ISSN 2047-3338

Analysis of Attacks on Internet of Things and their Countermeasures

Shahab Safdar, Muhammad Faizan Gulzar

Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan

Abstract**-- Internet of things provides integration between different sensors and objects for communication without any human intervention. With the time there is an increasing demand for IoT and its various applications, combined with the need to achieve foolproof security requirements. IoT provides a vast amount of data under several constraints that make IoT vulnerable to various security attacks. This paper presents overview of IoT, its architecture, technologies, security challenges and goals. The anatomy of related and current IoT security attacks for different layers of IoT is presented and discussed. A vision for possible security solutions and future research directions is presented.**

Index Terms**—IoT, Blockchain, Security, Privacy, Attacks, Bitcoin, Threats, RSA and Ledger**

I. INTRODUCTION

INTERNET of things refers to a universe of organized and networked smart objects which has an advanced component is interconnected. IoT empowers the interconnectivity of billions of gadgets to help figuring and interchanges. Computerized substances such as sensors, Radio-Frequency Identification (RFID), web furthermore, restriction innovation make it conceivable to change ordinary articles into shrewd items which are able to do deciphering and connecting with one another. The implanted sensors in savvy objects screen, sense, and gather various types of information about gear, climate, and human public activity. In spite of the handiness of IoT, there is a main pressing issue of safety defenselessness.

The associations between people, gadgets, sensors and administrations are all inclusive furthermore, ceaseless. Regardless of how very much planned, insightfully designed, effectively carried out and appropriately kept up with a security framework is, it should depend on human intercession what's more, isn't resistant to security dangers. Along these lines, human component is expected in planning network safety arrangements. Although innovative advancements have additionally improved security arrangements and made them completely safeguarded in quite a large number of cases, there is as yet a continuous requirement for security arrangements to advance and create to defeat new security challenges. In contrast to ordinary Internet Technology (IT) foundation, IoT gadgets are processor, memory, and power constrained, and they are typically conveyed in antagonistic, dynamic and heterogeneous conditions. In correlation with traditional IT foundations, IoT includes possibly various kinds of gadgets and organizations. The primary objective of IoT is to offer coordination among programming, sensors, interoperable correspondence conventions, network foundations, and actual articles. The implanted gadgets offer countless computerized administrations that help day to day human exercises. Along these lines, we can undoubtedly control, work gadgets, and offer information from significant distances in real time.

In any case, the fast and enormous scope organization of IoT gadgets represents a critical security concern. The validation, approval, framework design, check, access control, data capacity and the executives check, to give some examples, are the principal security challenges in the IoT domain. Fundamental data might spill or be altered whenever. The security of IoT gadgets, the data they contain furthermore, clients' protection are not ensured. To support more extensive arrangement of IoT, vigorous security is fundamental to give clients a feeling of security of their own data. Several studies on IoT security weaknesses and difficulties have been distributed between the long stretches of 2012 to 2020. Be that as it may, these studies have not taken into thought current assault classes, for example, complex assaults and other security challenges with IoT as far as their qualities and varieties.

Many investigations just gave the scientific classification of assaults, while others zeroed in just on explicit kinds of safety countermeasures for getting IoT. Apparently, no other concentrate on IoT security was done to join learning based, encryption and autonomic security countermeasures completely.

II. IOT OVERVIEW AND ARCHITECTURE

A. *Overview*

IoT empowers the interconnectivity of a few heterogeneous gadgets and organizations utilizing different correspondence advancements. As indicated by, correspondence may happen between machine-to-machine (M2M) or thing-to-thing (T2T), human-to-thing (H2T) or human-to-human (H2H) through various method for availability. IoT means to give shrewd and progressed administrations to its clients through data networks framed by reliable incorporation of actual items (e.g., PCs, cell phones, wearable gadgets, clothes washers, ice chest, lights, microwave, furthermore, prescriptions). The articles are interconnected or associated to the web or people and are fit for communicating ongoing data about patients, property, traffic, and power. These brilliant articles are likewise equipped for conveying the gathered lightweight information all over the planet. Gadgets outfitted with actuators can remove information, process them and support the correspondence effectiveness among brilliant articles.

IoT is appropriated and heterogeneous, and along these lines, the issues connected with security should be given impressive consideration. In any case, IoT is not the same as customary IT in a few settings, including security. IoT additionally varies in wording of innovation and sending. IoT gadgets are associated under the limitations of low power and lossy organizations (LLNs), which are frail in energy, memory and handling abilities. Not at all like commonplace IT framework, IoT is internationally associated through compacted Internet Protocol Version 6 (IPv6).

Fig. 1 presents security attack scenarios of some key IoT applications. IoT applications are deployed in almost every aspect of our daily lives, including homes, hospitals and industries. Multiple sensors in an application area (e.g., smart home, smart hospital, smart industry and smart transportation) communicate with each other and transmit vital information. Considering a scenario where a driver uses a global positioning system (GPS) to navigate a destination in order to catch up with an urgent meeting; the car's GPS device will usually be connected to multiple devices and utilizes different networks, which are exposed to cyberattacks. An attacker can potentially bypass the firewall and may launch a denial-of-service (DoS) attack, making the navigation service unavailable or send a wrong signal that misleads the driver.

In another scenario based on the same figure, remote operation of the smart home appliances exposes private data to an attacker, or the smart lock of the home could be broken to gain access to home appliances. In one more situation in light of Fig. 1, patients seek treatment and prescription at home or by the medical care administration supplier from a far-off medical clinic. Nonetheless, the patient's touchy data might be in danger of being taken or controlled by the trespasser who sidesteps the emergency clinic firewall, sitting either at the neighborhood organization or on the cloud web. The featured situations present issues that are connected with hacking, psychological warfare, and damage, which might actually influence huge scope astute IoT frameworks like power, clinics, workplaces, businesses and structures.

B. Architecture

Given the ceaseless turn of events and extension, IoT requires a general and versatile design that suits its heterogeneity and the different extent of its application. Right now, there is no generally taken on design. A few scientists have proposed various models for IoT. The three-layered engineering diagrams the basic idea of IoT. Fig. 2 presents an ordinary design of IoT, which is isolated into three essential layers along with their functionalities. The layers are introduced and talked about next.

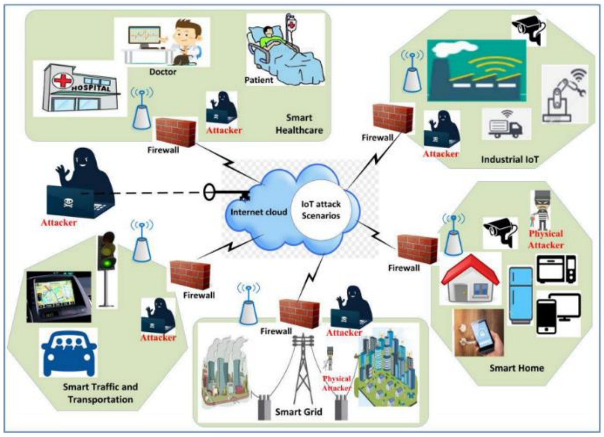

Fig. 1. IoT Security Attack Scenarios in Different Application Areas

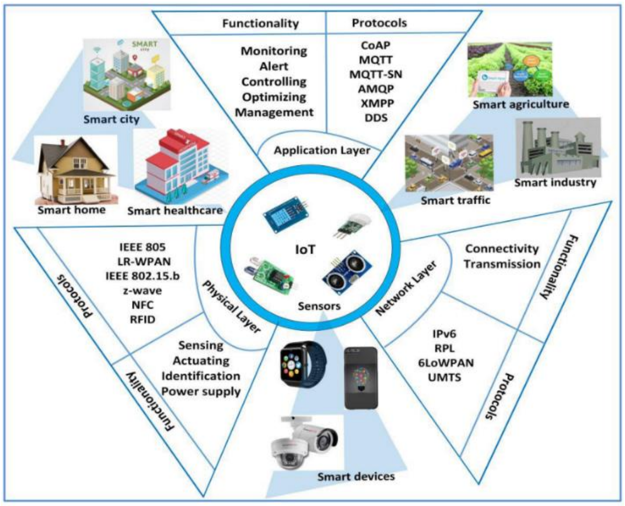

Fig. 2. An overview of IOT, architecture, functionalities

1) APPLICATION LAYER

This layer consists of smart IoT application solutions. The IoT market has colossal possibilities that draw in the improvement of brilliant applications assaults like Spoofing, Message Forging, Virus and Worms among others.

2) NETWORK LAYER

This IoT layer comprised of programming, conventions, and advances that empower object-to-endlessly object to-web network. It is primarily framed utilizing either nearby region organization, for example, remote and wired network, individual region organization close to handle correspondence (NFC), Bluetooth and wide region organizations like GSM, LTE, 5G, and distributed computing. The varieties of the IoT correspondence model have been laid out, as M2M interchanges, machine-to-entry way model, machine-to-cloud correspondences, and back-end information sharing model. The primary capacity of this layer is to send assembled information as a computerized signal, which is gathered from the actual layer of comparing stages through an associated network. This layer is helpless against various security dangers and assaults. Normal assaults in this layer incorporate Denial-of-Service (DoS), Sinkhole, Hello Flood, Blackhole, to give some examples. It is fundamental for the organization layer to have correspondence security for secure information transmission over a public organization.

3) PHYSICAL LAYER

The base layer of IoT engineering is known as the physical layer. In IoT, this layer is additionally alluded to as the insight layer. It incorporates actual world items and virtual substances. The fundamental errand of this layer is to gather information from the climate through different sensors. IoT gadgets are installed with electrical and mechanical equipment parts, for example, sensors, radio wires, actuators, processors. Cell phones, RFID innovation, wearable gadgets are fit for handling, recognizing, associating, conveying and putting away information. In the insight layer, the sensors or RFID convert the gathered crude information of the actual articles to the intelligible advanced signals. IoT objects sense and accumulates information from the actual world like temperature, stickiness, nearness, to give some examples. Be that as it may, this layer of IoT is inclined to a great deal of safety attacks like Jamming, Tampering, Collusion.

III. IOT SECURITY CHALLENGES, GOALS AND METHODS OF ATTACKS

Utilizing the traditional and existing security draws near straightforwardly in the asset compelled IoT gadgets isn't direct. To put it plainly, the security draws near, models also, models of the customary organization are planned in light of the clients' point of view, which may not forever be appropriate for M2M correspondence. The security dangers or assaults might be comparative for the two organizations, yet the arrangement procedures and approaches are different in each organization. The significant security challenges, security objectives and the techniques of safety assaults are presented next.

A. Security Challenges

This segment gives the security challenges while executing security in IoT for application, organization and physical layers.

1) Application Layer Challenges

Heavyweight programming or security arrangements may not be suitable for IoT gadgets. Accordingly, it merits considering the accompanying constraints prior to carrying out security modules in IoT gadgets.

- *Embedded Software*

Either a lightweight General Purpose running gadget (GPOS) or real-Time OS (RTOS) is embedded in low reminiscence IoT devices. Those IoT operating systems are geared up with tiny community protocol stacks, which may not come with adequate protection modules. Hence, lightweight, robust, and fault-tolerant safety modules ought to be designed for such skinny software and protocol stacks

- *Security Patch*

The deployment of IoT devices is probably in a faraway area. The sensing gadgets won't acquire Safety patches or software updates without affecting functional protection. A excessive price might also incur to update a safety patch. Mitigating capacity protection troubles would not be feasible remotely as IoT OS and protocol stack won't be able to get hold of and incorporate a new security patch.

- *Device and Data Volume*

A large wide variety of applications generate an sizeable extent of information which effect the safety and privateness at the records and devices. A report shows that less than 10,000 family gadgets are capable of generating a hundred and fifty million discrete data points in keeping with day.

2) Network Layer Challenges

IoT network layer gives functionalities, for example, correspondence and information steering among various gadgets across the web and inside 6LoWPAN organizations. However, IoT network layer is limited to some routing attacks due to following barriers.

- *Topological Changes and Mobility*

IoT gadgets are cell in many instances, and mobility is one of the primary features of IoT. IoT devices can also go away or join a network from anywhere at any time. The traditional safety algorithm won't be suitable for such dynamic topological modifications.

- *Scalability*

An increasing wide variety of latest, dynamic IoT gadgets are each day springing into life, and more gadgets are being connected to the worldwide network. Current protection schemes and their properties aren't scalable and appropriate for such growing variety of IoT devices.

- *Diverse Communication Medium*

Smart gadgets hook up with non-public, public, international, and local networks through a range of stressed out and wireless conversation mediums. Such numerous houses of wired and wireless hyperlinks make it complicated to increase a complete protection scheme.

- *Multi-Protocol Networking*

IoT devices might use IP or non-IP or aggregate of each network protocols on the same time for communication. It is difficult to make a traditional safety algorithm appropriate for IoT devices considering multiple verbal exchange protocols.

3) Physical Layer Challenges

The IP-associated IoT heterogeneous gadgets are for the most part asset compelled, which makes it more inclined to security dangers and assaults. Nonetheless, the current heavyweight security arrangements are not reasonable to execute in IoT gadgets due to the accompanying attributes.

- *Processor, Memory, and Power*

The battery-pushed IoT devices are strength inefficient, and due to the restrained power, the processor/CPUs have exceptionally low clock cycle. Therefore, devices aren't computationally powerful. Heavy cryptographic algorithms cannot be implemented in such devices. Restrained RAM and flash reminiscence are embedded in an IoT device. Therefore, memory-green safety schemes ought to be ported. The device may additionally run out of memory after booting up the running gadget if the heavyweight protection schemes designed for the conventional community are carried out in IoT.

- *Packaging*

A number of the IoT packages may call for placements in faraway places, which may additionally remain unattended. An adversary may additionally seize and tamper with the IoT gadgets. Cryptographic facts can also then be extracted to alter the programs or to update the gadgets with malicious nodes. Consequently, the tamper resistant packaging of such IoT gadgets is required to overcome this problem.

B. Security Goals

The security objective/need of IoT is talked about in this segment. The conventional and normal security objectives incorporate Confidentiality, Integrity, and Availability (CIA). In any case, separated from this CIA set of three, different necessities like security, lightweight arrangements, genuineness, and normalized approaches have become vital.
To achieve a secure communication for IoT, the following security principles should be considered.

1) Lightweight Solutions

Lightweight safety solutions may be delivered as a completely unique feature when you consider that IoT gadgets are taken into consideration computationally less effective and embedded with restrained memory. The Light-weight technique should be taken into consideration as a protection requirement even as designing, developing and enforcing an encryption or authentication protocols for IoT.

For example, RFID tags in e-passport can suffer from Un-traceability assaults; consequently, lightweight yet robust protection solutions have to be designed for such ultralight protocols. As the safety algorithms or protocols are supposed to be run on IoT devices, those ought to be well suited with the tool's constrained abilities.

2) Authenticity

By using addressing the limitations of IoT, it is crucial to verify and validate the customers worried in conversation. A comprehensive assessment of authentication mechanisms has been presented in. A light-weight authentication mechanism is proposed currently for useful resource-confined devices. RFID tags and NFC are few examples of such superior improvements, which IoT gadgets may additionally gain from as an authentication scheme. An NFC based totally authentication mechanism has been proposed to make sure that energy and processors aren't in use at end nodes. Other than these, accept as true with control, facts, device, and user authentication are also essential.

3) Confidentiality

Confidentiality is one of the key features for securing IoT. All records ought to be blanketed from unauthorized nodes for the duration of any transmission. This will be completed by means of using a shared key, wherein both sender and receiver use this key to encrypt and decrypt data.

4) Integrity

Data integrity guarantees that the statistics stays unchanged during transmission. A symmetric cryptographic algorithm is commonly used to help data beneath transmission through developing signatures for them. Another technique, specifically, Message Integrity check (MIC), is used to verify the integrity of obtained statistics. An autonomic security solution may additionally provide an acceptable degree of information integrity for IoT no matter inadequate sources.

5) Availability

Availability ensures that the entire machine, its components, practical properties, and required services are available at any time. The provision of these offerings and additives may be hampered because of safety assaults. Such assaults may physically damage IoT nodes and networks. The connected things must be available and purposeful on every occasion they're required.

C. IoT and its Methods of Security Attack

Confidentiality is one of the key features for securing IoT. All data need to be blanketed from unauthorized nodes all through any transmission. This will be carried out by means of the use of a shared key, where both sender and receiver use this key to encrypt and decrypt statistics.

1) Device Property

IoT devices are heterogeneous. Therefore, an invader can also assault IoT gadgets based on tool homes. Two such methods are:

- *Low-End Device Attack*

Gadgets with low reminiscence, strength and computational capabilities are taken into consideration as low-stop devices. The attacker uses such devices to release attacks on other IoT gadgets.

- *High-End Device Attack*

A high-end device refers to an effective and completely practical device. An adversary may additionally launch assaults the usage of high-end gadgets (i.e., laptop) so as to gain get admission to and motive harm to IoT devices and networks from everywhere.

2) Location Property

IoT gadgets are linked globally and are susceptible to assaults from the net or inside 6LoWPAN networks. The methods of such assaults are as follows:

- *Internal Attack*

An adversary's attack from a local network either the usage of his/her very own tool or a compromised legitimate device. Such assaults can also encompass routing assaults, namely Flooding, Blackhole, and Sinkhole attacks.

- *External Attacks*

Starting up an assault on IoT devices or networks, the attacker might be deployed out of doors and a way from a local community. Examples of such attacks are Brute-force, malware, comfortable Sockets Layer (SSL), and domain call gadget (DNS) assaults.

3) Attack Level

An adversary may additionally attack IoT gadgets or community at one-of-a-kind ranges such as energetic or passive a good way to either disrupt traditional capability or simply to accumulate crucial statistics.

4) Attack Strategy

An attacker may belong to exceptional interest corporations. They'll attack the IoT tool or community the usage of one-of-a-kind strategies.

5) Damage Level

IoT devices, networks, and packages are prone to a large number of protection attacks, which can also purpose unique ranges of damages. They will variety from facts leaks, provider disruptions to bodily damages of the IoT device

6) Host-Based Attacks

The gadgets used in IoT are embedded with software which could contain personal statistics, cryptographic keys and different sensitive information. The statistics can be targets of the attackers.

7) Protocol Attacks

Malicious attackers compromise popular protocols of IoT Gadgets and networks with a purpose to disrupt verbal exchange most of the gadgets.

IV. IOT LAYER-BASED ATTACK TAXONOMY

IoT architecture comprises of different technologies which paintings independently to make a whole device. Inside the previous segment, we taken into consideration the IoT's three-layered architecture. In this segment, we classify IoT attacks based at the three-layered architecture that consists of application, network and bodily layers. Protection attacks can also result in thousands and thousands of greenbacks in losses to massive business and highbrow belongings robbery.

A. Application Layer Attacks

Considering that worldwide standards and guidelines are but to be installed for IoT to govern the improvement and interactions for IoT Packages, IoT software layer is still liable to many Protection attacks. Numerous packages of IoT use exceptional Authentication strategies, which makes it tough to combine them on the way to ensure authentication and records privacy. The number of applications is growing, and a large quantity of gadgets are being connected to be able to percentage a tremendous Quantity of statistics. Packages, which examine the ones facts or Information, might also have a massive overhead and service can also Emerge as unavailable due to safety assaults. The most important assaults At the IoT software layer and their affects are described Beneath.

- *Virus and Malware*

These attacks are centered at the gadget with the purpose of breaching confidentiality. They normally occur within the form of applications consisting of Trojans, spams, and worms or other viruses. In IoT networks, smartphones, sinks or gateways and other high-give up IoT devices are drastically at better hazard of these styles of assaults than sensor-based motes. Furthermore, Bluetooth technology which include 802.15.4 enabled devices are at high danger. Consequently, mitigation of such viruses and malware in IoT applications have to be taken into critical consideration.

- *Spyware*

Adware is a program this is set up on customers' IoT devices without the users' consent. The main purpose of this attack is to secret agent or display users' behavior and acquire sensitive records which include user IDs, passwords, keystrokes, and credit card data. Adware commonly does now not purpose any harm to the IoT devices or customers directly; it specifically steals private statistics and sends returned to the distributor. The data is then used as the premise for advertising and marketing evaluation or pop-up ads. Traditional spyware detection procedures are signature, conduct, and specification-primarily based strategies. Signature-based totally strategies come across only recognized spyware; consequently, unknown spyware times continue to be unattended.

- *Spoofing*

An attacker may additionally impersonate a node to launch a spoofing attack. A spoofing attack is one
Of the high-threat attacks because of its attacking method with a suitable portable reader, a transmission would possibly be recorded. As the attacker impersonates the node, the retransmission might seem from a legitimate node.
This attack may also exist in all three IoT layers. Spoofing attacks by way of impersonating of nodes are categorized because the assault of authentication, and it additionally violates the privacy precept.

- *Code Injection*

An attacker inserts malicious code right into a smart software/device via misusing faulty or a system can also lose control, thereby ensuing in a total gadget shutdown.

- *Message Forging*

This attack happens when a malicious node modifies or creates a message to deliver contents apart from the unique. It is able to be categorized as a sort of Replay attack inside the case of enhancing information synchronization.

- *Intersection*

This attack is also known as a composition attack. It goals the gadget's privateness via gaining secondary information from the system. The attackers acquire such facts from 0.33 celebration sources or public statistics. The adversary objectives and uses the non-linkable detail. The anonymized records of the privacy information from exclusive assets are then getting used to link them.

B. Network Layer Attacks

IoT network layer verbal exchange isn't the same as that of traditional net because of M2M verbal exchange among heterogeneous devices. This sediment can also suffer from safety compatibility problems and is prone to distinctive safety attacks together with

- *Hello Flood*

Message flooding is one of the most important assaults inside the community layer, wherein, an attacker goals to exhaust network or node assets such as battery or bandwidth with the aid of sending a multitude of course status quo requests.

- *Replay Attack*

This attack takes place normally throughout synchronization to lie to the vacation spot node such that a malicious node stores transmitted data, and handiest to retransmit it at a later time. Missed frames retransmission request is usually made with the aid of transmitting packets time and again throughout a network with the series numbers to senders and receiver nodes.

- *Sinkhole*

On this type of assault, an attacker trespasses and compromises a relevant node of a network so as to make it unavailable which leads to packet dropping in addition to DoS attacks. The danger degree of sinkhole assaults is higher than that of tempering assaults, in which a few numbers of nodes are compromised. Regarding the infrastructure-based device, the sinkhole assaults could manipulate the whole network.

- Sybil Attack

Sybil attack is released by developing a node and offering its own numerous identities inside the network so as to benefit large affect, which in turn leads to the removal of authentic lively nodes from the routing table. Here, the machine's weak spot depends on a few elements including the benefit with which the ones multiple identities are created, the extent of have an impact on to which the system has the same opinion to take inputs from a relied-on entity, which isn't linked to a chain of consider.

- *Clone Id*

The name means that the adversary clones the identification of legitimate IoT node so one can benefit access to consumer data visitors. The malicious clone node can be recognized with the aid of storing the geographical vicinity and identification of each node at 6BR (6LoWPAN border router). It can additionally be traced, the usage of a dispensed hash Table.

- *Blackhole Attack*

During a Blackhole assault, the malicious node drops all the packets that it encounters and the whole community operations get affected. This assault is classified as a excessive effect assault because it absorbs all routing statistics. An outsider floods out malicious routing records to claim the satisfactory path to the vacation spot. The sender then chooses the malicious direction to transmit the packets. The attacker often sends fake path-respond (RREP) to the sender. The source node continues transmitting its packets through the malicious course, the attacker drops all the packets, and he/she does now not ahead any site visitors to the destination.

C. Physical Layer Attacks

The principal additives of the bodily layer are sensors, RFID tags, WSNs, cameras, and so on. This residue of IoT suffers from some of protection attacks and threats. There are a few solutions available to those attacks. But, imposing autonomic safety solutions within the hardware at the physical layer is greater robust and quicker. Complex schemes are usually extra high priced and need to be averted. Light-weight methods have to be implemented to be able to boom tool lifetime and decrease complexity. Attacks in the physical layer are described as follows.

- *Tag Cloning*

RFID tags can effortlessly be cloned through an adversary. It may be finished via accomplishing the required records by means of direct get entry to be a device or the usage of reverse engineering.

- *RF Jamming*

Radio Frequency (RF) jamming reasons the sharing of wireless bandwidth to be ineffectual for the underlying devices. There may be a substantial hazard level from jamming based totally attacks in IoT due to the feature of faraway, unmonitored deployment of clever gadgets. It's miles a bodily layer attack in which RFs are interrupted for interference and saturated noise signals. A DoS assault can result from RF signal jamming of underlying channels. Right monitoring of the cognitive spectrum might also prevent it.

- *Node Injection Attack*

This attack is a variant of the MitM assault. It's far one of the maximum effective attacks on the physical layer of IoT. The attacker injects or deploys additional node in between two or greater IoT nodes within the community topology. The injected node takes part in conversation and takes manage of the visitors inside the network.

- *Tampering*

This assault violates confidentiality and accessibility. In this sort of attack, the information of the stop tool is modified, introduced, or deleted by an attacker. The attacker bodily captures and compromises an stop node from the community. Thus, all records may be collected by using the attacker. Similarly, reprogramming, redeployment, and recuperation of facts from the sector can be executed through such an attack. An attacker recovers the layout and type of transmitted records, then tampers and regenerates the identical kind of data. Therefore, the precision of records generated via the network becomes remarkably doubtful.

- *Physical Damage*

An attacker physically damages IoT nodes by way of getting rid of or deactivating them. Therefore, the provider turns into unavailable. As a end result, the need of mitigation strategies for such an attack is giant for IoT. These days, clever cities are filled with IoT factors together with sensors, cameras and clever lights that may easily be damaged or stolen by means of adversaries. The adversary tries to assault onto the interface of IoT nodes for shutting down or bodily adverse them. A multitude of these attacks will purpose the community to fail.

- *Exhaustion Attack*

Jamming or previously cited DoS attacks may bring about exhaustion assaults. Specially, the battery-operated devices can also be afflicted by electricity exhaustion if an attacker continuously assaults the community. Repeated tries of retransmission may purpose collisions in IoT MAC protocols, which leads to excessive-energy exhaustion. Exhaustion is taken into consideration as a high effect DoS attack and is related to deactivation attacks a good way to lessen the network length and completely do away with the nodes from the community.

V. COUNTERMEASURES FOR SECURITY ATTACKS IN IOT

Every IoT layer is constituted of a set of protection protocols, techniques, algorithms, and protection kits employed to make it more difficult for an adversary to attack or hack into the system. A higher knowledge of those notions will permit the researchers to analyze the security breaches and the extent of defense this is wanted. In addition, Intrusion Detection structures (IDS), Intrusion Prevention systems (IPS), and other whole safety answers may be applied to protect IoT from protection threats. This phase brings together the prevailing countermeasures inclusive of getting to know-based, encryption based, autonomic, and other techniques to comfy IoT structures from application, community and physical layers. We gift learning-based totally, encryption-based totally and autonomic methods and speak their relevance for constrained IoT.

A. Learning-Based Countermeasures

Learning-based totally techniques have been notably used in nearly all regions, which includes intrusion detection due to their specific nature of resolving real-time troubles. Gadget studying (ML)/Deep gaining knowledge of (DL) strategies specifically examine from current facts and expect the future behavior of a device. It is able to enhance system performance with the aid of classifying every day or odd conduct of a machine. The performance of such getting to know-primarily based models can be evaluated in phrases of class accuracy. There are four classes of a gaining knowledge of set of rules in practice, inclusive of supervised, semi-supervised, unsupervised, and reinforcement studying. There is few research executed on ML and DL for IoT safety. The following subsections bring together and explain some state-of-the-art proposed methods based on ML/DL as countermeasures to various security attacks and intrusion in the IoT system for application, network and physical layers.

- Countermeasures to Application Layer Attacks
- Countermeasure to Network Layer Attacks
- Countermeasures to Physical Layer Attacks

B. Autonomic Approaches

Safety methods have to be dynamic and with minimal human intervention. Although unique security attacks/issues can also require exclusive safety solutions, however, a few researchers proposed self-comfy/autonomic processes. The time period 'autonomic' refers to 'self-sufficient' or 'self-recuperation', and 'self-protection' mechanism, which manages the sources of the safety gadget without user Intervention. Self-recovery solution uses precise countermeasures after an attack has been detected, and self-protection is used to save you the assaults before they manifest. Self-safety refers to a gadget that's able to figuring out and defensive itself from random attacks. The mixture of a self-restoration and self-defensive mechanism is known as a hybrid technique. This section gives and analyzes the viable solution tactics which might be classified based totally on one-of-a-kind IoT architectures. Distinctive intrusion mitigation and detection tactics comply with self-sufficient strategies for securing for IoT.

C. Encryption-Based Countermeasures

On this segment, we discuss various present symmetric and uneven cryptographic countermeasures for securing IoT. Cryptography is the illustration of fashionable mathematical methods to shield towards cybersecurity attacks towards confidentiality, entity authentication, integrity and authentication. The community of things consists of several restricted nodes that talk with every different the usage of IPv6-6BR. This countermeasure does no longer precisely comply with the shape of reviews visible in sub-sections of getting to know-based and autonomic countermeasures for 3 layers of architecture as mentioned earlier than. The following variations of encryption-based countermeasures are applicable to different attacks of IoT architecture.

- Countermeasures using Symmetric Key Cryptography
- Countermeasures using Asymmetric Key Cryptography
- Countermeasures using Hybrid Key Cryptography

VI. CONCLUSION

In this paper, we have studied and supplied an outline of IoT, its enabling technologies, and compared the factors associated with enforcing a complete security method in IoT with conventional internet. A focal point has been given on safety assaults primarily based on IoT architecture. Assault taxonomy and comparisons were supplied. It is essential to bear in mind IoT architecture, its obstacles and variety whilst presenting comprehensive safety. Moreover, we discussed the various factors associated with the capability and barriers of IoT inside the layout of security answers. On this regard, we've got considered the need for IoT safety, which include traditional Confidentiality, Integrity and Availability (CIA) triad. Not like different studies we aggregated and discussed various advanced protection countermeasures including cryptographic, autonomic, and mastering-based schemes which make sure secure conversation for IoT in comparison to current surveys which considered simplest positive forms of countermeasures. This survey study will function a useful manual for researchers to get right of entry to a extensive variety of safety assaults and answers that may be of advantage to them. Subsequently, a discussion on existing procedures, implementation demanding situations and future research instructions was also furnished. Many researchers have proposed light-weight schemes for IoT, yet greater research paintings in this field is needed to design a holistic, unified, and properly suited protection countermeasures for the IoT as a whole.

REFERENCES

[1]. A_Comprehensive_Study_of_Cyber_Security_Attacks_Classification_and_Countermeasures_in_the_Internet_of_Things_2021_researchgate.net/publication/348856522_A_Comprehensive_Study_of_Cyber_Security_Attacks_Classification_and_Countermeasures_in_the_Internet_of_Things

[2]. A Review in Recent Development of Network Threats and Security Measures_2021_ hal.archives-ouvertes.fr/hal-03128076/document

[3]. A dataset for analyzing cyberattacks in Internet of Health Things_2021_ sciencedirect.com/science/article/abs/pii/S1570870521001475

[4]. A survey of Sybil attack countermeasures in IoT-based wireless sensor networks_2021_ peerj.com/articles/cs-673

[5]. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things_2021_ mdpi.com

[6]. R. Klahr, J. Shah, P. Sheriffs, T. Rossington, G. Pestell, M. Button, and V. Wang, ‘‘Cyber security breaches survey 2017: Main report,’’ Tech. Rep.,2017

[7]. K. Finnerty, H. Motha, J. Shah, M. White, Y. M. Button, and V. Wang, ‘‘Cyber security breaches survey 2018: Statistical release,’’ Tech. Rep., 2018.

[8]. K. Finnerty, S. Fullick, H. Motha, J. N. Shah, M. Button, and V. Wang, ‘‘Cyber security breaches survey,’’ Tech. Rep., 2019.

[9]. R. Vaidya, ‘‘Cyber security breaches survey 2019,’’ GOV.UK, Portsmouth, U.K., Main Rep., 2019.

[10]. B. Sudqi Khater, A. W. B. Abdul Wahab, M. Y. I. B. Idris, M. Abdulla Hussain, and A. Ahmed Ibrahim, ‘‘A lightweight perceptron-based intrusion detection system for fog computing,’’ Appl. Sci., vol. 9, no. 1, p. 178, Jan. 2019, doi: 10.3390/app9010178

[11]. M. Gulzar and G. Abbas, ‘‘Internet of Things security: A survey and taxonomy,’’ in Proc. Int. Conf. Eng. Emerg. Technol. (ICEET), Feb. 2019, pp. 1–6.

[12]. J. Deogirikar and A. Vidhate, ‘‘Security attacks in IoT: A survey,’’ in Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC), Feb. 2017, pp. 32–37, doi: 10.1109/I-SMAC.2017.8058363.

[13]. K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, ‘‘Internet-of-Things security and vulnerabilities: Taxonomy, challenges,andpractice,’’ J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, Jun. 2018, doi: 10.1007/s41635-017-0029-7.