Security Threats and Attacks in Internet of Things (IOTs)

Sara Mutlaq Almtrafi[1] , Bdour Abduallatif Alkhudadi[1], Gofran Sami[2] and Wajdi Alhakami[1]

[1]College of Computers and Information Technology, Taif, Saudi Arabia
[2] Joint First Year Deanship, Umm Al-Qura University, Makkah, Saudi Arabia

Abstract
The term Internet of Things (IoTs) refers to the future where things are known daily through the Internet, whether in one way or another, as it is done by the method of collecting various information from various sensors to form a huge network through which people, things and machines are helped to make a link between them at all time and anywhere. The IoTs is everywhere around us such as connected appliances, smart homes security systems and wearable health monitors. However, the question is what if there is a malfunction or outside interference that affects the work of these IoTs based devises? This is the reason of the spread of security causes great concern with the widespread availability of the Internet and Internet devices that are subject to many attacks. Since there aren't many studies that combines requirements, mechanisms, and the attacks of the IoTs, this paper which explores recent published studies between 2017 and 2020 considering different security approaches of protection related to the authentication, integrity, availability and confidentiality Additionally, the paper addresses the different types of attacks in IoTs. We have also addressed the different approaches aim to prevention mechanisms according to several researchers' conclusions and recommendations.

Keywords*—Security; IoTs; Security; Attacks*

1. Introduction

Internet of Things (IOTs) is an application development domain that incorporates a range of technologies. Kevin Ashton invented the term 'Internet of Things'In 1999,. The first remarkable aspect of IOTs came from the term that describes. It's a collection of actual interacting things or Objects." Physical objects may be people, vehicles, environments, machines, etc. In addition , each "Thing" has an identifier in order to be identifiable.[1]

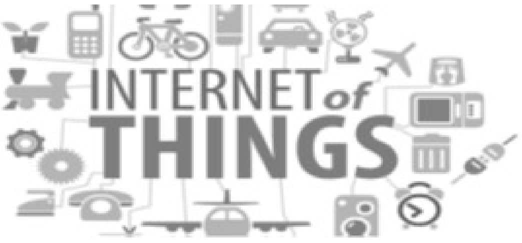

Fig. 1. Internet of Things (IoTs) [2]

As shown in Figure.1. the Internet of Things (IoTs) means that on the internet through which everything is linked. Such as smart home security systems and wearable health monitors and others. This is therefore a advancement of the Internet. It will organically merge different knowledge Sensors with the Internet in order to be configured with a large network with a wider variety, allowing humans, computers and objects to communicate at any time and wherever. IoTs is a significant forum both for a combination or development of multiple technologies similar as huge data, artificial intelligence and cloud computing . It's becoming another business in charge after the Internet. The exponential development of IoTs has entered a variety of fields, like manufacturing, distribution and modern state. The scale of IoT equipment showed an exponential rate of growth or the age for IoTs is coming. GSMA forecast data appeared to exceed the world amount of IoT devices (which include non-cellular and cellular) by 2025 to 25.2 billion by 2025. [3].

Devices required for IoTs are composed of low power radios, software actuators, embedded CPUs (Central Processing Units), and several smart sensors. These devices are capable of sensing, communicating, computing and monitoring environmental conditions by forming wireless sensor network (WSN). They could be embedded in handheld devices, industrial machinery, pollution sensors, medical equipment and more. They offer perspectives that drive businesses to cost savings, productivity gains, and new growth opportunities [4].

The Internet of Things (IoTs) as a new field has many challenges, one of its greatest challenges is the flow of data collected from IoTs devices. These devices monitor human activity all over the day with such sensitivity that makes it easy with analysis of such data to deduce personal habits, behaviors and preferences of individuals. This data is greatly sought for marketing companies for example to provide you with tailored ads, or by hackers to blackmail you. The collected data by different IoTs devices should not be shared with whom you don't know how it will be used [5].

In August 2014, over 500 private pictures of celebrities were hacked and posted online many of them were containing nudity. A few years ago, a group of hackers used rather unconventional methods to break into a casino. They managed to access an internet-connected thermometer in an aquarium and extract all sensitive details from its database [6].

Manuscript received January 5, 2021
Manuscript revised January 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.1.15

The safety and integrity of IoTs devices is still not under full control, there are always Cyber-security vulnerabilities can be exploited by various cyber-attacks. Such attacks have data that may put people's privacy and lives in danger. Imagine If an attacker managed to get access to your camera, your bank account, the control of your automobile vehicle, each scenario represents a disaster [7].

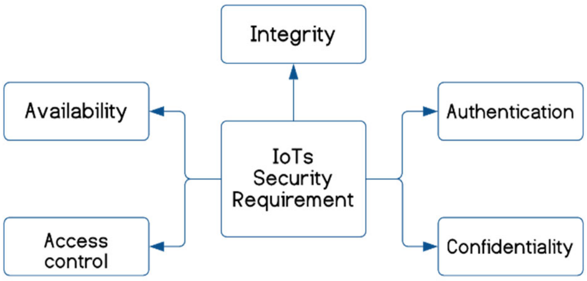

Fig. 2. Security requirements in IoTs

After we saw a form Fig.2, We can see Just security standards that must be implemented in order to achieve a stable communication environment for individuals, devices, processes and items.

1. **Authentication:**

It's about checking users to be sure confidentiality and integrity. Access control for authorized users (user authentication) and verification of data source authentication.

2. **Integrity:**

Prevent unauthorized tampering of data when it is being processed, or in transit or when at rest .Such that Verification of data source , audit trail of user access into the system, audit trail of user access to data , audit trail of changes to data.

3. **Confidentiality:**

Ensure that data is not revealed to or accessed by unauthorized individuals.

4. **Availability:**

Ensure that authorized users can access and use data on demand such that Access to the system, Data input validation.[8]

This paper is organized into five sections, Section 2 , represent the recent publish work by other researcher to achieve the security requirements .while section 3 , focuses on the threats and attacks mechanisms that target the IoTs environment. Therefore, a number of threats has been investigated and how to be prevented by a number of recent techniques . And comprehensive information of the attacks and threats in IoTs has been interduce in the paper . Section 4 , we discuss, and conduct review the security requirement mechanism and attacks that we talked about in sections 2 and 3 . Finally, in section 5, we have concluded our paper.

2. Security Mechanism in IoTs

In order to achieve safety in the Internet of things, we must know how to achieve safety requirements, in this section includes some of the mechanisms that researchers have implemented to achieve the security requirements of the Internet of Things:

2.1 Authentication mechanism in IoTs

Several research have been conducted in literature by other researchers to address the authentication aspect in IoTs [9] [10] [11] [12].

For example, authors in [9] use (TBLUA) which is an abbreviation of Token-Based Lightweight User Authentication. It's a novel technique to provide mutual authenticate mechanism for IoT devices. This approach is more efficient and lightweight solution as it provides relatively more security features and high security level such as Perfect Forward Secrecy, anonymity, and resilience against the well-known attacks.

Paper [10] is considering a related approach. The solution is therefore focused on the use of the Compact Authentication process, based strictly on hashing and XOR operations, of M2M encounters throughout the Industrial IoT environment. That effects becomes characterised by low cost of computing, networking including bandwidth storage, mutual authentication with confidentiality. of device's identity, agreement for session key , And resistance against some attacks such as replay attack, man-in-the-middle attack, impersonation attack the work provided in [11] presents a two-factor authentication system that are done by the method of maintaining the devices of IOTs, where the authentication factors is considered to be highly configurable as its results show that the security is not only strong against attacks, but also effective in computational efficiency. PUFs is a basic encryption system that has good popularity in security and has proven to be effective in many modern businesses, making it the only one of its kind, and the consequence of this is that it is impossible to make a clone of it as the security elements are available through where they suggest that IoT security devices is the solution in this.

The protocol scheme in [12] is introduced for the objects real-world physical, lightweight mutual authentication for an IoT environment . In addition, authers use Lightweight characteristics of the (CoAP) Constraint Application Protocol to allow clients to observe server-based resources in a manner that is energy efficient. They just use (AES) Advanced Encryption Standard with a data rate of 128 bits to set up a protected resource observation session. The scheme is computationally efficient, at the same time connection incurs less overhead, provides a robust defense various attacks such as, resource exhaustion, DOS, physical tampering and replay.

2.2 Integrity mechanism in IoTs

In [13] this paper a scheme a novel lightweight to protection data integrity depended. A delicate watermark is suggested to solve the confusion seen between protection layer and the awareness resource. Improve protection, however, improve protection to maintain zero data disruption. Analysis of outcomes and simulation protection demonstrate that the proposed scheme will successfully achieve low cost data integrity. In addition, the algorithm may significantly avoid a range of attacks, such as forged packet, packet tamper, , packet forwarding , packet delay transmission, and packet replay attacks triggered by malicious nodes.

authors in[14] using essential element revocable signature frameworks to establish a data integrity audit scheme for IoT devices with in cloud storage world. Users use private key attributes to create signature attributes and restrict user consent to use shared data by access control policies. Just because the consumer attribute must be used in the global set attributes or the attribute isn't really much less than unique code, the creator can only use the meaning attribute key to construct a valid signature that can be authenticated just under the signature strategy regulation. At around the same time, the Group Manager (GM) can send confidential service to the third-party auditor (TPA) to monitor the author of the signature and to the customer. is excluded from accessing the data as the company changes, and the user revocation of the user group members is made secure. Formal security review and experimental findings demonstrate that the data-audit schema approach is ideal for IoT devices in the cloud storage environment in terms of performance.

In [15] paper, the authors firstly Propose an improved audit scheme where its TPA conducts each block tag creation including integrity checking rather than the cloud users. Second, a data sharing approach is intended for data owners to exchange data in the cloud through registered users. And then, Merkle Hash Tree could be revamped to preserve a new knowledge frame node and boost authentication and integrity checking for shared information. Those who conclude that the integrity verification scheme experiment guarantees the safety and reliability of cloud data sharing and security examination and is more efficient in computation cost. System to validate data integrity followed by a short signature algorithm (ZSS signature)was proposed by [16] to support public auditing and protection for privacy via providing a trusted third-party or third-party thing. In the signature process, the reduction of the hash function overhead effectively reduces the computation overhead. The scheme proposes to be preserving data privacy via the use of a random masking technique, and the results showed that the scheme can withstand adaptive chosen-message attacks due to its high efficiency and safety.

2.3 Confidentiality Mechanism in IOTs

Based on CS and CSS, a framework of media data acquisition, low-cost and conditionality assured was proposed by [17] for the IoT. The paper presented three types of machinery, including, CSS-driven CS, the authentication mechanism, and the CSS-driven local perturbation. The authentication mechanism uses authentication and access passwords to prevent both passive and active tampering attacks. The results verified the effectiveness of the framework to obtain conditionality, authentication, and low-overhead.

In a study [18], they proposed a combination of covert algorithms that depend on elliptic curve coding (ECC), advanced coding (AES) and algorithm (MD5). And then merging the encodings of the document and the graphic location of the site with another mixed algorithm in order to enable that user to give confidentiality to each device separately, and it was concluded that the algorithm that gives strong secrecy for data transmission is the hybrid algorithm that is the highest confidentiality for transmitting Internet of things data and it gives better and better time for the term w.r.t for each From encryption and encryption time for a file of different size.

This paper [19] created a PTC scheme in WSN for IoT after modifying the RSP concept. Additionally, it included a private and common secret value for the sensor nodes and their secret random values S to form private and secret keys. The use of 0 key, which relies on secret keys and secret indexes, contributed to preserving the confidentiality of the information sensed between the sensor nodes and the BS in order to obtain a coupling value that has an unreliable or indirect trust. A method was proposed to discover the value of the association and the types of trust in a way of mutual trust without any negotiation process for the sensor and making the trust Between the nodes and the rejection of the malicious nodes, they contain a private key to make the association and trust mutual, and the results showed a PTC scheme capable of coping with the attacks of WSN.

The author in [20] study A hybrid solution for protecting IoT communication using data confidentiality and authentication to resolve weaknesses in the IoT network. The hash function was used for authentication with radix-64 conversion and the RSA conversion algorithm has been used for anonymity with radix-64 conversion as a part of the demand for secrecy during contact. The hybrid approach is difficult to decode. In comparison, this strategy helps in the elimination of the external attack on safety issues.

2.4 Access control Mechanism in IOTs

Paper [21] Introduces a new concept strategy for the introduction of the Card-based Entry Control Scheme for the entering and exiting of vehicles in the Truck-Loading Fuel Terminals aiming the system uses (IoTs) concepts. The developed system uses the Radio Frequency Identification (RFID), with its write capabilities. The technology RFID belongs data capture (AIDC) and the automatic identification. As it follows a new design system that is followed to provide performance and develop the topic presented of system with regard to speed, allocated resources and security .

Paper [22] Using a fine-grained access control mechanism for the IoTs devices, as well as a test framework is set up to validate the method. This approach creates fine - grained data control decisions which based on the position and the background details. We are developing anew Access Control Feature that Test Network by integrating the Mininet simulation platform and the WIA-PA-based system of industrial wireless . results Show that access management method will effectively filter unauthorised access of various system sources, access time and other items, request intervention.

2.5 Availability system for IOTs

In the study of the availability of people, the faces to workers are identified, remembered, evaluated and even the attendance is reported against all the index. The proposed method uses a HAAR Face Database Cascade algorithm for the identification, classification and comparison of faces[23]. The primary justification for designing this technology is to benefit people and to remove all the disadvantages involved with the existing and other approaches of the biometrics system. With the support of the divergent combinations for algorithms, the availability analysis of artefacts using IoT has thus proven to be safe and time saving.

Suggests the paper in [24] a technique to develop Markovian chain using tool and the proposed formal procedure. They suggest a special notation which enables step-by-step support of the development chain and the final configuration of MC utilizing digital resources. Estimate the protection and supply of IoTs. The goal is to reduce the risks of errors mostly during Markovian Chain (MC) creation of systems with a rather significant number of states. In table 1 we we summarize the security techniques for each security features.

Table 1. Recent Security *Approach* in IOTs

REF	**Security Requirement**		
	Year	Security features	Security Techniques
[9]	2018	Authentication	Uses Token-Based Light weight User Authentication.
[10]	2017	Authentication	Uses XOR and session key
[11]	2018	Authentication Confidentiality	Uses physically unclonab functions (PUTs)
[12]	2019	Authentication Integrity and Confidentiality	Uses Constrained Application Protocol (CoAP) and (AES)
[13]	2017	Integrity	Uses novel lightweight depended on fragile watermark
[14]	2020	Authentication Integrity and Access Control	Uses attribute-based revocable signature mechanisms, attribute Private key
[15]	2020	Integrity and Confidentiality	Uses lightweight auditing scheme in which TPA
[16]	2019	Authentication Integrity and Confidentiality	Uses short signature algorithm. (ZSS signature) .
[17]	2019	Authentication & Confidentiality	Uses low-overhead, CS and CCS
[18]	2019	Integrity and Confidentiality	AES, ECC and MD5.
[19]	2016	Confidentiality	Uses private secret key.
[20]	2017	Authentication & Confidentiality	Uses hybrid approach and RSA.
[21]	2018	Authentication, Confidentiality & Access Control	Uses RFID belongs data capture (AIDC) and the automatic Identification.
[22]	2020	Access Control and Availability	Uses fine-grained access control method
[23]	2017	Availability	Uses uses the HAAR face library.
[24]	2017	Availability	Develop Markovian chain using tools of software .

. 3. Threats and Attacks in Internet of Things (IoTs)

IoTs as a whole requires overall security which includes System security, network security and security of software:

1. System security: by identifying different security challenges, expected vulnerabilities, designing different security frameworks and providing proper security guidelines.
2. Security of software: functions with IoT applications by managing all security problems.
3. Network Security: deals for protecting an IoT communication system which occurs among various IoT devices.
4.

There are different types of attacks that IoTs face, as they are divided into active and passive, where in active attacks they can be classified into internal and external attacks and their characteristics are that they disturb the services of the system and for passive attacks, the attacker steals information and does not have the ability to steal or attack the system In general, the different attacks can be classified into four forms according to the degree of their severity:

1. Low-level attack: If this attack occurs, it is unsuccessful.
2. Medium level attack: that type of attack, attackers cannot modify or alter the integrity of the data
3. High Level Attack: In this case the attacker can modify the data and change its integrity
4. Extremely high-level attack: In this case, the attacker or intruder can disrupt the network, make the network unavailable, perform illegal operations, or send bulk messages as he enters the network through an unauthorized access. [25].

IoTs attacks can cause very extensive damage which reaches not only users but may extend to reach unsecured governments so it's important to know the expected attacks on the system, discover vulnerabilities in advance and manage to secure them. Figure .3 show some of the security attacks in IOTs. We are going to discuss these attacks and how to protect against them:

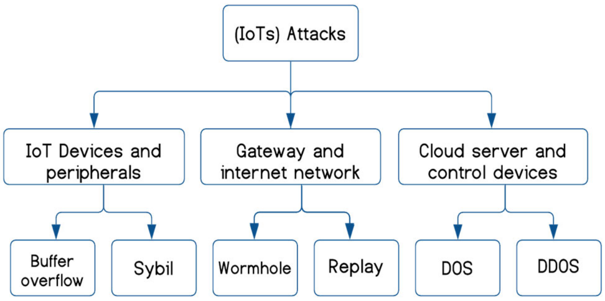
(IoTs) Attacks
IoT Devices and peripherals
Gateway and internet network
Cloud server and control devices
Buffer overflow
Sybil
Wormhole
Replay
DOS
DDOS

Fig. 3. Attacks in IoTs

3.1 Sybil Attacks:

Type of security threat via online Wherever one somebody is attempting to take over the network by taking over several accounts or machines. [26]

An author[26] suggests a trust management system, called a Fuzzy-based Trust Administration System for the Prevention of Sybil Attacks on the Web of Medical Stuff (FTM-IoMT). FTM-IoMT offers trust management to customers of eHealth networks using IoMT infrastructures. This is an intelligent system to identify sybil or unstable nodes as in scheme. The proposed system allows IoMT nodes to gather authentic and valid knowledge through its surrounding nodes as well as to ignore sybil nodes. The trust measure of a node is measured by fuzzy logic processing tracked by trust attributes like credibility, receptivity, and node compatibility. The FTM-IoMT offers a double validation check determined on fuzzy logic processing or a fuzzy filter. A system produces superior performance relative to situation-of-the-art solutions.

It is proposed in [27] that a model be used to formulate an efficient countermeasure upon the Sybil attack. The algorithm using K-mean clustering are suggested to visualise an attacker's deployment position collection process. The findings demonstrate that the suggested model successfully visualises the behaviour of sybil attacker in difficult IoTs conditions. The suggested deployment algorithm reaches 48.7 percent coverage using the K-mean clustering strategy.

A new, scalable, location-based protocol has been proposed and is the Geographic-PBFT protocol, as it is capable of developing applications and it has been proven through [28] that his theory is related to the fact that most IoT-blockchain implementations rely on fixed computers. to capture and process data through Internet of Things where G-PBFT was found to achieve high performance compatibility, low network expenses, high development and scalability by selecting a site-based supporter. As it has a fixed (Internet of Things) computing power higher than other portable devices.

3.2 Denial-of-Service Attacks:

The intruder performs a DoS assault by submitting some requests continuously thereby making the broker busy . and broker will not be able to handle new incoming requests.

In the paper [29] the authors propose a new system for detecting a lightweight intrusion based on an ambiguous logic called MQTT - Secure, through which the wrong activity can be identified when a connection occurs between Internet of things devices. This method uses a system that detects harmful behavior with the help of what is called fulfillment of the fuzzy rule. As it avoids the dense base by exploiting the mysterious base, where it is created dynamically, as this method is used in that it provides special protection for devices from DoS attack, as the results have proven that this method compared to other methods can accurately detect attacks.

A DoS attack are very important Though not just the data sources would be under strike, however in fact the IoT platform itself is under attack. The article in [30] Suggested method called REATO to define and counteract a DoS assault on an IoT interoperation named NOS.. Designed resolution, adjusted to the NOS architecture, or performing indices such as computing attempt, latency, or restoration time, was examined with in detection of faults nodes.

Hybrid-based IDS for IoT networks was proposed in [31], which implemented an IDS application scheme to detect abnormal network traffic from each of the network nodes. They have run IP datasets against it in this method, which can be described as an application, See how architecture may detect odd network packets or block unnecessary IPs until leading to the an initial DoS risk.

3.2 Replay Attacks:

Hacker analyses signals or retains a duplicate for potential use. The interface could be managed using the traffic previously interacted mostly with firewall. [32]

In [33] paper, they enhanced challenge-based anti-attack system has been proposed in order to create an effective authentication system and agreement to create a safe session. it is about message replay is a classic authentication threat. Efficiency and quality safety review reveals that the proposed scheme has a higher degree of protection and is nevertheless highly effective .

They suggest a resource-efficient protection scheme in [34] that involves device authentication with their network administrators, device authentication on various networks, and an attack-resilient key establishment. The formation of a new connection with the system Begins mostly with authentication process, followed by a key startup process.

Each system shares its nonce during the authentication process using that also includes the SID. For each new session, this SID is special and serves as timestamps in their case. Owing to the inclusion of the older SID, which have now stopped, if so. intruder did replays previous session authentication messages, they will be discarded.

3.4 Wormhole Attacks:

Over than double malicious nodes build a hidden path called a tunnel. Such that they should connect with the other nodes at a great speed across the network.[35]

In [35] They addressed the special method of intrusion detection method towards wormhole attack, which mentioned that a wise approach is recommended to eliminate black hole attack also And for ad-hoc network by delivering the directional antenna to the nodes. System decides its special antenna regions to make a link among them. Every node in the network assessed the position of gathering signals from any of them. The relationship between consecutive neighbours was once defined if the direction of the knowledge transfer from both nodes seems to be in arrangment with each other. This additional knowledge allows the detection of wormholes and causes fluctuation in the network. Such that it can be spotted smoothly.

The proposed work in This study [36] is really an application of the Wormhole Attack and Intruder Intrusion Detection Method (IDS). Among the most serious attacks seems to be a Wormhole assault on the 6LOWPAN RPL network adaptation layer. The suggested implementation of a IDS is now in Contiki OS, by using Emulator Cooja. The obtained signal intensity indicator (RSSI) was used to classify the attack and assailant node. After the IDS was applied against Wormhole Attack, it was shown that the IDS architecture detected an attack with a success rate of about 90 percent.

They suggest an approach based on an attack-defense tree in the [37] paper to test effective countermeasures for the security of IoT infrastructure. The suggested solution is to automatically Classify effective counter-measures which could raise the costs for threats, and minimize the likelihood of success. In order to create security configurations relevant to the IoT infrastructure, a compromise between defenses and their effect on attack costs is realized Attack-Defense Exploration tool is built upon a Statistical Model Checking (SMC) tool.

3.5 Distributed Denial-of-Service Attacks:

Unlike simple DoS attacks, DDoS Take a significant percentage of infected hosts are looking to exhaust network resources as quickly as possible.[38]

In [38], they A new system called the multi-layered system is proposed, which depends on the machine learning system and preventing DDoS attacks in the Internet of things system. Features have been discovered for four types of DDoS attacks which are UDP flood, SYN flood, ICMP flood and digital features. Where DDoS attacks are launched as an Internet scenario The objects from eight poles are good, and they concluded that the special detection of DDoS for multi-layer can be by the method of distinguishing between the different packages from the IoT devices with high accuracy where when the packets were detected, the F1-score was greater than 97 percent when detecting the normal beams and the SDN controller is defined Addresses for malicious devices and sending them to the blacklist. The key rules for the SDN are set from the blacklist, whereby all malicious devices on the blacklist are banned immediately in the keys. Therefore, the multi-layer DDoS system that was proposed does not detect malicious systems only, but rather works on Banned it too.

The new algorithm [39] can detect DoS and DDoS attacks early on and before they reach the network. Where this algorithm was designed for the flow of restricted networks and the Cooja Contiki simulation system was created, where the results reached that the algorithm proposed by Aaron performed better than E-Lithe, and a performance evaluation was made in order to evaluate the algorithm, which is the rate of delivery of harmful packets. This proposed algorithm can also be applied to all Internet of things devices from home to mega-industrial environments.

As for [40], they use DDoS, which is based on the blockchain, as it compares devices and analyzes existing methods against attacks. It also provides a system that works on the intgrity, immutability and reliability of transactions, and makes authentication between blockchain's nodes .

3.6 Buffer Overflow Attacks:

Attack of buffer overflow is subverting the function of a privileged program ,so that attacker can take control of this program, then control the host.[41.

In [41] They offered more than one mechanism to prevent over flow attacks such as Preventing the execution of data as it is considered as a protection system that works to prevent the execution of programmatic operations from the memory pool, heap, or stack pages, or by marking memory locations in a specific process, which means that it is not executable unless the site allows or contains executable instructions.

Paper [42] It introduces a new design in order to detect buffer overflow attacks as it is called an improved architectural design for safety devices, as it detects the exceedance of the capacity of the temporary storage device. Verification of instructions and monitoring is part of the design to track the behavior of program implementation and there is another method which is validation of the mark that is used to monitor the characteristics of each segment From memory clips. The implementation of the The architectural construction is taken out on the real platform OR1200-FPGA. The findings showed that the programmes suggested were are working on detecting buffer overflow attacks of warehouse capacity in a large amount, and the experimental result also shows that many temporary storage buffer overflow attacks can be detected with very simple designs and appropriate penalties.

In a study conducted by [43], they studied two types of algorithms, namely the whale optimizer (WOA) and the gray wolf optimizer (GWO), in addition to the use of each of the selection of the head of the block (CH) which is based on the imperialist algorithm (ICA) with a new system of similar wire meshes. The two algorithms solve some problems, especially the problem of increasing the buffer overflow when collecting data, and a comparison was also made between them and the use of different algorithms and other parameters such as Fuzzy-GWO, where the results showed that the two algorithms GWA / WOA have much better results that outperform the other algorithms in all cases. The discovery that the algorithm, which WOA claims, is very efficient when used in heterogeneous networks, as well as the GWO algorithm is very good in the case of large-scale networks, down100 nodes.

3.7 A man in the middle attacks:

Using various properties is willing to oppose contact between two nodes. and that makes him play the role of proxy [44]

A paper [45] in which a modern scheme for Man-in-the-Middle Attacks throughout the Iot technology were suggested to strengthen these attacks as well as the algorithm of such a scheme was formed to create nodes besides routing among IoT devices and to detect anomalies in TTS. in a good way as this helps to increase by detecting intruders in Good time in the internet of things.

Table 2. Attacks Has Been Consider in Recent Paper Related to The IOTs Security

Ref	Attack	Approach and Results	Prevent
[26] [27] [28]	Sybil	An algorithm using K-mean clustering to visualize the deployment location selection procedure of an attacker. Results show that suggested framework effectively visualises the actions of the a sybil attacker while threatening IoTs. A trust management mechanism Fuzzy-based for preventing Sybil Attacks in (FTM-IoMT),It provides a double evaluation. Double test depends on the treatment of both the filter and the fuzzy internet. The studies concluded that the results were very good when compared to modern methods.	G-PBFT
[29] [30] [31]	DoS	A REATO method was introduced to detect the DoS attack on the Internet of Things middleware(NOS).The designed solution, and performance indices like computing effort, Where the recovery and attack time were evaluated while malicious programs were present that harm the devices . Schema a lightweight fuzzy logic-based intrusion detection called Secure-MQTT, Simulation results show. This method detects the attacks with good accuracy when compared to the methods currently used.	Hybrid IDS
[33] [34]	Replay	They presented a framework of user authentication focused on enhanced challenge-response for resist. replay attack as an efficient mutual user achieve authentication and agreement a secure session key. The result show that scheme has a level higher security and is still efficient highly	Session Key Establish ment
[35] [36] [37]	Worm hole	The technique of intrusion detection system for wormholes attack for ad-hoc network by providing directional antenna to the nodes. This additional information enables wormhole The exploration and introduction of the fluctuation of the network. Such that it can be spotted smoothly.They proposed implemented of IDS is in Contiki OS, using Simulator Cooja. It was shown that the IDS was designed to detect an attack with just a success rate of about 90 percent.	Attack Defense Trees
[38] [39] [40]	DDoS	A multi-layer DDoS detection system based on machine learning to prevent DDoS attacks in IoT gateway. Their proposed system can detect DDoS attacks with high accuracy. Also blocks the malicious devices. Algorithm can detect DoS and DDoS attacks at an early stage before entering the constrained network. The results show the algorithm performs better than E-Lithe, proposed by Asma Haroon .	Block-chain
[41] [42] [43]	Buffer over flow	They offered more than one mechanism to prevent overflow attacks such as Data Execution Prevention (DEP) which protection which helps prevent code execution from the stack, heap or memory pool pages. Provides the architectural-enhanced device security architecture to detect directory traversal threats. Implemented on the real device OR1200-FPGA. Empirical research reveals that a vast variety of approaches can be discovered to buffer overflow attacks	GWA/ WOA
[45] [46]	MITM	The algorithm of this scheme was developed to make a dedicated contract for routing between the Internet of Things devices efficiently detect anomalies found in the TTS. This proposed solution contributes to real-time intruder disclosure is enabled to increase the safety of IoTs networks	Client-Server Based Authenti cation

In [46] They created a new user-defined device architecture. Authentication of systems with large systems against intruders Amount of transmission rate of data. Using a reliable method to ensure data integrity. When data is sent to the server, it is authenticated, especially the incoming data, on other hand, Client authentication will provide easy communication on just this device and reduce time of authentication. The term coined scheme implemented checks for any changes in its instantaneous details. Additionally, Simple devices such the motors or other industrial devices or sensors devices, monitor data integrity. Instead of using encryption, the authentication scheme based on the client-server is essentially used to prevent complicated operations and protect big data. In Table 2, we summarize the attacks and the protection methods for each attack.

5. Discussion

Several recent approaches that have been conduct by more than one researcher in the secure of IOTs will be discuss in this section. (TBLUA) which is an abbreviation of Token-Based Lightweight User Authentication. They use lightweight math operations such as hash and XOR. Similar mechanism used by another researcher. also use lightweight authentication mechanism only based on hash and XOR operation. Their result is characterized by low computational cost, communication, and storage overhead, with achieving mutual authentication, confidentiality of device's identity, agreement for session key. Another research work used different mechanism which called (PUFs) privacy-preserving tow factor authentication scheme for IOTs devices .it is result of the manufacturing process of Integrated Circuits (ICs) which introduces random physical variation to the micro-structure including its IC, allowing it unique.. and are thus difficult to predictable and impossible almost to clone. Advanced Encryption Standard (AES) is used by other researcher with even a block size of 128 bits, to set up a secured session for resource observation.

Many research papers use several mechanisms to achieve integrity. One of them used watermark. they use sha1hash function and secret key. Another researcher uses an attribute-based revocable signature mechanism to create a scheme for data integrity auditing IOTs devices in the cloud storage environment. It is suitable for devices IOTs in the environment cloud storage with respect to performance. Researchers also have also done The block-tag engendering and efficiency is carried out through a lightweight auditing design in which the (TPA) is implemented verification instead of the data owner. They also design data as the cloud data is shared with authorized users.

To achieve confidentiality, the researchers used several mechanisms. Where a framework has been proposed in order to obtain reliable, reliable and low-cost media through one of the authors, as he uses a coding system consisting of three layers. Advanced Encryption Standard (AES), Elliptic curve cryptography (ECC), and Message Digest algorithm (MD5), Another one uses a different algorithm which is hybrid Privacy is a mixture of advanced encryption, message summary algorithm and elliptic curve encryption, where document encryption and graphic encryption are combined and combined to the site to give the privacy of each device with the mixed algorithm where the hybrid algorithm is the most powerful thing that works to transfer data to the Internet.

Another researcher using It is a hybrid method used to secure communications on the Internet of Things through data confidentiality and authentication in order to address vulnerabilities in the Internet of things, authentication using radix-64 switching hash and maintaining radix-64 confidentiality as it uses the RSA algorithm to provide security when communicating and also to maintain data confidentiality. Each provides good security that as it's troublesome to hybrid solution decrypt.

To achieve access control, researchers used several and different mechanisms .one of them uses SDN technology to reduce the load on the switch. It is suitable for use in large networks to reduce the load. Another one of them introduces a new system in the implementation of the control system to access the card from the document in order for vehicles to enter and exit in the truck loading by using the (IoTs) system in order to improve the system's performance in speed and allocated resources, safety.

To achieve Availability, there are researchers used The algorithm called HAAR library for facial recognition and detection, and in the availability analysis through it, the faces of the employees are detected, compared, and the attendees are distinguished on the database. Another company is working to develop a chain of Markovian for the critical Internet of things feature and system by To use the suggested standardised protocols and the key concern is to reduce the levels of errors in the production of (MC) programmes. that have a number of the cases a very large. More than one researcher provided a mechanism to protect against some attacks. We mention some of the attacks here and review the mechanisms that were used.

The Buffer overflow is common attack in IOTs, and this kind of attacks can be prevented easily by using WOA /GWA This mechanism outperformed many of the algorithms used because it stored data temporarily in CH alpha, CH beta and CH delta. To reduce the burden. another mechanism can be implemented to provide security mechanism prevent Buffer overflow attacks Where a mark is placed on the memory locations in a specific process indicating that it is executable as the site contains explicit instructions for executable programming the researchers also presented solutions to sybil attacks. by using G-PBFT. They compared this mechanism with PBFT which works well in small networks. They have been able to prevent sybil attacks as they have used powerful devices as the endorsers to conduct the intensive consensus computation. other approach provides security mechanism prevent sybil attacks by using trust management mechanism. Where the nodes and trusted nodes are recognized within the system through this smart machine.

The Dos is common attack in IOTs and this kind of attacks can be prevented easily by using hybrid design of signature-based IDS, anomaly-based IDS to provide an accurate detection mechanism. But this design has not been tested in real-world. another mechanism can be implemented to provide security mechanism prevent Dos attacks by using The harmful activity was discovered by the use of what is called intrusion detection system where it is vague and called for Secure-MQTT detects harmful activities among Internet devices stuff that protect devices from forming special attacks of DoS. we see that the researchers who provided a replay attack prevention scheme had a high level of security in an IoT environment with limited resources. Unlike nonce schemas, which brings the disadvantage that the node has stored a list of unrecovered characters in the Device-specific memory as this is not possible in IOTs technology as it contains specific storage for limiting resource devices.

For man-in-the-middle attacks, the mechanism was client-server-based authentication which is faster and secure instead of encryption algorithms. the wormhole attack is also common attack in IOTs, and this kind of attacks can be prevented by using C-IDS to detect wormhole attacks in Internet of Things networks. this approach increases the cost of the attack and reduce the possibility of its occurrence. We think it is an appropriate solution, but it does not prevent these attacks from occurring. another mechanism can be implemented to provide security mechanism prevent wormhole attacks by intrusion detection system for wormholes attack Where a special system is provided for nodes where the node uses special areas for communication, and these areas are defined. As each pair of nodes is evaluated through which the direction of receiving information is received, and from that the relationship between successive neighbors is made, if the information flow of the two nodes is compatible with each other.

Finally, the approach that has been suggested by researchers to mitigate DDos attacks is to use blockchain technology. We think that this solution is appropriate, but this technique is still in the early stages of implementation. But they also offer SDN technology to use with the blockchain, as SDN filters and detects DDos attack traffic while using the blockchain to announce the attack. different approach used Whereas, the DDoS system has been discovered and adopts a machine learning system that prevents DDoS attacks in the Internet of things, where when abnormal packets appear, MAC addresses and IP addresses of harmful devices are sent to the console and this works on adding them to the blacklist, and then it is attended immediately their proposed system can detect DDoS attacks with high accuracy.

5. Conclusion

Internet of Things (IoTs) is a way to establish a virtual network and interactions between objects and people as well as objects with each other. Such grown has become an integral part of our live. It facilitates and aids many areas such as the professional and the academic sectors. IoTs information transmits through sensors which must be protected from unauthorized users. However, as IoTs technology develops, security and privacy need to be improved. Thus, there should be more attention on security requirements and on exploring novel possible security solutions to avoid threats and attacks. This step is vital to help IoTs environment to prevent all potential risks. In this study, we explored the recent research suggested by more than one researcher on how to achieve the IoTs security requirements and mechanisms such as confidentiality, authentication and access control, integrity and availability. In addition, we presented the common types of attacks mechanisms that target the IoTs environment and the available methods to prevent them. We discussed and compared the mechanisms of the security requirements recommended by many experts. This could benefit the reader to obtain a deeper understating of IoTs network security and threats. In the future work, we keep search for more recent approaches papers in order to highlight the novel propose work for investigation and highlight their benefits for contributing to the security mechanism in IoTs.

References

[1] Abbasi, M., Yaghmaee, M. H., & Rahnama, F. (2019, April). Internet of Things in agriculture: a survey. In 2019 3rd International Conference on Internet of Things and Applications (IoT) (pp. 1-12). IEEE.

[2] Jaladi, A. R., Khithani, K., Pawar, P., Malvi, K., & Sahoo, G. (2017). Environmental monitoring using wireless sensor networks (WSN) based on IOT. Int. Res. J. Eng. Technol, 4(1), 1371-1378.

[3] Li, J., Yi, X., & Wei, S. (2020, June). A Study of Network Security Situational Awareness in Internet of Things. In 2020 International Wireless Communications and Mobile Computing (IWCMC) (pp. 1624-1629). IEEE.

[4] Kocakulak, M., & Butun, I. (2017, January). An overview of Wireless Sensor Networks towards internet of things. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1-6). IEEE.

[5] Loukil, F. (2019). Towards a new data privacy-based approach for IoT (Doctoral dissertation, Université Jean Moulin Lyon 3)

[6] Tabari, A. Z., & Ou, X. (2020). A First Step Towards Understanding Real-world Attacks on IoT Devices. arXiv preprint arXiv:2003.01218.

[7] Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 5, 41-70.

[8] Jabangwe, R., & Nguyen-Duc, A. (2020). SIoT Framework: Towards an Approach for Early Identification of Security Requirements for Internet-of-things Applications. e-Informatica Software Engineering Journal, 14(1), 77-95.

[9] Dammak, M., Boudia, O. R. M., Messous, M. A., Senouci, S. M., & Gransart, C. (2019, January). Token-based lightweight authentication to secure IoT networks. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-4). IEEE.

[10] Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., ... & Bastos, J. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. IEEE Internet of Things Journal, 6(1), 288-296.

[11] Gope, P., & Sikdar, B. (2018). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. IEEE Internet of Things Journal, 6(1), 580-589.

[12] Jan, M. A., Khan, F., Alam, M., & Usman, M. (2019). A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems, 92, 1028-1039.

[13] Zhang, G., Kou, L., Zhang, L., Liu, C., Da, Q., & Sun, J. (2017). A new digital watermarking method for data integrity protection in the perception layer of IoT. Security and Communication Networks, 2017.

[14] Wang, Y., Chen, C., Chen, Z., & He, J. (2020). Attribute-Based User Revocable Data Integrity Audit for Internet-of-Things Devices in Cloud Storage. Security and Communication Networks, 2020.

[15] Lu, X., Pan, Z., & Xian, H. (2020). An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. Computers &Security,92,101686.

[16] Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B., & Xin, Y. (2019). A secure and efficient data integrity verification scheme for cloud-IoT based on short signature. IEEE Access, 7, 90036-90044.

[17] Zhang, Y., He, Q., Chen, G., Zhang, X., & Xiang, Y. (2019). A Low-Overhead, Confidentiality-Assured, and Authenticated Data Acquisition Framework for IoT. IEEE Transactions on Industrial Informatics.

[18] Chanal, P. M., & Kakkasageri, M. S. (2019, July). Hybrid Algorithm for Data Confidentiality in Internet of Things. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.

[19] Lin, C. H., Hsieh, W. S., Mo, F., & Chang, M. H. (2016, March). A PTC scheme for internet of things: Private-trust-confidentiality. In 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA) (pp. 969-974). IEEE.

[20] Purohit, K. C., Bisht, S., Joshi, A., & Bhatt, J. (2017, September). Hybrid approach for securing IoT communication using authentication and data confidentiality. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-6). IEEE.

[21] Bahgat, M. M., Farag, H. H., & Mokhtar, B. (2018, December). IoT-Based Online Access Control System for Vehicles in Truck-Loading Fuels Terminals. In 2018 30th International Conference on Microelectronics (ICM) (pp. 1-4). IEEE.

[22] Wei, M., Liang, E., & Nie, Z. (2020, January). A SDN-based IoT Fine-grained Access Control Method. In 2020 International Conference on Information Networking (ICOIN) (pp. 637-642). IEEE.

[23] Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017, April). Towards better availability and accountability for IoT updates by means of a blockchain. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 50-58). IEEE.

[24] Volochiy, B., Yakovyna, V., & Mulyak, O. (2017, September). Queueing networks for availability and safety assessment of the IoT data service. In 2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT) (Vol. 1, pp.393-396).IEEE.

[25] Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): a comprehensive study. International Journal of Advanced Computer Science and Applications, 8(6), 383.

[26] Almogren, A., Mohiuddin, I., Din, I. U., Al Majed, H., & Guizani, N. (2020). FTM-IoMT: Fuzzy-based Trust Management for Preventing Sybil Attacks in Internet of Medical Things. IEEE Internet of Things Journal.

[27] Mishra, A. K., Tripathy, A. K., Puthal, D., & Yang, L. T. (2018). Analytical model for sybil attack phases in internet of things. IEEE Internet of Things Journal, 6(1), 379-387.

[28] Lao, L., Dai, X., Xiao, B., & Guo, S. (2020, May). G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications. In 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS) (pp. 664-673). IEEE.

[29] Haripriya, A. P., & Kulothungan, K. (2019). Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. EURASIP Journal on Wireless Communications and Networking, 2019(1), 90.

[30] Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2018). REATO: REActing TO Denial of Service attacks in the Internet of Things. Computer Networks, 137, 37-48.

[31] Shurman, M. M., Khrais, R. M., & Yateem, A. A. (2019, December). IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS. In 2019 International Arab Conference on Information Technology (ACIT)(pp.252-254).IEEE.

[32] Rajendran, G., Nivash, R. R., Parthy, P. P., & Balamurugan, S. (2019, October). Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[33] Feng, Y., Wang, W., Weng, Y., & Zhang, H. (2017, July). A replay-attack resistant authentication scheme for the internet of things. In 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (Vol. 1, pp. 541-547). IEEE.

[34] Khan, S., Alzahrani, A. I., Alfarraj, O., Alalwan, N., & Al-Bayatti, A. H. (2019). Resource Efficient Authentication and Session Key Establishment Procedure for Low-Resource IoT Devices. IEEE Access, 7, 170615-170628.

[35] Ghugar, U., & Pradhan, J. (2020). Survey of wormhole attack in wireless sensor networks. Computer Science and Information Technologies, 2(1), 33-42.

[36] Deshmukh-Bhosale, S., & Sonavane, S. S. (2019). A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things. Procedia Manufacturing, 32, 840-847.

[37] Chehida, S., Baouya, A., Bozga, M., & Bensalem, S. (2020, June). Exploration of Impactful Countermeasures on IoT Attacks. In 2020 9th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-4). IEEE.

[38] Chen, Y. W., Sheu, J. P., Kuo, Y. C., & Van Cuong, N. (2020, June). Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning. In 2020 European Conference on Networks and Communications (EuCNC) (pp. 122-127). IEEE

[39] Kajwadkar, S., & Jain, V. K. (2018, October). A Novel Algorithm for DoS and DDoS attack detection in Internet of Things. In 2018 Conference on Information and Communication Technology (CICT) (pp. 1-4). IEEE.

[40] Singh, R., Tanwar, S., & Sharma, T. P. (2020). Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy, 3(3), e96.

[41] Nicula, Ș., & Zota, R. D. (2019). Exploiting stack-based buffer overflow using modern day techniques. Procedia Computer Science, 160, 9-14.

[42] Xu, B., Wang, W., Hao, Q., Zhang, Z., Du, P., Xia, T., ... & Wang, X. (2018). A security design for the detecting of buffer overflow attacks in IoT device. IEEE Access, 6, 72862-72869.

[43] Hamidouche, R., Aliouat, Z., Ari, A. A. A., & Gueroui, M. (2019). An efficient clustering strategy avoiding buffer overflow in IoT sensors: a bio-inspired based approach. IEEE Access, 7, 156733-156751.

[44] Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). Internet of things and the man-in-the-middle attacks–security and economic risks. MEST Journal, 5(2), 15-25.

[45] Kang, J. J., Fahd, K., Venkatraman, S., Trujillo-Rasua, R., & Haskell-Dowland, P. (2019, November). Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks. In 2019 29th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-6). IEEE.

[46] Mustafa, K. A. R. A., & Furat, M. U. R. A. T. (2018). Client-Server Based Authentication Against MITM Attack via Fast Communication for IIoT Devices. Balkan Journal of Electrical and Computer Engineering, 6(2), 88-93.

SARA ALMTRAFI received the B.Sc. degree in Computer Science from Umm Al Qura University, Makkah, Saudi Arabia, in 2018. She is currently pursuing M.Sc. in Cyber Security at Taif University, Taif, Saudi Arabia. Her research interests include the Internet of Things and Cyber Security.

BDOUR ALKHUDADI received the B.Sc. degree in Computer Science from Taif University, Saudi Arabia, in 2019. She is currently a cyber security Master's student, Taif University, Taif, Saudi Arabia. Her research interests include the Internet of Things, and Cyber Security.

GOFRAN SAMI received the B.Sc. degree in Information System, college of Computer Science & Engineering, Taibah University, Saudi Arabia, in 2011. the M.Sc. degree in Information Management and Security from the University of Bedfordshire, United Kingdom in 2015. She is currently a lecturer with Joint First Year Deanship, Umm Al-Qura University, Makkah, Saudi Arabia. Her research interests include human computer interaction, information systems and security, and big data analytics.

WAJDI ALHAKAMI received the B.Sc. degree in Computer Science from Jeddah University, Saudi Arabia, in 2007. the M.Sc. degree in Computer Network, and the Ph.D. degree in Network Security from the University of Bedfordshire, United Kingdom in 2011 and 2016 respectively. He is currently an Assistant Professor with department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia. His research interests include the Internet of Things, Cyber Security, and Computer Networking.