Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

INTERNET OF THINGS SECURITY AND PRIVACY: A LAYER-BASED HIERARCHICAL SURVEY

Zeeshan Qureshi[*1], Dr. Santosh Kumar Banbhrani[2], Dr. Ali Raza Rang[3], Dr. Dhani Bux Talpur[4]

[*1,2,3,4]*University of Sufism and Modern Sciences, Bhitshah*

[*1]zeeshan.qureshi@usms.edu.pk

DOI: https://doi.org/10.5281/zenodo.18138649

Keywords

Article History
Received: 11 August 2025
Accepted: 25 September 2025
Published: 15 October 2025

Corresponding Author: *
Zeeshan Qureshi

Abstract

With the fast development of Internet of Things (IoT), heterogeneous devices have become easily interconnected, thus creating great progress in intelligent applications of smart homes, healthcare, transportation, and industrial automation among others. But the extensive use of IoT systems has also brought about serious security and privacy issues because of its distributed design, device constrained resources, and heterogeneous communication systems. In this paper, one will encounter a systematic hierarchical survey of the security and privacy threats of IoT systems on a four-layer architecture that is composed of application layer, middleware layer, network layer, and the perception layer. Each layer undergoes the systematic analysis of attacks, such as cryptographic, malware injection, denial-of-service, routing and protocol-level, physical tampering, and side-channel attacks. The survey emphasizes the fact that the vulnerabilities on various layers can be exploited to either damage the confidentiality, integrity, availability, and user privacy alone or together. This study will help gain more insight into the current vulnerabilities and assist researchers and practitioners to create well-designed and secure IoT systems because it offers a systematic layer-based classification of the threats of IoT security.

INTRODUCTION

Internet of Things (IoT) has become a fast-growing paradigm that offers the opportunities of interconnecting heterogeneous physical objects via the Internet and enabling them to sense, collect, exchange, and process the data on their own. IoT unites sensing technologies, communication networks and smart data processing to serve a great variety of applications, including smart homes, healthcare systems, industrial control, smart cities and transportation. Nord et al. [1] state that IoT is a change in technology whereby physical objects create, transmit, and use information to facilitate automation and informed decision making, but due to its tremendous advantage, unscrupulous people have posed serious security and privacy threats. IoT devices are usually limited in resource, open to the environment, and they do not have standardized security mechanisms, hence they are prone to cyber threats. Chen et al. [2] point out that the vulnerabilities associated with IoT environments include weak authentication, insecure communication, inadequate encryption, and physical attacks. The weaknesses can be taken advantage of to affect confidentiality, integrity, availability, and user privacy.The IoT systems are usually built on a layered architecture whereby each layer has different roles and is exposed to varying security risks. One of the commonly used models has four layers: the perception layer, which sensitizes the data and handles physical interaction; the network layer,

which makes data flow and route it; the middleware layer, which processes data, stores and gives the services; and the application layer, which delivers services to final users. Weaknesses at one of the layers can spread throughout the IoT ecosystem, expanding the attack surface [3], [4]. Some of these studies have examined the IoT security and privacy concerns in diverse ways. Deogirikar and Vidhate [4] were surveying popular IoT attacks, such as malware injection, denial of service, and equivalent authentication threats. Lipman et al. [5] examined a vast scope of IoT vulnerabilities on communication protocol and device level security. Gupta et al. [6] talked about phishing and social engineering attacks which pose a threat to IoT enabled applications. Routing protocols like RPL are also susceptible to attacks, which are sinkhole, wormhole, Sybil, and rank manipulation attacks as described in [7], [8] and [9]. Even though the available literature can be helpful, numerous scholars concentrate on individual layers or single types of attacks, and their work does not represent the architectural perspective of the IoT security threats. Such a discontinuous view of attacks complicates learning how they travel across the system through several layers and interrelate. Thus, there must be a rigorous and systematic survey of security and privacy threats in the IoT. This paper will provide a layer based hierarchical survey of IoT security and privacy attacks. The paper categorizes attacks systematically based on the four layer IoT architecture which includes application, middleware, network, and perception layer. The purpose behind this structured taxonomy is to assist the researchers and practitioners to know the vulnerabilities of IoT and that of inventing effective solutions to secure IoT. The rest of this paper is structured in the following manner. Section 2 provides the architecture of the IoT, Section 3 explains the taxonomy of the IoT security and privacy attacks, Section 4 covers the research methodology, and the last section ends the paper with the future directions of research. One of the emerging and prevalent technologies today has been internet of things (IOT). IOT has to do with establishing the information of thing [1]. It is a series of physical gadgets that are connected through Internet. The physical equipment is incorporated which communicates with states internally and externally. That is, objects make decisions and communicate in other words sensing. The item can also be defined as industrial robots, goods, smart phones, censors and electrical equipments. [2]. IOT constitutes a mixture of four layer architecture that is depicted in figure1.11. Our study is aimed at analysing the IOT security and privacy issues.

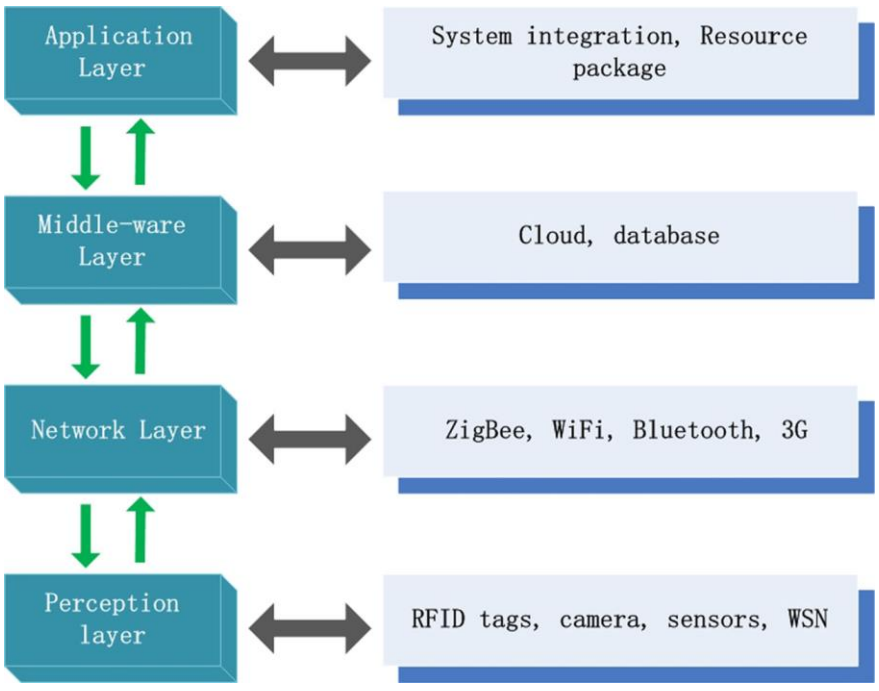

Figure 1.10

Application layer: includes all applications of IOT, that can be smart homes, smart cities, smart health, animal tracking and many more. The layer is responsible to handle and process data through middleware layer also it provides quality of service to the end user.

Middle-ware layer: is application that works as an intermediate between communicating devices of IoT. Middleware creates a bridge between dissimilar, difficult and current programs. It may provide strong and additional storage capability.

Network layer: It provides fundamental connectivity of IOT devices. The data is taken from Lower layer and Resent to Upper layers. The transfer of data can be performed using wired or wireless, ZigBee, WiFi, Bluetooth, 3G are the prominent technologies which are used in this layer.

Perception layer: the layer is responsible for collecting information about the environment, it uses sensors to detect smart objects in surrounding. RFID tags, cameras, sensors, wireless and sensor network (WSN) are the major technologies used in this layer.

IoT attack taxonomy: Criminals motive is to gain access, attackers will always keep attempting different techniques to alter the normal operations of the IOT system and this problem will keep growing. We now put our concern to Exploration of the IoT attacks and its privacy/security problems according to layer wise, based its architecture. Figure 2.11 presented the attack classification [2][3] .

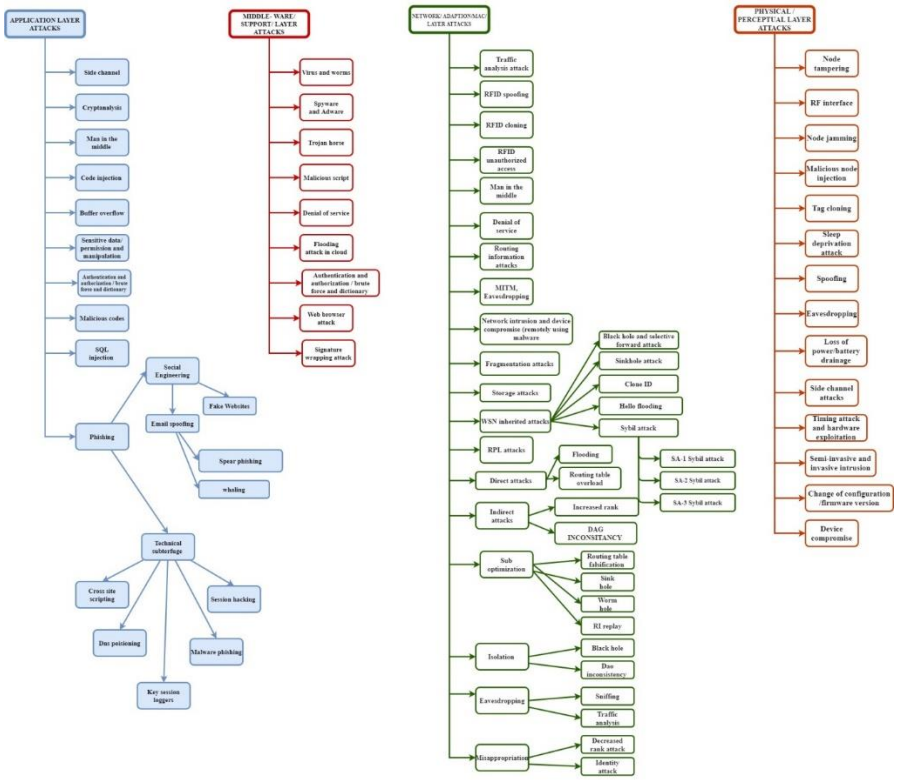

Figure 1.11

IOT security and privacy issues on Application layer:- the diagram 1.12 highlights several security issues in application layer. The major attack in this layer focuses on unauthorized access of confidential data.

The cybercriminal usually exploits the vulnerability of application and program, for example code injection, buffer overflow are techniques also to obtain permission as a legitimate user by faking identity.

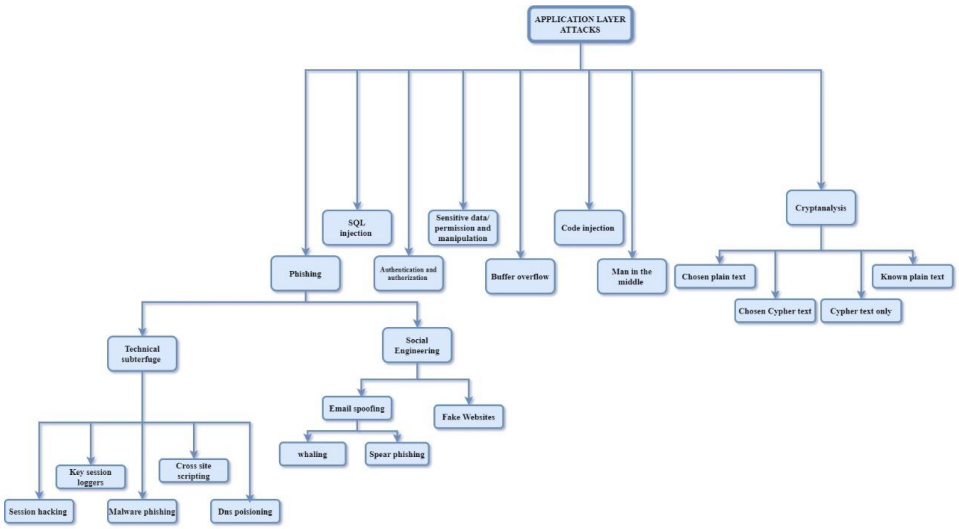

Figure 1.1.2

Cryptanalysis: The technique gets the encryption key through plaintext or cipher text. cryptanalysis attacks has few more types which are listed below.

Cipher text Only Attack: The cybercriminal accesses the cipher text and control the corelated plain text.

Known Plaintext Attack: here attacker knows some parts of the cipher text. The purpose is to decrypt the next part of the cipher text by using known information.

Chosen Plaintext Attack: here he searches for encryption key by using what plaintext is encrypted.

Chosen Cipher text Attack: By selecting the method of plaintext of chosen cipher text by which the encryption key can be found by attacker easily [4].

Man in the middle: Attacker grabs the key while users are communicating and exchanging key[4].

Code injection: Attacker injects malevolent program in the Computer system by creating program errors. The sole purposes is to get data, have system control, and to Spread worms [2].

3.1.4. Buffer overflow: Hacker inserts a large amount of data in a given field, which causes the sequence to overflow beyond the predetermined field of location. The outcome may be altering other data causes the implementation of malicious code and program destruction. Buffer overflows are also one of the most prevalent software and application attacks[2].

Sensitive Data Permission/Manipulation: The cause of attack is a manipulation of the data because of unauthorized access which is a violation of user privacy. It also takes advantage of design weaknesses in permission model. the attackers take advantage of issue that exists in permission model to manipulate applications in smart homes, which leads to issues such as break-in and theft [2].

Authentication and Authorization: The interface of protectiveness of IoT security and privacy. The current authentication systems are unable to do fine-grained verification. One of the issues is excessive privilege that allows the device to view the information without necessarily using all the needed, an attacker can use this susceptibility to develop attacks to different extents, the smart card has a weakness in remote authentication. Also, due to the absence of an ideal authentication system in the smart home, an attacker will be able to carry out unauthorized actions, including opening the door[2].

SQL injection : Malicious code is injected into the paired Android smartphone applications [5].

Phishing Attack: cyberpunk impersonates himself and masquerades as an authority or a trusted user to gain access to sensitive data including passwords and credit card information. This attack is usually done through email where an attacker has been able to obtain sensitive information when the users open the

mail [2]. The phishing attacks can be categorized with respect to the mechanism through which the phisher is capable of accessing personal information of an attack victim. A phisher can defraud any innocent user with the help of spoofed emails, or he can defraud them with the help of the fake websites. Phishing could be divided into 2 attacks. Social Engineering and Technical subterfuge.

Social Engineering:- The attempt is all about grabbing entrance to systems or stealing information, which is related to an individual or a group or organizations, by using user name and Password. The technique uses spoofed e-mails. The phishing attack based on social engineering is divided into two forms, fake websites and spoofed emails.

Fake Websites The technique is considered to be phishing websites, the appearance is same as it is legitimate site visually, The method is to achieve personal information by generating online link which is embedded with phishing emails or via online ads or using crack of licenced software.

Spoofed Emails: It is another type of phishing emails. An untrusted mail server generates emails, or some tricks and techniques are used to make believe that the email is sent by a trusted party also it is about gaining confidence of victim, so that he/she may not hesitate by sharing his/her personal information. Spoofed emails further subdivided into 2 more attacks, spears phishing and whaling.

Spear Phishing: The attacker targets specific person or organization. In 2009, major organizations like yahoo, Symantec and the Giant google has remained victim of malware and spear phishing. This was called an Aurora attacks.

Whaling: This is aimed at high profile workers of large groups in order to overdo highly confidential information. It is also referred to as CEO fraud, here These attacks are even hard to trace because they never involve malware or spoof sites but rather, the hackers employ social engineering to lure users to provide their bank details, employee information among others.

Technical subterfuge: The target is to steal consumers online account in which he tries to get usernames and passwords. Also, Attacker corrupts local navigational infrastructures to misdirect consumers to counterfeit websites." The phishing based on technical subterfuge is further classified based on attacks listed below:

Cross-Site Scripting – The susceptibility occurs when dynamic web page present input without proper validation. A malicious JavaScript is generated in the page that is frequently used by victim side. After this, login credential can be gained easily.

Session Hijacking – The technique is called cookies hijacking. A session key is stolen by using denial-of-service attack. It is used to gain identity which helps to have an access on the unauthorised resources.

Malware Phishing – here malware is used to steal the data of the owner and organization.

DNS Poisoning A fake DNS server is used to trick the client to be trapped, it is done through malicious websites or by installing malware into their systems.

Key/Screen Loggers- Key loggers are very hard to detect, with screen logging software, "virtual keyboards" have no utility at all. It capture the screen snapshots and mouse movements which are sent to the phisher who is at a remote location[6].

IOT security and privacy issues on Middleware layer:-

The layer is responsible for providing services and interface for Upper layer to Application layer. The attack on server and database is very effective which creates hinderance in the operation security and Information security. It aims at virtualization of data. It creates bad quality of service. Figure 1.13 shows hierarchy of security and privacy issue of Middleware layer.

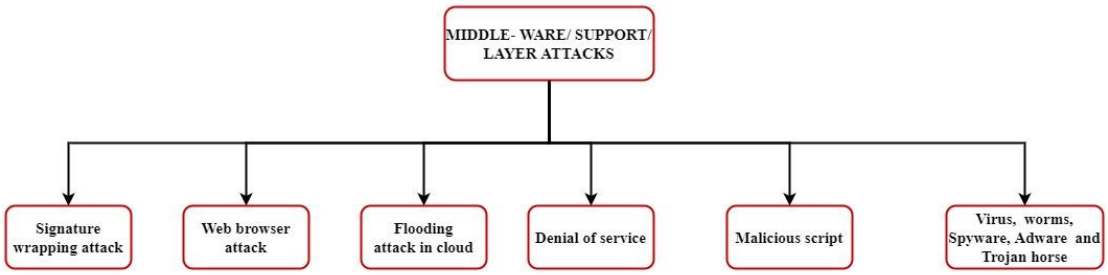

Figure 1.1.3

Virus, Worms, Trojan horse, Spyware and Aware: These are malevolent codes, and are spread via email or downloaded something from internet[4].

Malicious Scripts: it inserts malicious script in the system after which the attacker can gain access[4].

Denial of Service: the user is blocked by attacker from application layer by using denying services[4]

Flooding Attack in Cloud:. A requests is sent by unauthorized person in the cloud, which drain out the resources in the cloud, this attack is used to affects the quality of service.[2]

Web Browser Attack: Web browser is executed to issue commands to remote servers, In the cloud, e.g., authentication and authorization commands But the browser itself does not produce encrypted XML tokens. This weakness is used by attackers to have unauthenticated access. The Web service based cloud service is capable of producing certain metadata which include a huge volume of material about cloud service and service implementation. Having the metadata available to the attackers, they can become a threat to the cloud[2].

Signature Wrapping Attack: XML signature is employed in the cloud system in order to ascertain the integrity of the service. The eavesdropped messages are altered by the attacker without nullifying the signature. SOAP vulnerabilities are used to alter eavesdropped messages by attackers. Moreover, an attacker is able to perform arbitrary actions and tasks as legitimate users[2].

IOT security and privacy issues on Network layer:-

IOT has various networks, Internet and WSN are its part, distinct protocols for distinct networks and devices. Network layer is vulnerable for having various attacks and that can be very destructive, it may cause any network communication down.

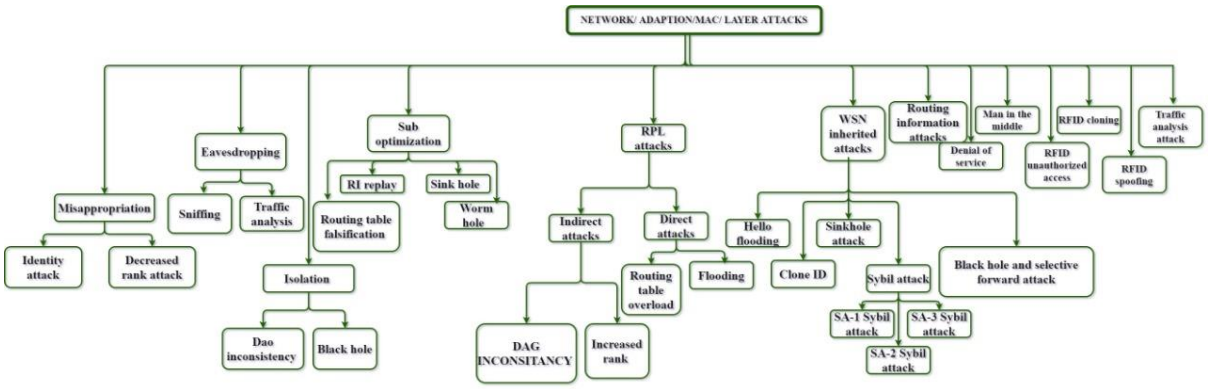

Figure 1.1.4

Traffic analysis attack: This is done by capturing and scanning messages to acquire network information[4]. The pattern and load of communication are determined by analysing the number and the size of the transmitted data packets,

deduced by attackers. This sort of attack may be used in encrypted packets, its pattern of communication can be analysed. Traffic analysis can be used to obtain three types of information in WSN. First, an attacker is able to identify the activity in the network. Second, an attacker is able to acquire the physical position of wireless access points (APs). Lastly, an attacker is able to know the type of information transmitted in the protocol used in the transmission process[2].

RFID Spoofing: The attacker grabs user credentials which is sent via using Radio frequency identification tag. It sends incorrect details and information, which seems to be correct and that the system acknowledges [4].

RFID Cloning: Incorrect data or control is inserted; it is done via cloned node by using adversary copying data by using radio frequency identification tag to another similar tag. It does not duplicate real ID of RFID tag. [4].

RFID Unauthorized Access: If the correct authentication is not provided in the Radio frequency identification systems then the adversary can observe, modify or remove information from any nodes on the network[4].

Man in the middle: The attack is real time and occurs between two communicating victim nodes. The attacker disguises a node as a legitimate node that communicates with two victim[2]. The attacker over the internet intercepts the communication between the two nodes. They obtain the sensitive information by eavesdropping. This type of attack is a real-time attack, occurring between two communicating victim nodes. The attacker disguises a node as a legitimate node that communicates with two victims and also gains the trust of two nodes and obtains information about two victim nodes[4].

Denial of Service: An attacker can send broadcast packet which causes overflows and huge traffic that may lead services unavailable to intended users[4]. In network, a denial-of-service attack (DoS attack) is accomplished by flooding the victim with requests, thereby generating a large amount of network traffic. This type of attack can exhaust all available resources, making network resources unavailable to users. Furthermore, many unencrypted user information can also be leaked [2].

Routing Information Attacks: The attacker spoofs, modify or sends routing information. The outcome will lead allowing or dropping of packets also forwarding incorrect data or segmenting the network[4].

WSN attacks: IoT networks have inherited several WSN routing attacks having small variations in their methods to cope with IoT paradigm.

These attacks are discussed further below.

Blackhole and selective and forward attack: It will simply discard any packets received, rather than forwarding them, like blackhole in the network and result in a Denial of a Service. In a more advanced attack, packets of certain protocols will be sent and rest will be dropped; such as RPL control messages will be forwarded, and all the other packets will be dropped. This is referred to as Selective and Forward attack. The primary distinction between blackhole and selective forward attacks depends on the aim: Blackhole attack is supposed to produce a DoS within the network, whereas that of Selective and Forward is to produce a massive upheaval on routing paths.

Sinkhole Attack: Here, malevolent nodes try to sink as much traffic as possible by advertising a fabricated route with better metrics. This will attract nearby neighbours to send their traffic through the adversaries -By itself, sinkhole attacks are not disruptive, but when they are combined with other types of attacks (e.g., blackhole or wormhole attacks); where the passing traffic can be altered, forged or used for spoofing; the new mixture makes a very powerful attack.

Clone ID: malevolent node(s) gets the identity of another legitimate node.

HELLO Flood Attacks: When any node likes to connect a network, most of the time it starts by broadcasting a "HELLO" message. In RPL, DIO messages are considered as HELLO messages. An attacker can send DIO messages with strong routing metrics and/or strong signal; then it might just disappear or reduce its transmission power to normal This is known as Hello Flood Attack. Another effect of such attack is the exhaustion of legitimate nodes and network congestion due to increased control overhead[7].

Sybil attack: This attack is done through malevolent node stealing several identities from authentic nodes. It is classified into three types:-

SA-1, SA-1 has all nodes unchanged and the malevolent nodes are arranged in one space having strong bonding. The goal of these nodes is to disguise itself and change data so that it can steal the credentials of legitimate nodes on the network.

SA-2, In this type with bonding malevolent nodes are spread among legitimate nodes. The major concern is to disrupt the routing topology.

SA-3, It inherit the functionality of SA-2, the nodes do not keep long relationships with their neighbours. the detection of SA-3 types nodes is harder due to having its capability to be mobile[7][8].

RPL attacks: This attack transforms control messages, they also recognized as alteration and Spoof Attacks.

Direct Attacks, The cyberhacker attacks by flooding packets by using routing tables by keeping storing mode active.

Flooding Attacks: Internal and external attackers are responsible for generating huge amount of traffic in a network and that may cause nodes and links unavailable. The purpose is to drain out the network resources. HELLO flood attack technique is applied.

Routing Table Overload Attacks: In this attack, broadcast or flooding of Dao messages are routed on fake routes to target nodes on the networks. It may cause memory overflow.

Indirect attacks: The malevolent nodes make other nodes to make network overloaded. It is done by combining rank attacks, DAG inconsistency attacks and version number attacks.

Increased Rank Attacks: It voluntarily increases the rank value of a RPL node to create loops in the network.

DAG Inconsistency Attacks: when RPL node finds it inconsistent because of it receives the packet value having Down 'O' bit. If the path of the packet is mismatched the rank relationship, It may lead to a loop in the graph.

Version Number Attacks: The version number is a mandatory field of all DIO message. It is spread without any change down the DODAG graph and is incremented by the root only.

Sub optimization: In this type the network have no converge to the best form.

Routing Table Falsification Attacks: Here, it is possible to imitate or change routing information to advertise falsified routes to other nodes. This attack can be performed in the RPL network by modifying or forging DAO control messages to build fake downward routes. This can only be done when the storing mode is enabled.

Sinkhole Attacks: This attack is performed in two phases. First, falsified data is advertised to attract no of users on the network. Secondly, getting the traffic in an illegitimate manner, it modifies or drops it.

Wormhole Attacks: It is also classified as a set of RPL attacker nodes, here, this type of attack alters the routing path and channels routing information to alternative part of the network, nodes which are vague, they ensure each other as if they are in the similar neighbourhood. It results, non-optimized routes of the nodes on the network.

Routing Information Replay Attacks: The target is to archives valid control messages from other nodes and send them later in the network. The attack is destructive, if it is a dynamic network, also topology and the routing paths often altered.

Worst Parent Attacks. The result is that the given path is not optimized due to deficient performance by choosing systematically the worst chosen parent conferring to the objective function.

Isolation attacks: The objective is to keep the nodes separate from each other so that they must not have their connectivity with root nodes.

Black hole Attacks: Here, packets are dropped that are supposed to be sent on the network. If joined with a sinkhole attack can be very destructive and can create the loss of a large part of the traffic. It can be observed as a type of denial-of-service attack.

DAO Inconsistency Attacks: the route is no longer valid in the routing table of the child due to; a node has a downward route that was before known from a DAO message.

Eavesdropping attacks: Here, the malevolent nodes perform eavesdropping activities like, sniffing and examining the traffic of the network.

Sniffing Attacks This attack is vulnerable for wired and wireless networks. The attacker directly capture the packets from the shared medium.

Traffic Analysis Attacks:- This attack use the features and patterns of the traffic on a link, routing information can be gained.

Misappropriation Attacks. It allows the hacker to gain knowledge about network and its topology to intercept a large part of the traffic.

Decreased Rank Attacks: It causes malevolent node illegitimately to advertise a lower rank value, it over claims its performance.

Identity Attacks it's a combination of spoofing and sybil attacks. combining both may cause Cloning ID's; here the nodes pretends that they are legitimate. The objective is to sniff the network traffic to detect the root node. If hacker succeeds, he spoofs the address of the DODAG root and get the control on the network [9].

IOT security and privacy issues on Perception layer:-

Perception layer uses sensor technology and ad hoc network technology is used by sensors to dynamically modify the network topology plus They use wireless communication due to the variety of deployment environment, the attacker can easily access the connected features of the device via physical attacks.

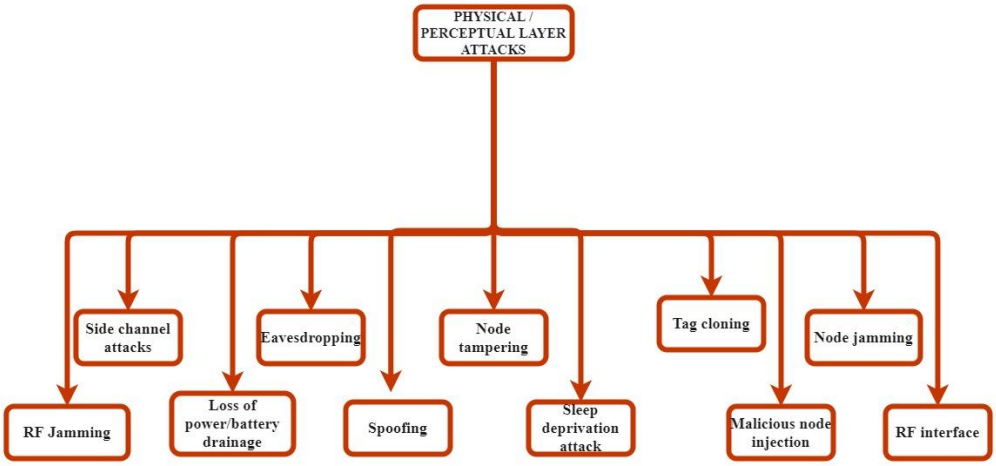

Figure 1.1.5

Node Tampering: A physically change is done, the sole purpose is to gain sensitive information such as encryption key[4]

RF Interference on RFIDs: In this method Dos attack is carried by transferring noise signals via radio frequency signals [4]

Node Jamming: It is about disturbing the wireless communication by using Denial of service attack and technique[4]

Malicious Node Injection: Here the process of injecting malevolent node between two or more nodes is performed, Data is altered and circulated to other nodes[4].

Tag Cloning: Here RFID tags are cloned, relevant information is obtained by using reverse engineering[2].

Sleep Deprivation Attack : Here Hacker consume more power that causes nodes shut down[4] The devices in this layer have some limitations due to less power of the battery [2].

Spoofing Attack: The attacks may cause packet loss during transmission process. It also accelerates the utilization of node power, it may cause diminishing the node lifetime on the network.[2]

Eavesdropping: Antennas are used with the help of RFID to record information [2].

Side-Channel Attacks. Here plaintext or cipher text messages are used, it is about processing time or power utilization of the computers for

encrypting/decrypting data, also for computation of security channels [5].

RF Jamming: Here RFID tags are used to attack all the signals within its range [2].

Methodology

The study adheres to the systematic survey design in order to explore the security and privacy concerns of

Internet of Things (IoT) systems. The methodology aims to systematically identify, categorize and examine the IoT attacks through a layer based architecture approach. The research is based on the available academic studies and not on the experimental application.

The relevant literature was gathered in the academic databases with high quality, such as IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library and Google Scholar. The keywords used in the search process include Internet of Things, IoT security, IoT privacy, IoT vulnerability, IoT attack taxonomy and layer based IoT architecture. The articles that were peer-reviewed and published in the last five years (2014-2021) were taken into account to provide the foundational coverage and the recent coverage.

The gathered papers were filtered out by relevance, technical and clarity in explaining the threats on the IoT security. Articles that were not about the IoT or even those that were not technical enough were filtered out. Based on the chosen studies, crucial data was obtained such as the type of attack, the layer of the IoT affected, the purposes of an attack, and the security property, which was impacted, such as confidentiality, integrity, availability, and privacy.

The classification framework was a four-layer IoT architecture model that includes the application, middleware, network and perception layers. The mapping of attacks was performed systematically against the layer to which they were associated, and eventually, hierarchical taxonomy of IoT security and privacy threats was achieved. To be accurate and reliable, cross-checking of the identified attacks and their classification was done with several authoritative sources.

Such an approach allows gaining systematic and in-depth insight into the issues of IoT security and creates a reliable background that will be used in future studies and development of secure IoT systems.

Results

The paper offers a holistic hierarchical risk assessment of security and privacy threats in Internet of Things systems on a 4 layer architecture platform. Through the systematic review and categorization of the available literature, the findings show that the IoT environments are subject to a large number of attacks across all architectural layers, with different potential effects on confidentiality, integrity, availability, and user privacy.

The analysis indicates that the application layer is very susceptible to attempts to attack it in the context of unauthorized access, manipulation of data and impersonation of a user. Some of the attacks that are often reported in the literature include code injection, buffer overflow, phishing, cryptanalysis, and authentication failures. Such attacks are mostly aimed at sensitive user information and application level services and they usually abuse the ineffective access control mechanisms and the weaknesses in the realization of software. Findings reveal that vulnerabilities of application layer are very serious privacy issues especially in smart home, healthcare, and cloud connected IoT applications.

At the middleware level, the outcomes indicate that there are serious threats associated with service quality and data security. At this layer, malware based attacks, denial of service, flooding attacks in a cloud environment, and running of malicious scripts are the common ones. The results indicate that middleware is a sensitive attack surface because it facilitates data aggregation, processing as well as virtualization. Breach of this layer may worsen the quality of service and allow attackers to modify or manipulate large amounts of IoT data.

The network layer is considered to be one of the most targeted layers since it is involved in communication and routing. The findings have shown that routing attacks, network denial of service, traffic analysis, man in middle attacks, and protocol specific attacks like RPL based attack are common. Spoofing, cloning, sinkhole, wormhole, Sybil, and rank manipulation are especially susceptible to wireless sensor networks and RFID based type of communication. These attacks may destroy network topology, isolate nodes and cause large scale service failures.

Under the perception layer which consists of sensors, RFID tags and physical devices, the findings show that it is highly vulnerable to physical and energy based attacks. The most common attacks are node tampering, malicious node injection, sleep deprivation, jamming, spoofing, and eavesdropping attacks. The devices in this layer have low power,

memory, and processing power, so their security facilities are not very strong, and hence are easily targeted by attackers who have access to the physical device.

In general, the findings show that the threat of IoT security is not centralized and is scattered throughout the architecture. The taxonomy hierarchy built in this paper also illustrates the interdependence of the layers in the way a vulnerability in the underlying layers can be compounded by serious attacks at the higher levels. These studies highlight the importance of combination and layer conscious security solutions instead of independent countermeasures.

Conclusion

This paper gives a systematic hierarchical survey of security and privacy threats in the Internet of Things systems based on a four layer architecture perception, network, middleware, and application layers. The analysis shows that IoT systems are vulnerable to various attacks at all layers with the physical and energy based threats at the perception layer to the unauthorized access, phishing, and manipulation of data at the application layer. Routing, denial of service, malware and protocol based attacks are known to have a high susceptibility in network and middleware layers and can result in compromised service availability, integrity of data and the functioning of systems in general.

The outcomes of this paper point out that the security of IoT is multi layer in nature, and the vulnerability in a given layer can spread and increase the threat in another layer. This highlights the necessity of coming up with integrated and layer conscious security mechanisms that consider the special attributes and constraints of every layer and provide cross layer resiliency.

The hierarchical taxonomy that was created in this survey gives an organized picture of the vulnerabilities of the IoT that can be used as a guide by the various researchers, developers, and practitioners who would like to improve the security of the IoT. It can be used in the future to develop strong security models, lightweight authentication models, intrusion detection models, and privacy preserving models, which are highly customized to the limitations of the IoT devices and networks. Besides, new technologies, like artificial intelligence, blockchain, and edge computing, can be used as an opportunity to detect and mitigate threats and respond to them within IoT settings.

REFERENCES:-

[1] J. Nord, A. Koohang, J. P.-E. S. with Applications, and undefined 2019, "The Internet of Things: Review and theoretical framework," *Elsevier*, Accessed: Dec. 23, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417419303331.

[2] K. Chen *et al.*, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," *J. Hardw. Syst. Secur.*, vol. 2, no. 2, pp. 97–110, Jun. 2018, doi: 10.1007/s41635-017-0029-7.

[3] M. K. Kagita, N. Thilakarathne, S. Dharmendra, D. Rajput, and S. Lanka, "A Detail Study of Security and Privacy issues of Internet of Things," 2020.

[4] J. Deogirikar and A. Vidhate, "Security Attacks inIoT: A Survey," in *ieeexplore.ieee.org*, 2017, pp. 32–37, Accessed: Jan. 06, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8058363/.

[5] J. Lipman, R. Ping Liu, W. Ni, I. Makhdoom, and M. Abolhasan, "Anatomy of Threats to The Internet of Things," *ieeexplore.ieee.org*, vol. 21, no. 2, pp. 1636–1675, 2018, doi: 10.1109/COMST.2018.2874978.

[6] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, Feb. 2018, doi: 10.1007/s11235-017-0334-z.

[7] A. Raoof, A. Matrawy, C. L.-I. C. Surveys, and U. 2018, "Routing attacks and mitigation methods for RPL-based Internet of Things," *ieeexplore.ieee.org*, vol. 21, no. 2, pp. 1582–1606, 2018, Accessed: Jan. 06, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8570741/.

[8] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil Attacks and Their Defenses in the Internet of

Things," *IEEE INTERNET THINGS J.*, vol. 1, no. 5, 2014, doi: 10.1109/JIOT.2014.2344013.

[9] A. Mayzaud, R. Badonnel, and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," 2016. Accessed: Jan. 06, 2021. [Online]. Available: https://hal.inria.fr/hal-01207859.