest IoT security solutions. Some unanswered questions were posed and hints for potential investigations were suggested. The study of centralized and divided methods was the subject of Roman et al. [7] They presented an attacker's model for clustered and hierarchical IoT architectures and addressed the key issues and promising solutions for security frameworks. In the table 1, we've collected a list of the most common IoT security issues at each IoT layer.

Table 1 shows the most common….security threats against each IoT layer

IoT Layers	Security threats	Description
Perception Layer	Unauthorized access, Availability, Spoofing attack, Selfish threat, Malicious code, Denial of services [Dos], Transmission threats, Routing attack.	Three security problems confront the IoT perception layer. As IoT nodes operate outdoors, they are susceptible to physical attack. It is possible for an attacker to interfere with components of the computer. As a second example, The dynamic network's heterogeneous nature enables for mobility. IoT devices make up a large portion of this. A computer's capacity to do calculations, on the other hand, It has a high power consumption and a limited storage capacity, which makes it problematic. Threats and attacks of all types can befall them. Third, Considering that the Internet of Things relies on wireless technology to transmit data, Other existing waves, including information, can cause a decrease in the frequency of the sound [20].
Network Layer	Date breach, Public key and private key, Malicious code, Denial of services, Transmission threats, Routing attack.	The broadcast nature of the transmission channel and the compute and power limitations of the sensor node make the network layer more susceptible to DOS assaults. Passive monitoring, traffic analysis, and eavesdropping attacks can undermine the privacy and confidentiality of the network layer, in addition to DoS attacks on the network. Due to the data interchange between devices and remote access techniques, several attacks are possible.
Application Layer	Remote configuration, Misconfiguration, Security management, Management system	As IoT lacks standards and worldwide polices that regulate the creation and interaction between different apps, the application layer faces several security-related concerns [21]. Since the applications use various authentication techniques, integrating them might be a challenge while simultaneously providing identity authentication and data protection. In turn, applications that evaluate the data might be burdened with an enormous amount of work, which has a negative influence on the services' availability. It is important to consider the volume of data that will be sent, as well as the interaction between users and different apps, while building IoT applications.

	User control over data exposure and authentication of other communication partners must be built into certain technologies [22].

3. Challenges in IoT Security and Privacy

IoT has offered enormous advantages to consumers but still some obstacles.

The main fears of the cited analysts and technology experts are cyber security and privacy threats. Both of these are a considerable challenge for both businesses and public bodies. The flaws in IoT technology have been highlighted by prevalent high-profile cyber security attacks [23].

None of these challenges, for example protection and confidentiality, have a more important impact on IoT adaptation. Unfortunately, though, it does not always happen until a violation is committed, leading to massive harm such as the destruction of crucial information, that consumers have the necessary recognition of the security impacts. With the continuous safety violations that affect the privacy of customers, there is now a decrease in the consumer's appetite for poor protection. The IoT in market quality did not do well in a new study of privacy and protection.

1.1 Security

The IoT differs from ordinary computers and is vulnerable to security problems [19]. Below point mentions difference ways to provide security in IoT.

- Several systems for large-scale internet deployment of Things are expected. An excellent example is the sensors.
- The use of IoT usually involves a series of devices with similar features, or almost identical ones. This similarity increases the severity of any security flaw that can impact all of them greatly.
- Many organizations have already developed guidelines on the conduct of risk assessments. This move means that there is no precedent for the possible number of connections between IoT products. It is also evident that all of these systems immediately connect and communicate with other devices irregularly. This requires consideration of open IoT tools, technology and strategies.

Despite the fact that the security problem in the IoT field is not recent, IoT deployment has presents special issues that must be tackled. The consumer's confidence is in the Internet of Things devices, and the systems are protected from vulnerabilities, particularly as the technology becomes more passive and embedded into daily lives. Through not having proper secure data sources, poorly secured IoT devices and services are one of the most critical routes for cyber-attacks and consumer data leakage. If the system is not well protected and wired, the interconnection of the IoT systems ensures they have the ability to impact international security and internet resilience. The problem of the overwhelming use of IoT uniforms is clearly causing this action.

It also makes sure that IoT consumers and developers are expected to guarantee that all users and the internet itself are noticed as damages in addition to the right to mechanically link them to other computers. It is limited to how it protects a threat like denial of service (DoS) by replay attacks or Authentication used. Data secrecy is one of the major vulnerable areas of IoT security as insecure applications are proliferating due to the natural variety in IoT data storage. If you can take a contactless credit card example [24].

credit card can be read without the IoT verification of card numbers and names; This enables hackers to buy merchandise using a card holder's bank account number and name [19].

A middle guy that uses the communications channel to classify nodes that connect networks with third parties is one of the most common IoT attacks.

The bank server sees the transaction as legitimate when a central attack occurs such that a person's name cannot be identified by the adversary [25].

3.1 Privacy

The efficiency of IoT depends on the extent to which citizens' privacy decisions are valued. Full adoption of IoT can contribute to privacy issues and potential harm related to IoT. The fact that respect for customer privacy and privacy is essential in ensuring the trust and autonomy of consumers on the Internet, connected devices and associated services is crucial to be well understood [4].

There is a lot of effort to ensure that IoT redefines privacy issues such as increased surveillance and tracking. Privacy problems are caused by the omnipresent, intertwined intelligence objects, through which knowledge is sampled and disseminated almost anywhere in IoT. The ubiquitous connectivity over Internet connectivity is another crucial element in addressing this issue, since it is easier to display personal data from anywhere in the world, unless a particular device is used [26].

3.2 Interoperability

An environment of fragmented IoT-owned technological use is deemed to prevent market advantage. Although full interaction between goods and services is not always feasible, customers may not want to buy products or services where vendor lock-in has no options or concerns. Lowly built IoT devices may mean that they have a detrimental effect on network services [27].

Cryptography is another main function used for many years in many security systems [28]. A single protection framework cannot be used as an e-defensive device against committed attacks. It thus needs different protection layers against threats to IoT authentication. Hackers can be avoided by developing more sophisticated safety features and incorporating them into goods. This evasion is when consumers purchase devices with adequate safety measures that avoid vulnerabilities. The mechanisms for cybersecurity reflect several steps being taken to ensure stable IoT [29].

In addition, a number of considerations and issues may affect the efforts made to protect the internet of devices, including:

- Remote access: IoT systems use different remote access network such as Wireless, ZigBee and Z-Wave. Relevant controls that may be used to deter cyber-criminals are generally not discussed. Via these remote access protocols hackers may easily create malicious connections.
- Automation: Companies and end-users also use the IoT-systems automation property in data collection or business simplification. Included AIs will however use malicious sites where these origins are not listed, meaning that threats can enter in the device.
- Embedded Passwords: IoT devices store passwords that are embedded for helping service technicians solve or update operating systems problems remotely. However, hackers can use the feature to penetrate protection devices.
- Occasional updates: typically, security fixes are updated by IoT vendors on a quarterly basis. Often upgraded are OS models and safety updates [30]. Hackers thus have time to break safety codes and steal classified information.
- Authentication for the improper device: Most IoT apps do not use authentication services to limit or restrict risks to the network. In doing so, attackers enter the door and violate confidentiality.
- Various third-party apps are available on the Internet, with various software applications that companies can use to carry out complex activities. The validity of these applications cannot, however,

be readily detected. Installing or accessing end users and staff would automatically cause threats to penetrate the system and cause corruption in the embedded database.

- Weak system surveillance: all IoT producers typically configure specific device identifiers to manage and track machines. Such distributors, however, do not have safety policies. Therefore it is very difficult to detect suspect online activity.

4. Limitations of IoT Device

Why are IoT protection features as used in conventional internet hard to protect and apply? The question of IoT limitations and their impact on the use of the latest encryption instruments in the conventional Internet was raised by Trappe et al. [31] the battery life and computing power are the two major drawbacks.

4.1 Extension to Battery Life

Due to the fact that some IoT equipment is used in areas where charging is not available, they are only restricted in the energy required to perform the intended features. To alleviate this dilemma, three possible methods can be used. The first is to use minimum safety standards for the system, which are not particularly advised if confidential data are handled. The second solution is to improve the power of the battery. Most IoT cameras, however, are compact and lightweight. For a bigger battery, there is no extra capacity. The final solution involves power harvesting from natural resources (such as the sun, fire, agitation and wind), but the infrastructure would need to be upgraded, and budgetary expenses would skyrocket [32].

4.2 Computing Lightweight

The paper [31] stated that traditional encryption cannot operate on IoT systems because computers have little memory capacity that cannot accommodate sophisticated cryptographically algorithm computing and storage requirements. The writers recommended reusing existing features to support protection measures for restricted devices. For instance, a physical layer authentication is used to detect whether the signal transmission is from the intended transmitter in the expected region by applying signal processing on the receiver side.

Analog information can also be effectively encoded by a transmitter using a certain analog trait. This analog complexities of fabrication cannot be expected or regulated and should be used as a single key. The authentication method requires little to no overhead energy when radio signals are used. Kotamsetty et al. [33] suggested latency reduction solution in IoT processing by using latency hiding techniques to process queries using encrypted data, which consist of broken down large-size inquiry findings in small data sets. This model helps to calculate a data set when collecting the rest of the encrypted information. Furthermore, the study suggested a data-size algorithm that adjusts the algorithm adaptively to reduce the difference between estimation and contact latency in order to determine the optimal data size required in each iteration to minimize latency. There are two data-size algorithms: First, the scale begins with the large query size fraction. The starting size is set in the second version. Results showed that the method suggested outperforms current latency methods for greater data sizes queries. Shafagh et al. [34] proposed IoT encoding CP algorithm. The solution allows for secure storage in the cloud of encrypted IoT information and efficient management of data base requests over encrypted data. Alternative lightweight cryptographic algorithms are in particular used to replace additive homomorphic encryption and Elliptic Curve El Gamal algorithms and to change the order preserving them to comply with computer IoT computer limitations. The platform replaces connectivity in an End-to-End mechanism for the web-based program, where encrypted data is saved on the client side from personal data devices in a cloud database and encrypted data is performed. The key is a personal computer that takes away all the secret keys from a relying official. Three key parts of the device architecture are: IoT, consumer and cloud. By loading system data directly on the smart device or through a gateway as a wearable tracker you can save application data on the Cloud. The papers addressed only the most common IoT processing queries for encryption mechanisms. The concept can however be expanded to include further plans. Compared to current programs, the experiment findings showed an increase in the time efficiency. Salami et al. [35] suggested a lightweight, smart house-built encryption scheme based on the latest Identity Crypto that identifies the public key without digital certificates. This system is known as the stately IBE system of Phong, Matsuka and Ogata (PMO). This is the overview of the stately encryption scheme of IBE and Daffier Hellman (DH). The study analysis examines the security method for core encryption and encryption to improve the reliability of the proposed scheme and reduce connectivity costs. The second data-size algorithm is emphasized because the chip text generated by key encryption is greater than the encryption size. The result was a double-sub algorithm: key encrypt and data encrypt. The first is an encryption session key, and the second is the encryption of information. The resulting cipher text is transmitted independently from the sub algorithms such that data cipher text is transmitted several times without adding the key chip text. The findings of the assessment suggest that the scheme suggested is Secure from threats by plaintext. Also in terms of accelerating encryption operations and reducing about a third of communications overheads, the efficiency evaluation reveals that it executes the standard IBE scheme

5. Different Attacks on IoT Security

IoT security is a major challenge, as it is dynamic, heterogeneous and has a vast number of interconnected tools. The opposition will attack the IoT system using the protocol defects, or use a malicious program, or cryptographically breaking these nodes (e.g. physical vulnerability) by damaging or exploiting them or by using malicious programs. As Figure 3 shows, On the basis of these flaws, the attack was classified as physical, network, software and encryption attack, classified to four groups. From the whole assault of this group considered one that is most dangerous.

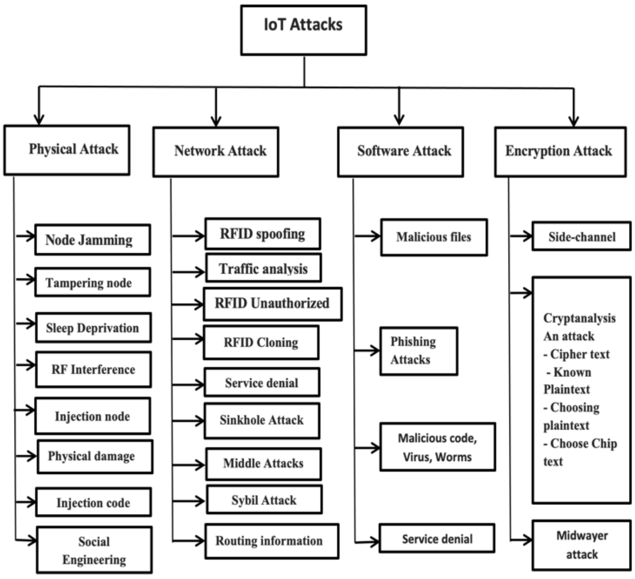

Fig. 3 IoT and its attacks on security [36]

A risky attack after a physical attack was a malicious injection node attack.

As the services are not alone suspended, the documents are still changed.

The threat from Sinkhole's network attack is the riskiest. It can also lead to risks such as selective routing, modification or decrease of packets by an attacker, and can also attract all traffic to the base station. We've picked worms from a system assault as the most uncertain. Worms are probably internet malware's most damaging and destructive form. The computer is impaired by the auto replication program's use of security troughs in network applications and hardware It can uninstall device files, steals information like passwords, it can change passwords, it triggers screen lockouts, etc. without your notification.

Andrea et al. [37] the paper categorizes IoT attacks into four major physical, network and cryptography groups. The physical assault begins while the intruder is near the IoT. When an attacker accesses the IoT network, the network attacks happen and a certain computer is exploited to inflict harm. The IoT application program attack has some glitches that cause the attacker to enter IoT devices by means of which the code is affected. Finally, when the hacker break off IoT encryption, an encryption attack will occur. The study concluded IoT needed multiple steps to make it more secure e.g. authentication, digital certificates secured booting, privacy encryption and reliable software in order to allow approved users to access and power IoT devices only. In response to other investigators' assaults [38].

5.1 Physical Attacks

These attacks concentrated on the hardware in IoT devices:

- Sleep Deprivation : The attacker aims to use more power to close nodes [39].
- WSN Node Jamming: the hacker interferes with the use of a jammer to make wireless communication. It permits denial of service attacks [40].
- Tampering node: In the attacker the node is modified and confidential information such as encryption key can be obtained [40].
- RF Interference: The intruder attacks the server by transmitting radio frequency signals to the service Denial. This signal is used for contact with RFID [41].
- Injection malicious node. The attacker injects into two or more nodes a new malicious node. It updates the data and sends the incorrect data to the other nodes. In order to attack a malicious node, the attacker uses the different nodes [42]. The adversary attaches a B clone node first. Inserts subsequent other malicious nodes (node M1). These two nodes work together to perpetrate the attack. This results in crashes at the victim's node. The assaulted node would interrupt any packet receiving/sending. Therefore, a misrepresentation of the targeted node (the legal node) as malicious could be influenced by the inference of watchdog nodes. A tracking (MOVE) system used to avoid this attack. The control node(s) outcomes can also be verified and malicious activity can be properly detected. The verifier node decides whether or not the node is malicious, according to the acknowledgment.
- Physical damage attack: the intruder physically destroys IoT device components which lead to a service denial [43].
- Injection of malicious code: The opponent physically inserts a malicious code into the IoT node. The intruder should have full IoT device power [39].
- Social Engineering: The perpetrator communicates and manipulates IoT devices consumers physically. In order to accomplish its objectives the intruder receives confidential information [44].

5.2 Network Attacks

The attacks are aimed to the server of the IoT system. Get into the network through a wireless network or router attack, etc. as described below.

- RFID spoofing occurs as an attacker spoofs RFID signals the information transmitted from an RFID tag is then captured by the device. Spoofing attacks have incorrect information that seems to be right and that the machine acknowledges [38].
- Traffic analysis attacks occur when an intruder intercepts and analyses communications in order to collect network intelligence [40].
- RFID Unauthorized Access: if the correct authentication is not granted in RFID schemes, the opponent can see, change or erase node information [37].

- RFID Cloning: Adverse RFID copies of a new RFID tag in this attack. No copying of the original RFID tag ID The attacker will either inject incorrect data or monitor the data passage through the cloned node [37]
- Service denial: An attacker is overwhelming the network with massive traffic, which blocks services to their intended customers [45].
- Sinkhole Attack: an opponent takes up a sinkhole attack and performs an attack with this node inside the network. The node in question passes the wrong routing information on to its neighboring nodes and attracts traffic. It then changes the data and reduces the packets. In paper [46], The sinkhole nodes definition approach is straightforward. The proposed approach generates the hop dictation and identification in the database whenever a node sends a packet to its neighboring node. The average count of hop is thus comparable to the average and lowest count of hop. If this minimum is less than the average hop value, the sinkhole attack is vulnerable.
- Middle Attacks: The attacker stops connectivity across the internet between the two nodes. You get sensitive information by waking up [37].
- Sybil Attack: Malicious node in this attack, which takes and behaves as several nodes. For example, the single node device will vote several times over in the Wireless Sensor Network [39].
- Routing information attacks: The attacker may spoof, modify, or deliver routing information to complicate the Network. As a result, packets are permitted or removed, wrong data is transmitted or the network is split.

5.2.1 Attacks on Software

The assailant targets using malware, worms, spywares etc. to rob documents, reject facilities etc.

- Malicious files: The intruder may have access to the computer with malicious scripts inserted.
- Phishing Attacks: The attacker receives personal information, such as the username and passwords, through email spoofing and flawed websites.
- A malicious code may be used to damage the device by the attacker. Virus, Worms, Trojan Horses, Spyware, and Aware: These codes are shared through e-mail attachments. Without human interference, the worm will replicate. The virus will find with an anti-virus, malware detection and an intrusion tracker. In The study [47] Mixes abnormalities detection and signatures to protect the system from worms with a nice pot. This hybrid scheme takes advantage of the detection and protection of the worms of the honeypot and irregularities and signatures. Service denial: the attacker blocking applications from the user's application layer.

5.2.2 Encryption Attacks

The threats are based on destroyed encryptions and on the private key.

- Attacking the side channel: The attacker uses side channel information encrypting the system. The text does not include the plaintext or chip text; it includes data on the performance, the time it takes, the number of errors, etc. This information is used to detect encryption key by attackers. Various forms of side-channel attacks are available, such as timing attacks, simple and differential power analysis, and differential fault analytics [23] attempt to attack time. Timing attacks rely on the time it takes to perform operations. It contains information on the secret keys [48]. Cryptosystems perceive various inputs at various times. The hitting of RAM cache, the instructions running during unfixed time, etc.
- Cryptanalysis An attack: In this antagonist uses either plaintext, or cipher text to extract the encryption key. Different forms of attacks are carried out based on the methodology used [37]. Cipher text attack [48], Known Plaintext Attack

[48], Choosing plaintext Attack [48], Choose Chip text Attack, Midwayer attack [39]

Andrea et al. [37] A new classification of IoT attacks is available in four different categories: physical attacks, network attacks, software, and attacks for encryption. A part from data encryption IoT protocols, each of these encompasses an IoT device layer. The physical attack occurs while the attacker is within a radius from the device. The network attacks can exploit the function of the IoT network. Software attacks happen because the attackers manipulate the possibilities and destroy system due to certain security defects in IoT programs.

6. Hardware Security in IoT Devices

"Pain pyramid," as seen in Figure 4, based on the Cisco IoT model of comparison, is defined in Reference [49] and assess from a risk point of view for the IoT system. On the top of the pyramid is the most fragile section of the IoT structure with the lesser effects. Sensors are the most fragile component of the IoT ecosystem, since they are the most available on top. The relation between the sensors and the data gathered from the sensors is the next sensitive aspect. Attackers using sensors or the network may obtain links to these data. Then come the hardware abstraction and firmware for communicating with the device and the data, which lays out the application programming interface (API). In the end, the hardware platform, such as SoC, DSP (digital signal processors), etc., is a lowest usable component of the pyramid. While the hardware platform is at the bottom of the pyramid, it needs the greatest consideration, because in the event of an attack, the device has the greatest damage effects. Hardware can be said to form the basis for the IoT device and to be the most pain-causing component in the event of a cyberattack. IoT protection should then start with security of hardware. HT is the largest threat to hardware, which is why this article focuses on.

In a number of pieces, Al-Omary et al. [50] studied hardware dependent IoT protection. First, the paper demonstrated IoT protection needs such as anonymity, honesty and trustworthiness. The framework used in IoT/CPS systems was transferred to the layers of operation, network layer, and vision layer in separate layers. Subsequently, the debate on IoT/CPS stability and standardization. The paper then explained the distinction in several layers between IoT and wireless safety in detail. Finally in the paper various IoT hardware techniques were listed and a variety of hardware modules were discussed. The paper concludes other hardware-dependent security solutions

that can be improved and delivered at reasonable cost for building an IoT-CPS system that's cheap and secure.

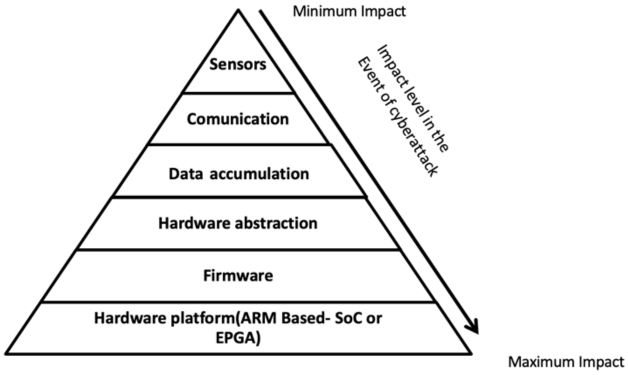

Fig. 4 Based on the vulnerability study, Pyramid of Pain

7. Discussion

It is obvious from previously stated literature reviews that The IoT protection has several aspects and needs many countermeasures to improve it, numerous research studies have concentrated on because of their importance. In This section of study showed that researchers presented different aspects of IoT security and many important features. In Table 2, shown these aspects and objective assessment between these experiments that have been proposed by previous researchers.

Table 2: Summarizing some areas of IoT security

Author	Year	IoT security aspect	Discerption

Li and Lan [10]	2012	IoT architecture	Analyze the safety standards in the various layers of the lOT perception layer, network layer and application layers, and then provide a framework of security infrastructure that can provide a technical reference for establishing secure information security structures in the future.
Trappe et al. [31]	2015	Limitations of IoT device	IoT limitations and their impact on the use of the latest encryption instruments in the conventional Internet have two major drawbacks,
Kotamsetty and Govindarasu [33]	2016	latency reduction solution in IoT	Two main characteristics of currency: (i) have a modern latency-aware adaptive algorithm and (ii) an IoT new service cache architecture. Both inputs together reduce query latency while keeping overhead resources at a minimum. The reliability for latency and energy efficiency of the proposed adaptive algorithm has been assessed. The findings show that, relative to current energy efficiency techniques, the proposed adaptive approach greatly improves the latency capacity.
Andrea et al. [37]	2015	Attacks on IoT security	• There would be a physical intrusion when the attacker is close to the IoT device. • Network attacks occur after an attacker receives IoT network access and manipulates an attacker's device in order to cause damage. • A software assault happens where an IoT application contains bugs that allow an offender to enter and destroy IoT computers. • An invasion on encryption takes place when a hacker violates the IoT encryption to initiate an attack.
Alaba et al. [19]	2017	Compares various dangers to IoT security	Discuss and analyze the potential threats on the IoT security situation. Open testing questions and threats to IoT security delivery are also outlined. The aim of this survey is to act as a helpful manual for current threats in protection and vulnerabilities in IoT's Heterogeneous Environments.
Yang et al. [32]	2017	Limitations of IoT device	1- Extension to Battery Life Some IoT equipment is used in areas where charging is not available, they are only restricted in the energy required to perform the intended features. To alleviate this dilemma, three possible methods can be used. The first is to use minimum safety standards for the system, the second solution is to improve the power of the battery. The final solution involves harvesting electricity from natural resources. 2- Computing lightweight Traditional encryption cannot operate on IoT systems because computers have little memory capacity that cannot accommodate sophisticated cryptographically algorithm computing and storage requirements.
Ahmad et al [8]	2018	Security of 5G systems	Provides a comprehensive analysis of security problems in clouds, networking software and virtualization network features, and device privacy issues. This article will now be available to solve these problems and provide potential guidance for stable 5G networks.
Al-Omary et al. [50]	2018	Hardware Security in IoT Devices	New safety issues arise from the increased use of IoT/CPS platforms. Because of the design of the IoT/CPS scheme, which relies heavily on connected low-energy devices with sensors, As an example of this form of encryption, consider TEE, TNCand Hardware-based modules in IoT.
Tawalbeh et al. [9]	2020	Challenges and Solutions in IoT	Used the AWS-enabled IoT cloud environment for top layer implementation (the cloud). In order to secure user data protection, authentication protocols and essential management sessions had to be held between each layer. Also introduced Security Certificates. The suggested device template not only removes potential safety risks, but may also serve to mitigate cyber security risks from each of the layers, server, edge and IoT with best security techniques.

8. Future Work

As IoT employs the conventional network architecture to communicate between multiple devices, it has lacunae and vulnerabilities of old network architectures.

The present network design has to be improved, or new network architecture needs to be created, lightweight, effective, and safe, so that performance and safety related problems may be resolved to a large extent. The authors look forward to the problems and the safety layers on each network tier as a future piece. This study covers IoT systems security and privacy from several points of view. It also offers solutions for IoT system assaults. The IoT systems and sensitive user data protection are provided with several effective options. But the assailants seek to increase the effectiveness and strength of their assault techniques.

This makes the provision of stronger IoT systems protection solutions necessary. An effective solution might offer for protecting IoT systems based on the facts and information presented in this survey paper in the future. A solution that minimizes the risk and enables IoT systems to eliminate most of the hazards. A solution adapted to the kind and type of architecture of IoT systems.

9. Conclusion

The IoT is everywhere in our everyday lives. They are used for monitoring and recording environmental change, fire safety and other useful roles in our home, in hospitals and in outdoor environments. Nevertheless, all these benefits may be immense with the lack of privacy and security. Many research studies have been done against these problems to improve their privacy and protections security and to reduce or mitigate the influence of IoT products. The problem is that the new security system cannot be implemented for the limited output section of IoT devices. This constraint demands that lightweight algorithms supporting IoT devices be presented. The study examined many proposed IoT algorithms and authentication mechanisms to avoid various kinds of attacks, Explore the IoT-based ecosystem and technologies and identify different stability, privacy issues and methods and potential security approaches, security solutions. Moreover, In order to prevent various forms of attacks despite the IoT interface limitation, several proposed algorithms and authentication methods were examined. And talk about some IoT computer hardware security.

10. References

1. I. Analytics, "Why the internet of things is called internet of things: Definition, history, disambiguation," ed, 2014.
2. V. M. Kumar, N. Yamsani, S. N. Korra, A. Harshavardhan, and B. V. Kumar, "A Scope on Auspices and Seclusion Issues in Internet of Things."
3. B. Lam and C. Larose, "How did the internet of things allow the latest attack on the internet?," ed, 2016.
4. S. Chaudhary, "Privacy and security issues in Internet of Things," Int. Educ. Res. J., vol. 3, pp. 2433-2436, 2017.
5. J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," IEEE Communications Surveys & Tutorials, vol. 17, pp. 1294-1312, 2015.
6. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer networks, vol. 76, pp. 146-164, 2015.
7. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, pp. 2266-2279, 2013.
8. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," IEEE Communications Standards Magazine, vol. 2, pp. 36-43, 2018.
9. L. a. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," Applied Sciences, vol. 10, p. 4102, 2020.
10. L. Li, "Study on security architecture in the Internet of Things," in Proceedings of 2012 international conference on measurement, information and control, 2012, pp. 374-377.
11. R. H. Weber, "Internet of Things–New security and privacy challenges," Computer law & security review, vol. 26, pp. 23-30, 2010.
12. S. Kraijak and P. Tuwanut, "A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends," in 2015 IEEE 16th International Conference on Communication Technology (ICCT), 2015, pp. 26-31.
13. C. Qiang, G.-r. Quan, B. Yu, and L. Yang, "Research on security issues of the internet of things," International Journal of Future Generation Communication and Networking, vol. 6, pp. 1-10, 2013.
14. M. Burmester and B. De Medeiros, "RFID security: attacks, countermeasures and challenges," in The 5th RFID academic convocation, the RFID journal conference, 2007.
15. X. Xingmei, Z. Jing, and W. He, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the internet of

things," in Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, 2013, pp. 825-828.

16. A. Kamble and S. Bhutad, "Survey on Internet of Things (IoT) security issues & solutions," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 307-312.
17. A. K. Hussain, "A modified RSA algorithm for security enhancement and redundant messages elimination using K-nearest neighbor algorithm," IJISET-International Journal of Innovative Science, Engineering & Technology, vol. 2, pp. 858-862, 2015.
18. M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in 2016 3rd International Conference on Electronic Design (ICED), 2016, pp. 321-326.
19. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10-28, 2017.
20. J. Choi, S. Li, X. Wang, and J. Ha, "A general distributed consensus algorithm for wireless sensor networks," in 2012 Wireless Advanced (WiAd), 2012, pp. 16-21.
21. A. V. Singh, V. Juyal, and R. Saggar, "Trust based intelligent routing algorithm for delay tolerant network using artificial neural network," Wireless Networks, vol. 23, pp. 693-702, 2017.
22. Z. Bi, L. Da Xu, and C. Wang, "Internet of things for enterprise systems of modern manufacturing," IEEE Transactions on industrial informatics, vol. 10, pp. 1537-1546, 2014.
23. H. Song, G. Fink, and S. Jeschke, Security and privacy in cyber-physical systems: Wiley Online Library, 2017.
24. M. Medwed, "Iot security challenges and ways forward," in Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, 2016, pp. 55-55.
25. M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," IEEE Communications Surveys & Tutorials, vol. 18, pp. 2027-2051, 2016.
26. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.
27. D. Zaldivar, A. T. Lo'ai, and F. Muheidat, "Investigating the security threats on networked medical devices," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020, pp. 0488-0493.
28. X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A security framework for the internet of things in the future internet architecture," Future Internet, vol. 9, p. 27, 2017.
29. A. T. Lo'ai and T. F. Somani, "More secure Internet of Things using robust encryption algorithms against side channel attacks," in 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1-6.
30. F. Dalipi and S. Y. Yayilgan, "Security and privacy considerations for iot application on smart grids: Survey and research challenges," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2016, pp. 63-68.
31. W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," IEEE Security & Privacy, vol. 13, pp. 14-21, 2015.
32. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, pp. 1250-1258, 2017.
33. R. Kotamsetty and M. Govindarasu, "Adaptive latency-aware query processing on encrypted data for the Internet of Things," in 2016 25th International Conference on Computer Communication and Networks (ICCCN), 2016, pp. 1-7.
34. H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, "Talos: Encrypted query processing for the internet of things," in Proceedings of the 13th ACM conference on embedded networked sensor systems, 2015, pp. 197-210.
35. S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 382-388.
36. A. Abdullah, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," Cryptography and Network Security, vol. 16, 2017.
37. I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in 2015 IEEE symposium on computers and communication (ISCC), 2015, pp. 180-187.
38. S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (iot)," in 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011, pp. 1-5.
39. M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," International Journal of Computer Applications, vol. 111, 2015.
40. S. Uke, A. Mahajan, and R. Thool, "UML modeling of physical and data link layer security attacks in WSN," International Journal of Computer Applications, vol. 70, 2013.
41. H. Li, Y. Chen, and Z. He, "The survey of RFID attacks and defenses," in 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, 2012, pp. 1-4.
42. [42] F. Kandah, Y. Singh, W. Zhang, and C. Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks," Security and Communication Networks, vol. 6, pp. 539-547, 2013.
43. Q. Gou, L. Yan, Y. Liu, and Y. Li, "Construction and strategies in IoT security system," in 2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE

cyber, physical and social computing, 2013, pp. 1129-1132.

44. F. Salahdine and N. Kaabouch, "Social engineering attacks: a survey," Future Internet, vol. 11, p. 89, 2019.
45. A. Wahid and P. Kumar, "A survey on attacks, challenges and security mechanisms in wireless sensor network," International Journal for Innovative Research in Science and Technology, vol. 1, pp. 189-196, 2015.
46. M. I. Abdullah, M. M. Rahman, and M. C. Roy, "Detecting sinkhole attacks in wireless sensor network using hop count," IJ Computer Network and Information Security, vol. 3, pp. 50-56, 2015.
47. P. Jain and A. Sardana, "Defending against internet worms using honeyfarm," in Proceedings of the CUBE International Information Technology Conference, 2012, pp. 795-800.
48. M. Zulkifli and Z. W. Mohd, "Attack on cryptography," Comput. Secur, vol. 12, pp. 33-45, 2008.
49. V. Venugopalan and C. D. Patterson, "Surveying the hardware trojan threat landscape for the internet-of-things," Journal of Hardware and Systems Security, vol. 2, pp. 131-141, 2018.
50. A. Al-Omary, A. Othman, H. M. AlSabbagh, and H. Al-Rizzo, "Survey of hardware-based security support for IoT/CPS systems," KnE Engineering, pp. 52–70-52–70, 2018.