EAI Endorsed Transactions
on Security and Safety

Review Article EAI.EU

A Systemic Security and Privacy Review: Attacks and Prevention Mechanisms over IOT Layers

Muhammad Shoaib Akhtar, Tao Feng*

School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Abstract

In this contemporary era internet of things are used in every realm of life. Recent software's (e.g., vehicle networking, smart grid, and wearable) are established in result of its use: furthermore, as development, consolidation, and revolution of varied ancient areas (e.g., medical and automotive). The number of devices connected in conjunction with the ad-hoc nature of the system any exacerbates the case. Therefore, security and privacy has emerged as a big challenge for the IoT. This paper provides an outline of IoT security attacks on Three-Layer Architecture: Three-layer such as application layer, network layer, perception layer/physical layer and attacks that are associated with these layers will be discussed. Moreover, this paper will provide some possible solution mechanisms for such attacks. The aim is to produce a radical survey associated with the privacy and security challenges of the IoT. This paper addresses these challenges from the attitude of technologies and design used. The objective of this paper is to rendering possible solution for various attacks on different layers of IoT architecture. It also presents comparison based on reviewing multiple solutions and defines the best one solution for a specific attack on particular layer.

Keywords: Internet of Things, Security and Privacy, IoT layers, attacks with solution mechanisms

Received on 22 April 2022, accepted on 03 August 2022, published on 05 August 2022

doi: 10.4108/eetss.v8i30.590

* Corresponding author. Email: fengt@lut.edu.cn

1. Introduction

Internet of things has a combination of various devices; the things which are connected through the internet are sensors and actuators. Our world today contains billions of sensors and electronic devices that constantly track, store, compile and analyze vast amounts of personal information. This information may include our position, browsing habits on the contact list, and details on health and fitness. The Internet of Things plays a major part in the day-to-day life of every individual. It's a service that allows transmissions from person to object or object to object. As IoT is the incorporation of frequent heterogeneous networks so, to establish reliable connection among nodes is challenging. The IoT comprises of sensors, smart devices, networks, cloud computing, all connected by common standards. Every band put susceptibilities and threats to security. Discouragingly, the availability moves towards the cost of safety and protection gambles with that private, exemplify information can present broad mischief to our property, dependability and individual security assuming it is uncovered by unapproved specialist. Such tools also include assets which are provided by their suppliers at different stages with their supply chain of development, in addition to our personalized data. Such modes include fuses, firmware, and debugging. Million dollars of stolen intellectual property will be lost through unauthorized access also it can cause misuse of these resources. Such security vulnerabilities can be disastrous with the widespread implementation of these apps. IoT applications are used in many fields as illustrated in figure 1 such as environmental monitoring, home automation, transportation, health care and medical systems, and so on. In this regard, data ensuring and safety of privacy is the largest challenge. There are some main technologies

of IoT which includes RFID technology, Sensor technology, embedded system technology, and Nanotechnology. Therefore, construction technology is posing main threat.

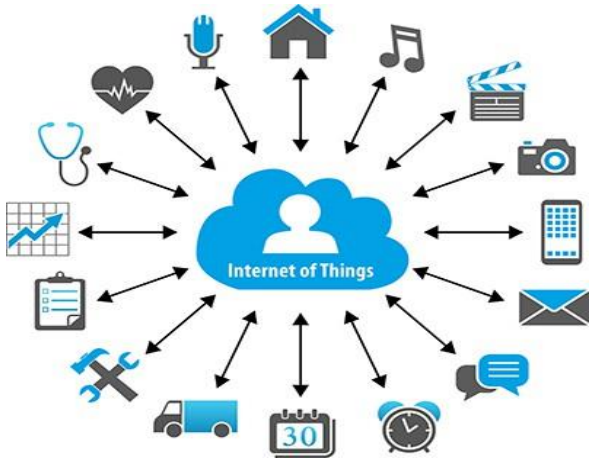

Figure 1. Importance of IoT

1.1 IoT Security Challenges

Due to the extensive consequences on daily life, each and every IoT appliances are susceptible for challenges of security and privacy such as authenticity, confidentiality and integrity. Security problems are split up into various classifications, like confidentiality of data, observing and tracing down the activities, sidestep the malicious insiders, hijacking of services or procedures, phishing, fraudulent activities and exploitation etc. [14] [15]. Information Technology's (IT) security reflects [8-10] reflects three features which includes availability, integrity and confidentiality. These are called as CIA triad, and these are also the key purposes [11]. Data security refers to the confidentiality, although integrity is not changing the data while it is transmitting [12] [13]. Additionally, whenever it is essential to transmit data smoothly, the availability will be helpful. Among multiple security difficulties, the necessary challenges are:

- Data Privacy & Security: Data have to be secured, and hidden so that the data will be safe from stealing and from the hackers, while transmitting data seamlessly.
- Insurance Concerns: Many companies are setting up IoT devices which are helping to gather data to make decision about insurance.
- Technical Concern: Now a day's excessive use of IoT devices generates lot of traffic, so it requires large network and storage capacity.
- Need of Common Standard: Although, there are numerous standards for IoT devices but the most backbreaking factor is to connect the authorized and un-allowed devices.

In IoT, whole security is dependent on Three-layer architecture. If physical layer is in control then it will be easy to get access and attack to other nearby devices with the help of original node. On the other side of spectrum, devices that have online ability can be easily hacked, if device has no virus protection then these devices are used as "bots" to deliver malicious code [10]. Resent survey of HP shows that 70% of IoT devices are not secure. Therefore, one of the major concerns regarding IoT devices are security and privacy because these two things show that communication between devices and internet is reliable. So, this paper presents some threats, attacks and vulnerabilities that are associated with three-layer architecture and provide possible solution regarding these issues. [10]. The main contribution of this paper as follows:

1. This paper presents security survey of IoT layered architecture.
2. Review of many IoT security approaches, to tackle security issues and challenges of individual layer.
3. Complete analysis of the structure and working flow of these techniques and solutions along with their pros and cons.
4. Comparison is made through table that will give proper direction, which technique is best solution of every layer's security and how it is different from others as a result.

1.2 Key Role of Layers in IoT

The following section presents the introduction of Three-Layer architecture. Application layer consists multiple application such as smart energy saving, smart home and smart cities. Network layer is integrated with communication and transferring data accurately which is collected through sensor nodes. Conversely, last tier is physical which contain various hardware technologies like RFID devices, sensor etc.

1.3 Physical Layer/ Perception Layer

In three-layer architecture of IoT, the Physical layer comes in the top bottom layers. Identifying devices provide connectivity and provide service discovery are main responsibilities of physical layer [15]. In IoT manners, Wi-Fi, Bluetooth, ZigBee are physical devices that are used to connected two devices through internet either directly or indirectly. These are used in IoT because of low energy consumption and low power for connectivity furthermore, every device has a tag which has unique identity to connect with other devices. Perception layer is a part of physical layer but there is a bit different between them that perception layer sense data through sensors and collect information to environment. It has many sensors like temperature sensor, vibration sensor, RFID that allow devices to sense other objects.

1.4 Network Layer

As like the physical layer, network layer is answerable for correspondence and availability through various communicational conventions: there is no question that IoT is having not have such conventions and guidelines but rather a few like MQTT and CoAP are being utilized in IoT. The main goal of network layer is to transfer data in between devices [12]. With the help of wireless sensor physical layer send information or data to network layer then it transmits to any particular processing system.

1.5 Application Layer

Application layer consist the services that are provide through IoT. Application layer is known as service-oriented. It stores information or data in his database and retrieve information when user need it for example Smart home, healthcare and smart cities as illustrated in figure 2 below.

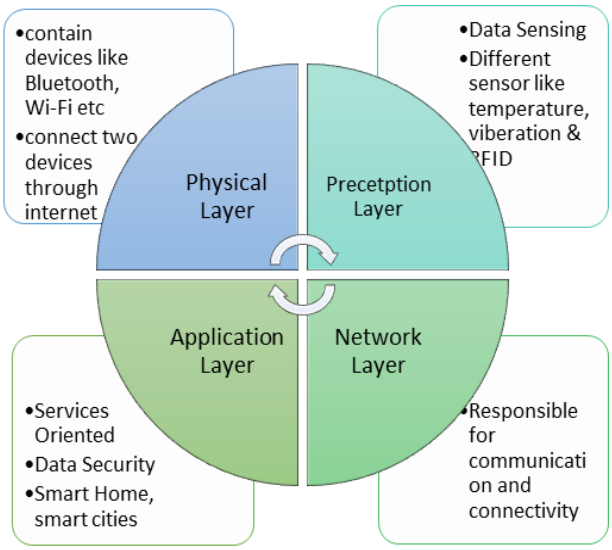

Figure 2. Four-Layer Architecture for IoT

2. Attacks and their Countermeasures on Layer Architecture

2.1 Network Layer

Network layer is liable for the property of the internet of things infrastructure [7–9]. This layer conjointly transfers information to the next upper layer by gathering information from perception layer. For communication the wired or wireless medium is used. Moreover, the foremost technologies which are used are ZigBee, Wi-Fi, Bluetooth, 3G, and so and so forth [9] [10]. Network layer has several attacks, usually moving organization of labor and data sharing between devices [10]. Very much like the other Network Layer model this one incorporates network limits, correspondence channels, and organization. Controlling, information upkeep, and scholarly interaction, and are especially to fault for the correspondence and property of the relative multitude of gadgets in IoT framework through the help of numerous correspondence conventions. The first normal conventions that are as of now being utilized are MQTT three. [9] and furthermore the impacted Application Protocol (CoAP) [10]. It's at breaks this layer that the congregated information from the Physical Layer are sent to a particular data science framework at stretches the organization abuse Wireless Sensors [10] or to an out of entryways network over existing correspondence structures very much like the net or a Mobile Network.

2.2 Network Layer Attacks:

Figure 3 below illustrate different types of attacks which could be done over network layer in IOT Applications.

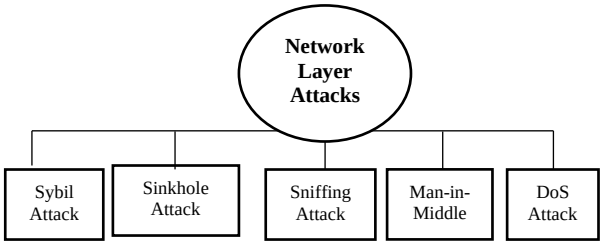

Figure 3. Network Layer Attacks

2.2.1 Sybil Attack

An attack in which an isolated attacker can literally take our network, but the attacker faking it to be bunches of other nodes, it happens in peer to peer network. It is very pragmatic attack because attacker sends a lot of fake requests to network and the network does not really know either request is original or fake. Single user pretends many fake or Sybil (create various account from different IP addresses) identities. In this regard's attacker can completely take over the peer network Sybil attack could affect the performance, resource utilization and data integrity [1].

2.2.2 Countermeasure

Solution for this problem is a trending research area in this decade. Many researchers are doing working on it such as, improving the security nodes in smart grids Golestani et al. [25] has proposed a technique. Similarly, Demirbas et al. [24] have a technique for detection, through RSSI (Received Signal Strength Indicator) value that can get from neighboring nodes. Douceur's approach is also very popular that used as a solution of Sybil attack.

The above-mentioned mechanisms are most expensive for resource constrained devices in respect of storage and processing. As compare to these approaches this paper suggests the best solution for Sybil attack is "behavioral profiling" [1]. With the help of network parameters, they develop a behavioral profile for every node. As a result of these profiling nodes that have less trusted values are rejects, through reliable nodes, packets are routed again.

2.3 Sinkhole Attack

In sinkhole attack the attacker compromise with one network node and treat it as an attacker furthermore, it is absolutely after the steering grid (that convention for the most part utilizes) this assailant hub sends counterfeit data and give its all to entrance entire traffic of other adjoining meeting focuses (called hubs), this occurs in remote sensor network [2]. After managing traffic, it launches a particular attack then all the data packets will pass it before going to base station.

2.3.1 Countermeasure

There are many traditional approaches to overcome this problem but these approaches are categorized such as key management based, rule-based and anomaly based. In Papadimitriou et al [58] where RESIST protocol has been invented the key management approach is used there. Sharmila, S. and Umamaheswari, G. [59] proposed a message digest algorithm for anomaly-based sinkhole detection furthermore, Krontiris et al [27] proposed detection rules for rule-based detection. The above-mentioned techniques are not suitable for IoT low end devices. In contrast of these above EM & RSSI technique is best one solution. To detect sinkhole attack Extra Monitor node (EM) and Received signal strength indicator (RSSI) are being used. The basic functions of EM are: provide high communication range along with calculating the RSSI of node it sends to base station with next hop and source ID. A visual graphical guide (VGM) is likewise utilized in this cycle; RSSI values are utilized by the base station to quantify VGM. The place of the hub can be demonstrated through this VGM. After this recognizable proof when base station beneficiary one more changed esteem from EM since EM send refreshed RSSI esteem then, at that point, base station distinguishes that bundle stream are not matched to past one so it demonstrates there is a sinkhole assault [2].

2.4 Sniffing Attack

It a generic attack, sniffing is basically intercepting traffic between two hosts which has got verity based on mode of attacks. It is usually used to control the traffic and snatch confidential data. LAN network attack is harmful and easy to do. Malicious user can easily steel confidential information because of network traffic sniffing. Two types of sniffing are passive sniffing and active sniffing. Passive sniffing is possible in 'hub' cases while we use hub devices (hub use to broadcast data or message), attack or hacker no need to put extra effort to get traffic from network. If you get access to hub then sniffing performance is so easy. Conversely, active sniffing is used in switch cases, in switches if one computer intends to communicate to other then it will not broadcast the data it will directly connected to 2nd computer. If attacker wants to listen that traffic, then attack will make his land card in promiscuous mode.

2.4.1 Counter Steps

One of the most appropriate techniques is proposed in Namrata Shukla et al. [14] for revealing this attack. According to this method a log file has been created which have content of data separately by frequency, space and position as well. On the other hand, by using the substitution method they encrypt the data then pass to receiver side along with, they send the log file that is organized in a way of cryptic message as well. Conversely, recipient matches data conforming to frequency, position or message, for a sense if it does not match. The error can be observed by them, and they will never approve that file. Several other mechanisms have been proposed like Tag based client-side detection [16], server-side content sniffing attack prevention technique [17].

2.5 Man-in-Middle Attack

In environment of server client, Man-in-middle attack is generally perceived. A game called cup telephonic is used to understand man-in-middle attack, in which two friends can talk to each other through cup in a string. While conversation a third unknown person come and cut the string, put two cups in between string and start listing conversation. This third person intercept the network and possible to alter the communication message. Same happens in this attack, an attacker insert himself in a network or start interrupting the conversation or steel personal information. This attack can be possible where sending and receiving process occurs.

2.5.1 Countermeasures

According to above statements, one major factor is involved in this attack which is authentication. If we have a command in this manner we can resolve this problem. Multiple techniques such as DNS spoofing, Gateway spoofing, DHCP spoofing, IP address spoofing, stealing of port are used in man-in-middle attack. Majority of the mechanisms that are used against this attack are authentication mechanisms like secret question, 2-step authentication, voice recognition, biometric, public key infrastructure etc. Many other modern mechanisms are involved such as: one-time password authentication (time synchronized), MitM detection system [35], multifactor authentication to protect login and software toolbar etc. Furthermore, one of the best countermeasures is

communication with symmetric or asymmetric algorithms such as AES, DES.

2.6 DOS Attack

Denial of service attack is one of the perilous attacks for user in which attacker make device or computer unavailable for its user by sending multiple request, sending wrong password furthermore, by disconnecting host, it degrades the network performance. DOS is used to get unauthorized access along with it help to control the system. Many attacks are including in DOS such as: TCP SYN attack, HTTP flood attack, SIP flood attack, UDP flood attack, slow request/response attack and bandwidth depletion attack.

2.6.1 Countermeasures

Ingress/egress is one of the best approaches which can overcome DOS attack. With the help of spoofed IPs, these techniques prevent traffic. Ingress filtering use to filter the malicious traffic and egress filtering use to discard this malicious traffic to local network. It works like in the event that a client enter network, entrance permit traffic to enter in the network (which coordinate with the predefined scope of space prefix) moreover, in the event that the client use IP parodying (which doesn't coordinate with characterized prefix) departure dispose of this in the switches. [5]. Various other mechanisms are used to prevent this attack like Route based packet filtering, Game Theoretic Approach [31], An Ant Based Framework, Protection using KDS [34], Hop count filtering, path identifier, history-based filtering, honey pots and load balancing etc. The above techniques depend on nod's malicious behavior, routing algorithms, parameter analysis and what parameter has considered for detection of attacks so, due to that factor Ingress/egress is a best one technique.

Table 1. Summary of Network Layer Attacks and its Prevention

Attacks Name	Challenges	Research Comparison	Best Prevention Technique
Sybil Attack	Creating and sending lot of fake requests	Demirbas at el [24]: Sybile detection technique by using RSSI. Sharmila at el [26]: Energy and hop count-based detection Golestani at el [25]: Detection for smart grid by traffic analyzing	Behavior profiling "Develop a behavioral profile for every node"
Sinkhole Attack	Select specific node for attack and reroute data toward it	Krontiries at el 1271: Rule based approach "creating two rules and implemented in IDS" Roy at el [23]: Dynamic trust management system	For sinkhole detection using EM (Extra Monitoring node) & RSSI (Received Single Strength Indicator) technique
Sniffing Attack	Intercepting traffic between two hosts	AnimeshDubey et al. [29]: Propose an efficient partition technique for web based files Op, html, php), text (word, text files) and PDF files. Ahmed Qadri et al. [30]: Tag based client side detection.	Prevention through Log file: log have content of data separately by frequency, space and position as well.
Man in the Middle	Information modification between two parities without their knowledge	B. Aziz at el [35] MitM detection system that uses arrival time of packets to infer the possibility of MitM J. Liu at al [36] use computing resources known as Registration Authority (RA), who is responsible authenticating.	Encrypt communication with either symmetric or asymmetric algorithms e.g AES, DES, RSA, Diffie-Hellman, ECC, etc.
Denial of service (DOS)	Sending huge non-relevant request for making server unavailable for particular user	AfrandAgah at el [31] Game Theoretic Approach Maryam Mohi at el [32] A Bayesian Game Approach. Yi-ying at el [33] Message Observation Mechanism (MoM)	Ingress/egress technique: Ingress filtering use to filter the malicious traffic and egress filtering use to discard this malicious traffic to local network

2.7 Perception Layer

Perception layer is one of the bottom layers which are used for the purpose of information or data collection from WSN, heterogeneous devices; sensors type real world objects, humidity, and temperature etc. Single purpose of perception layer is to identify address. Figure 4 below illustrates various types of attacks possible on this layer.

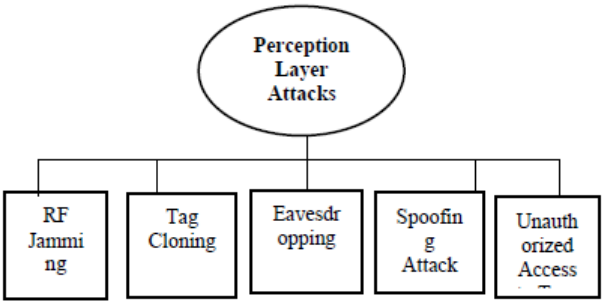

Figure 4. Perception Layer Attacks

2.7.1 RF Jamming

One of the basic attacks in perception layer in which attacker send Radio signals to create interfere between readers and legitimate tags. RFID tags are used to create interruption between communications and prevent radar to communicate all with tags within its range [11].

2.7.1.1 Countermeasures

Solution of RF jamming is dependent on the type of jammer either reactive or proactive. Many researchers are still working on wireless anti-jamming techniques [6] such as Signal strength technique, Regulated Transmitted Power, using of LDPC (Low density Parity Check) codes [59], Ultra-Wide Band Technology and Using Reed-Solomon codes with respect to 802.11b techniques has been proposed for jamming detection. The above mentioned are working in various direction like some are focusing on the designing of physical layer, some are on sensor network and some are on MAC layer. On the other hand, Frequency-Hopping Spread Spectrum is one of the best techniques for RF jamming in which radio signal spread through different switching among many frequency channels.

2.7.2 Tag Cloning

Cloned tag is a duplicate copy of original one. The middle man means the attacker build a tag same like original when the reader read tag it is impossible to him to differentiate between them. With the help of this tag the attacker can sense data, captured information and modify it as he intends.

2.7.2.1 Countermeasures

There are two basic approaches prevention and detection is used to avoid tag cloning. Having encryption and cryptograph technology, prevention method provides security against tag cloning but this technique is not affected for low cost tags [7]. Conversely, detection is used in low cost tags to handle clone tag issues. Several other methods such as: GREAT, BASE and DeCloneare used to overcome tag cloning. But clone detection through EPC is a best approach to prevent tag cloning. In EPC (electronic product code) a specific identity has given to a particular physical object, which may be used to track all king of object. So, the attacker cannot build that specific identity and will not be able to steal your data.

2.7.3 Eavesdropping

Eavesdropping is one of the perilous attacks in perception layer in which the attacker is sitting somewhere in network and can steal information or traffic, through peace of software. The attacker inserts a piece of software in the form of malware or other method to compromised device later on he can easily retrieve data through this piece of software. Due to wireless era, it become very easy to get personal information like password through Eavesdropping

2.7.3.1 Countermeasures

Several RFID private authentication protocols are used to overcome eavesdropping problems. Network division is one of the best approaches for revels eavesdropping. Before establishing connection, every device should be verified so network access control mechanisms are used in this manner. Network segmentation, network monitoring, security technologies like firewall, VPNs and anti-malwares are most important. On the other hand, Anonymous Forward-Secure Mutual Authentication Protocols (AFMAP) and RWP authentication purpose are also effective for this problem [8].

2.7.4 Spoofing Attack

In spoofing, attackers create a fake IP packet which behave like an original one and broadcast in RFID system. It shows like authentic source and create security hole in system furthermore, attacker can get access to network and send malicious data, wrong information to system through this hole.

2.7.4.1 Countermeasures

Several researchers are working on spoofing attack. With the aid of filtering mechanisms (which can filter the outgoing and incoming packets) the spoofing attacks could be defended moreover, Trusted Credential Area (TCA) technique [45], web-spoofing attack, patch method [60] are used. But these approaches have ambiguities: TCA is much costly and web spoofing is not well for hand-held devices as well. So, one of the best approaches is access control list (ACLs) and Secure Scout Layer (SSL) authentication mechanisms that are used to decrease the risk of spoofing attack [13].

2.7.5 Unauthorized Access to Tags Attack

As we can observe it by name that an unauthorized person can access your data. With the increasing rate of technology, the usage of RFID tags is increasing too in commercial and industrial application for quickly, powerful and flexible response. Different types of tags are used to shear information but fake RFID reader fail this authentication mechanisms moreover, he can keep record of personal information from tags and can modify, delete or access this confidential information.

2.7.5.1 Countermeasures

With the help of hash and encryption algorithms YapingZaing [22] proposed protected data exchange protocol which is used to provide privacy and avoid information leakage. Transmission of information, authentication identity and disconnect communication are main three parts of this algorithm. Many other mechanisms such as: sequence encryption mechanisms are used to resolve this issue.

Table 2. Summary of Perception Layer Attacks and its Prevention

Attacks Name	Challenges	Research Comparison	Best Prevention Technique
RF-Jamming	Hurdles to exchange data through frequency jamming	Wood and Stankovic at el [37]: This study posed the issue of jamming detection in the loose context of the utility of the communication channel. J. G. Proakis. At el [38] for jamming resistant focuses on the design of physical layer technologies, such as spread spec turn.	Frequency-Hopping Spread Spectrum technique: "radio signal spread through different switching among many frequency channels"
Tag Cloning	Head off data flow between tags	Bu K., at el [40] GREAT using Aloha-based anti-collision protocol to find irreconcilable collisions. Bu K., at el [41] BASE: ID cardinality and tag cardinality Bu K., at el [41] DeClone using a hybrid design of slotted aloha and tree traversal to determine collisions	EPC (Electronic Product Code) technique: in which a specific identity has given to a particular physical object.
Eavesdropping	Interrupted data during; transmission over HTTP	Nguyen at el [43]: A hybrid prevention method for eavesdropping attack. Li, X at el [42]: a framework that taking account into various channel conditions and antenna models	Anonymous Forward-Secure Mutual Authentication Protocols (AFMAP)
Spoofing Attack	Fake IP packet which behave like an original one and broadcast it.	Herzberg at el. [45] proposed the concept of trusted credential area (TCA) of the browser window Felten at el. [44] an attacker stays between the client and the target site such that all web pages destined to the user's machine are routed toward the attacker's server.	Access control list (ACLs): system or resources are granted to operate Secure Scout Layer (SSL): for secure transmission

2.8. Application Layer

Application layer consist the services that are provide through IoT. Application layer is known as service-oriented. It stores information or data in his database and retrieve information when user need it for example Smart home, healthcare and smart cities. Various types of attacks over this layer are presented in figure 5 below.

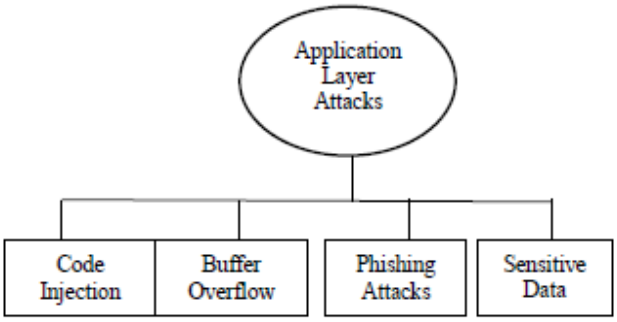

Figure 5. Application Layer Attacks

2.8.1 Code Injection

Code injection is used for several purpose, get personal information or data, to control system and spread worm. HTML script injection and shall injection be common code injections. In this attack Malicious code will be injected in application furthermore, the injected code is able to compromising privacy property, correctness and security and database integrity. It could be used to steal data and provide authentication control [14]. Code injection attacks are used to losing the control on system or even used to completing shutdown.

2.8.1.1 Countermeasures

The best avoidance procedure is WAVES which is known as black-box testing is proposed by Huang and his allies for testing the web application Vulnerabilities with respect to code infusion or SQL. Web crawlers are utilized in these strategies that distinguish the point at where SQL can perform, after that it makes determined focuses, focuses that in light of assault procedures. When attack happened, WAVES then monitor the application's response moreover, it used machine learning techniques to improve and prevent code injection attacks. Several other techniques like, Combined Static and Dynamic Analysis [43], Taint Based Approaches, URL scan, HP SCRAWLR are used to prevent code injection [18].

2.8.2 Buffer Overflow

Memory storage which holds data temporary is called buffer furthermore, it holds data in its transfer time from one location to other. When the data volume exceeds the storage capacity of memory buffer then buffer overflow occurred. The result of buffer overflow may cause the application crashes, memory access error and generate incorrect results. Buffer overflow give permission to attacker to overwrite the memory of application. This change can distract the path, release private information and be responsible for damage files.

2.8.2.1 Countermeasures

Many solutions such as static symbolic execution [48], evolutionary calculation method [49], Data execution prevention, Structured Exception Handler Overwrite Protection (SEHOP) are also used to overcome this predicament. In contract these, one main solution of buffer overflow is Address Space Location Randomization. In this scenario, it arbitrarily hither and thither, according to the data region of specific addresses space locations. Classically, to get the information about the zone of executable code mostly a buffer overflow attack happens, but it can be purposeless by randomizing address spaces.

2.8.3 Phishing Attack

It is very parlous attack for application layer. E-mail and other communication applications are hit list in this manner. In punishing attack, attacker pretends his self like original user forgetting personal information of user like password of credit card details. It is a common type of cyber-attack. Fake E-mails that have send through attacker and designed to lure victim. The message looks like original one and received from trusted sender. If receiver fills the attacker's requirements then attacker can easily get access to your password or other information.

2.8.3.1 Countermeasures

The best prevention technique is the Anti-Phishing Authentication (APA) strategy to identify and forestall real-time phishing attacks. It utilizes 2-way validation and zero-information secret key confirmation. Clients are prescribed to redo their UIs and accordingly guard themselves against parodying [57]. There are many other techniques for preventing phishing attacks such as end-host based anti-phishing algorithm [56], phishing prevention approach based on mutual authentication is provided [54], but these methods are depending on type of data just like in attribute based Anti-phishing provides different kind of checks like URL check, image attribute check. In URL check 'it checks the URL of any page either it is new or not furthermore, for checking the similarity of legitimate page to suspected page image attribute check are used. The only ability of attribute checking technique is to detect unknown phishing attack and new one. Same like this, many other are used such as Identity Based Anti-Phishing Approach, Content Based Anti-Phishing Approach and genetic Algorithm-based Anti-phishing Techniques.

2.8.4 Sensitive Data Permission

This attack refers to manipulate the sensitive data, illegal access and violation user privacy as well. Attacker will get access and will be entered in permission model then they have given permission to attacker to exploiting vulnerabilities in permission model. Now attack have right to control application. In this manner, the privacy of user will be violated because smart devices send data to smart application so, due to the lake of sufficient protection it will not complete securely. Many unauthorized used can get this sensitive data.

2.8.4.1 Countermeasures

Several techniques could be used such as: train your user to avoid clicking unknown and malicious links, many

software tools and spam filter are available in market to prevent E-mail from suspicious person, extensions and ads-on must be enable to prevent users to clinking malicious links and more pivotal is two factor authentications must be applied.

Table 3. Literature Survey of Application Layer Attacks

Attacks Name	Challenges	Research Comparison	Best Prevention Technique
Code Injection	Inject malicious code to application or HTML source	C.Gould at el [48]: JDBC-Checker is a technique for statically checking the type correctness of dynamically-generated SQL Queries R McClure at el & W R Cook at el [49] [50]: New Query Development Paradigms: SQL DOM and Safe Query Objects, use encapsulation of database queries to provide a safe and reliable way to access databases.	Black box testing: Web crawler are used that identify the point at where SQL can perform, WAVES then monitor the application's response.
Buffer Overflow	Overwrite the memory of application	Duraes at el. [51]: proposed an automatic identification method for buffer overflow vulnerability of executable software without source code. Dudina at el. [52]: used static symbolic execution to detect buffer overflow vulnerabilities S Rawat at el. [53]: proposed an evolutionary calculation method for searching for buffer overflow vulnerability	Address Space Location Randomization (ASLR): randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.
Phishing Attack	Using of disguised sources to steal credential information	n Chen at. el [54]: End-host based anti-phishing algorithm Michael Atighetchiat.el [55]: A framework based on attribute based checks for defending against phishing attacks. DmytroIlievat.el. [56]: Phishing prevention approach based on mutual authentication is provided	Anti-Phishing Authentication (APA) technique: It uses 2-way authentication and zero-knowledge password proof

3. Open Issues

This review indicates some attacks and vulnerabilities regarding three tire layered architecture and provide some possible solutions as well. We recommend that other security and privacy concerns should be considered as like middleware layer security in IoT, Mobility first Architecture in IoT, security and privacy in ICN based architecture for IoT and security and privacy regarding mobile IoT. These attacks index is calculated from IoT environments. Conversely, the above recommendation will find more ways in IoT security manners, if these will perform with respect to time and training.

The Internet of Things (IoT) surrounds and links the physical world via physical objects that have vulnerable sensors. In terms of its security objectives, needs, architectural layers, operating principles, vulnerabilities, threats, and assaults on each architectural layer, this article provides a thorough review of IoT systems and suggests potential strategic approaches. Future studies will concentrate on assaults specific to the Internet of Things on the 5G network.

4. Conclusion

IoT technology and things are surging day by day conversely, with this development the only hurdle in Internet of Things progress is security. Privacy of data is another challenge with the development of IoT. Internet of things (IoT) systems specifically concentrate on various security challenges, to design appropriate perception for network's security, and also different security frameworks i.e. system security. The basic concept of this paper is to emphasize the security issues & also their challenges of IoT in different layers, and reflecting the security concern in various layers and their possible corrective measures. It presents every attack at IoT layered architecture, with its working and provides possible solution separately; furthermore, we also discussed other possible solution those can also use to resolve the challenge according to situation and help to boost IoT performance too. It shows the paramount importance of security in developing viable IoT solutions. It also presents clear comparison based on working and characteristics of every solution technique of single layer individually. I hope this article will help you in selecting secure IoT technique for layered architecture in your organization.

References

[1] Muhammad Shoaib Akhtar, Tao Feng, "Deep Learning-Based Framework for the Detection of Cyberattack Using Feature Engineering", Security and Communication Networks, vol. 2021, Article ID 6129210, 12 pages, 2021. https://doi.org/10.1155/2021/6129210

[2] Muhammad Shoaib Akhtar,Tao Feng, Year: 2022, Comparison of Classification Model for the Detection of Cyber-attack using Ensemble Learning Models, SIS, EAI, DOI: 10.4108/eai.1-2-2022.173293

[3] M. Demirbas and Y. Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, pages 564–570. IEEE Computer Society, 2006.

[4] Thakur, B. S., & Chaudhary, S. (2013). Content sniffing attack detection in client and server side: A survey. International Journal of Advanced Computer Research, 3(2), 7.

[5] Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1550147717741463.

[6] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005, May). The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (pp. 46-57).

[7] Muhammad Shoaib Akhtar, Tao Feng Year: 2022 Comparison of Classification Model for the Detection of Cyber-attack using Ensemble Learning Models SIS EAI DOI: 10.4108/eai.1-2-2022.173293.

[8] Nguyen, T. H., &Yoo, M. (2017). A hybrid prevention method for eavesdropping attack by link spoofing in software-defined Internet of Things controllers. International Journal of Distributed Sensor Networks, 13(11), 1550147717739157.

[9] Najafabadi, S. G., Naji, H. R., &Mahani, A. (2013, December). Sybil attack Detection: Improving security of WSNs for smart power grid application. In 2013 Smart Grid Conference (SGC) (pp. 273-278). IEEE.

[10] Çeker, H., Zhuang, J., Upadhyaya, S., La, Q. D., & Soong, B. H. (2016, November). Deception-based game theoretical approach to mitigate DoS attacks. In International conference on decision and game theory for security (pp. 18-38). Springer, Cham.

[11] Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti–jamming techniques in wireless networks: a survey. International Journal of Ad Hoc and Ubiquitous Computing, 17(4), 197-215.

[12] Gao, L., Li, Y., Zhang, L., Lin, F., & Ma, M. (2019). Research on detection and defense mechanisms of DoS attacks based on BP neural network and game theory. IEEE Access, 7, 43018-43030.

[13] Qi, F., Bao, F., Li, T., Jia, W., & Wu, Y. (2006, April). Preventing web-spoofing with automatic detecting security indicator. In International Conference on Information Security Practice and Experience (pp. 112-122). Springer, Berlin, Heidelberg.

[14] Gautam, B., Tripathi, J., & Singh, S. (2018). A Secure Coding Approach For Prevention of SQL Injection Attacks. International Journal of Applied Engineering Research, 13(11), 9874-9880.

[15] Conti, M., Dragoni, N., &Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

[16] Qadri, S. I. A., & Pandey, K. (2012). Tag based client side detection of content sniffing attacks with file encryption and file splitter technique. International Journal of Advanced Computer Research, 2(3), 215.

[17] Barua, A., Shahriar, H., &Zulkernine, M. (2011, November). Server side detection of content sniffing attacks. In 2011 IEEE 22nd International Symposium on Software Reliability Engineering (pp. 20-29). IEEE.

[18] SaiKiran, P., SureshBabu, E., Padmini, D., SriLalitha, V., &Krishnanand, V. (2017). Security issues and countermeasures of three tier architecture of IoT-a survey. International Journal of Pure and Applied Mathematics, 115(6), 49-57.

[19] Iqbal, M. A., Olaleye, O. G., &Bayoumi, M. A. (2017). A review on internet of things (IoT): security and privacy requirements and the solution approaches. Global Journal of Computer Science and Technology.

[20] Farooq MU, Waseem M, Khairi A, Mazhar S (2015) A critical analysis on the security concerns of Internet of Things (IoT). Int J ComputAppl 111:7

[21] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., &Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

[22] Zhang, W., &Qu, B. (2013). Security architecture of the Internet of Things oriented to perceptual layer. International Journal on Computer, Consumer and Control (IJ3C), 2(2), 37-45.

[23] Dubey, A., Gupta, R., &Chandel, G. S. (2013). An efficient partition technique to reduce the attack detection time with web based text and PDF files. International Journal of Advanced Computer Research (IJACR), 3(9), 80-86.

[24] M. Demirbas and Y. Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, pages 564–570. IEEE Computer Society, 2006.

[25] S. G. Najafabadi, H. R. Naji, and A. Mahani. Sybil attack detection: Improving security of wsns for smart power grid application. In Smart Grid Conference (SGC), 2013, pages 273–278. IEEE, 2013.

[26] S. Sharmila and G. Umamaeshwari. Energy and hop based detection of sybil attack for mobile wireless sensor networks. International Journal of Emerging Technology and Advanced Engineering, 4(4), 2014.

[27] Krontiris,I., Dimitriou,T., Giannetsos,T. and Mpasoukos, M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. In Networking and Communications, 2008. WIMOB'08. IEEE Interational Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[28] Roy, D.S., Singh, A.S. and Choudhury, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management. In Computers and Communications, 2008. ISCC 2008. IEE Symposium on (pp. 537-542). IEEE.

[29] AnimeshDubey, Ravindra Gupta, Gajendra Singh Chandel," An Efficient Partition Technique to reduce the Attack Detection Time with Web based Text and PDF files", International Journal of Advanced Computer Research (IJACR),Volume-3 Number-1 Issue-9 March-2013.

[30] Qadri, S. I. A., & Pandey, K. (2012). Tag based client side detection of content sniffing attacks with file encryption and file splitter technique. International Journal of Advanced Computer Research, 2(3), 215.

[31] AfrandAgah, KalyanBasu, and Sajal K Das. Preventing dos attack in sensor networks: a game theoretic approach. In Communications, 2005.ICC 2005. 2005 IEEE International Conference on, volume 5, pages 3218–3222. IEEE, 2005.

[32] Maryam Mohi, Ali Movaghar, and PooyaMoradianZadeh. A bayesian game approach for preventing dos attacks in wireless sensor networks. In Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on, volume 3, pages 507–511. IEEE, 2009.

[33] Yi-ying Zhang, Xiang-zhen Li, and Yuan-an Liu. The detection and defence of dos attack for wireless sensor network. The journal of china universities of posts and telecommunications, 19:52–56, 2012.

[34] Dines Kumar.V.S and Navaneethan.C. Protection against denial of service (dos) attacks in wireless sensor networks. International Journal of Advanced Research in Computer Science & Technology, 2:439–443, March 2014

[35] B. Aziz, G. Hamilton, Detecting man-in-the-middle attacks by precise timing, in: 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 81–86.

[36] J. Liu, Y. Xiao, C. P. Chen, Authentication and access control in the internet of things, in: Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, IEEE, 2012, pp. 588–592.

[37] A. Wood, J. Stankovic, and S. Son. JAM: A jammed-area mapping service for sensor networks. In 24th IEEE Real-Time Systems Symposium, pages 286 - 297, 2003.

[38] J. G. Proakis. Digital Communications. McGraw-Hill, 4th edition, 2000.

[39] C. Schleher. Electronic Warfare in the Information Age. MArtech House, 1999.

[40] Bu K., Liu X., Luo J., Xiao B., and Wei G., ªUnreconciled collisions uncover cloning attacks in anonymous RFID systems,º Inf. Forensics Secur. IEEE Trans., vol. 8, no. 3, pp. 429±439, 2013.

[41] Bu K., Xu M., Liu X., Luo J., Zhang S., and Weng M., ªDeterministic Detection of Cloning Attacks for Anonymous RFID Systems,º IEEE Trans. Ind. Informatics, vol. 11, no. 6, pp. 1±1, 2015.

[42] Li, X., Dai, H. N., & Zhao, Q. (2014, November). An analytical model on eavesdropping attacks in wireless networks. In 2014 IEEE International Conference on Communication Systems (pp. 538-542). IEEE.

[43] Nguyen, T. H., &Yoo, M. (2017). A hybrid prevention method for eavesdropping attack by link spoofing in software-defined Internet of Things controllers. International Journal of Distributed Sensor Networks, 13(11), 1550147717739157.

[44] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Web spoofing: An Internet Con Game. 20th National Information Systems Security Conference, 1997

[45] Amir Herzberg, Ahmad Gbara, TrustBar: Protecting (evenNaive) Web Users from Spoofing and Phishing Attacks. 2004:CryptologyePrint Archive: Report 2004/155

[46] Andre Adelsbach, Sebastian Gajek, and JorgSchwenk. Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures. In Proceedings of Information Security Practice and Experience '2005, LNCS 3469, pp.204-216, 2005.

[47] Gould, C., Su, Z., &Devanbu, P. (2004, May). JDBC checker: A static analysis tool for SQL/JDBC applications. In Proceedings. 26th International Conference on Software Engineering (pp. 697-698). IEEE.

[48] Gould, C., Su, Z., &Devanbu, P. (2004, May). JDBC checker: A static analysis tool for SQL/JDBC applications. In Proceedings. 26th International Conference on Software Engineering (pp. 697-698). IEEE.

[49] McClure, R. A., & Kruger, I. H. (2005, May). SQL DOM: compile time checking of dynamic SQL statements. In Proceedings. 27th International Conference on Software Engineering, 2005. ICSE 2005. (pp. 88-96). IEEE.

[50] Cook, W. R., &Rai, S. (2005, May). Safe query objects: statically typed objects as remotely executable queries. In Proceedings of the 27th international conference on Software engineering (pp. 97-106).

[51] Durães, J., & Madeira, H. (2005, October). A methodology for the automated identification of buffer overflow vulnerabilities in executable software without source-code. In Latin-American Symposium on Dependable Computing (pp. 20-34). Springer, Berlin, Heidelberg.

[52] Dudina, I. A., &Belevantsev, A. A. (2017). Using static symbolic execution to detect buffer overflows. Programming and Computer Software, 43(5), 277-288.

[53] Rawat, S., &Mounier, L. (2010, October). An evolutionary computing approach for hunting buffer overflow vulnerabilities: A case of aiming in dim light. In 2010 European Conference on Computer Network Defense (pp. 37-45). IEEE.

[54] Chen, J., &Guo, C. (2006, October). Online detection and prevention of phishing attacks. In 2006 First International Conference on Communications and Networking in China (pp. 1-7). IEEE.

[55] Atighetchi, M., & Pal, P. (2009, July). Attribute-based prevention of phishing attacks. In 2009 Eighth IEEE

International Symposium on Network Computing and Applications (pp. 266-269). IEEE.

[56] Iliyev, D., & Sun, Y. B. (2010, April). Website forgery prevention. In 2010 International Conference on Information Science and Applications (pp. 1-8). IEEE.