JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

EXPLORATION Of ATTACKS On INTERNET Of THINGS; POSSIBLE VULNERABILITIES And COUNTERMEASURES

Ms. Shruti Jain, Dr.Kanak Saxena, Mrs.Sumeet Dhillon
M Tech Scholar, Associate Professor, Assistant Professor
Department of Computer Science & Engineering
Samrat Ashok Technological Institute, Vidisha, India

Abstract: **IoT is a promoter for modernization and intelligence of various crucial attributes of day-to-day life like smart homes, auto transport, smart cities, smart medical facilities, etc. But, all these comfort level possibilities are the open doors to welcome threats and attacks to the privacy and security of devices. The fear of losing privacy or confidentiality of data and devices has lead to a downfall in the adoption as well as promotion of Internet of Things. Thus, this paper represents a comprehensive specification regarding IoT, including a explicit literature study on preceding research and survey papers, moreover, recent attacks on different layers of IoT, its vulnerabilities and possible countermeasures to secure devices from prevailing attacks are analyzed.**

IndexTerms **- Internet of Things, Wireless Sensor Network, Cloud**

I. INTRODUCTION

Just like every basic need of human beings, internet is also becoming a fundamental necessity of humans. Referring to data record 2022, around 4.96 billion people all over the globe exploits the internet which is approximately 63.5 percent of the world's entire population. The continuous growth of internet has lead to the development of human surroundings by automating the tools and devices encircling them. Thus, has given arise to a new technology denoted as Internet of Things. In recent times, Internet of Things has become one of the dominant technologies of the 21st century allowing the objects and machines to interact, compute, synchronize and communicate with one another.

Now a days, one can connect everyday objects like kitchen appliances, vehicle, baby monitors to the internet via embedded devices, seamless communication is possible connecting people, processes, and things. The rapid growing network of connected physical objects, permit to exchange and collect data using embedded sensors, software, and other technologies. The Internet of Things, refers to the arrangement of interrelated processing or communicating devices, mechanical machines and digital machines, articles, creatures or individuals that are furnished with UIDs (unique identifiers) and the capacity to exchange information or data over an organization without expecting human-to-computer or human-to-human communication.

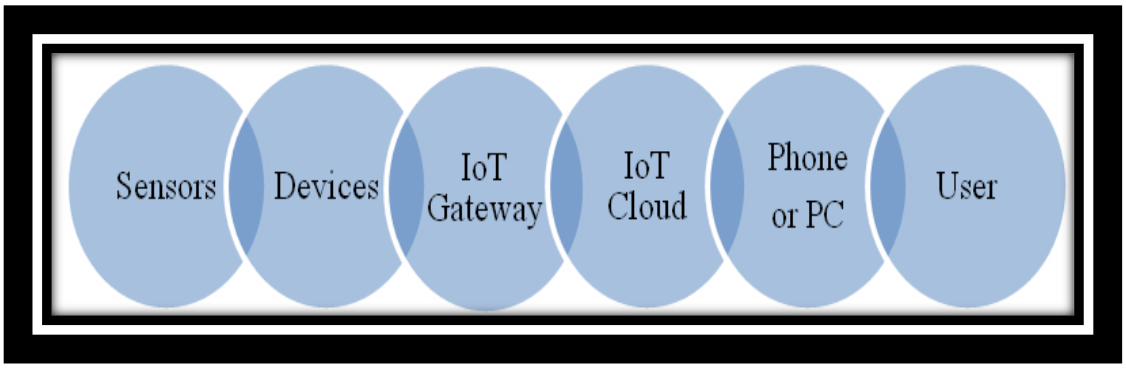

Figure 1 IoT Model

With IoT, number of devices available in our surrounding can connect and communicate with each other and exchange information using internet. Few of the devices are smart television, smart lock, smart vehicles, smart healthcare, smart wearable and many more. These smart gadgets function by using sensors to transmit data to PC or software's permitting them to execute crucial task. Due to their availability and automation, there has been an increment in the number of things that are being connected to internet.

Internet of Things has the strength to monitor and address devices as well as track them. IoT helps in reducing the workload with automation and helps save time and cost. Thus, the devices are designed in a way so that little or no human interruption is required to operate them. Therefore, reduces human efforts to great extent. The Internet of Things (IoT) system inspire M2M that is machine to machine communication which results in long term efficiency by saving resources and money of organizations and consumers. Internet of Things yet has a very long way to go, there is still a huge potential in this technology. The organizations need to secure the data or information they collect from their users by protecting it in the best possible way.

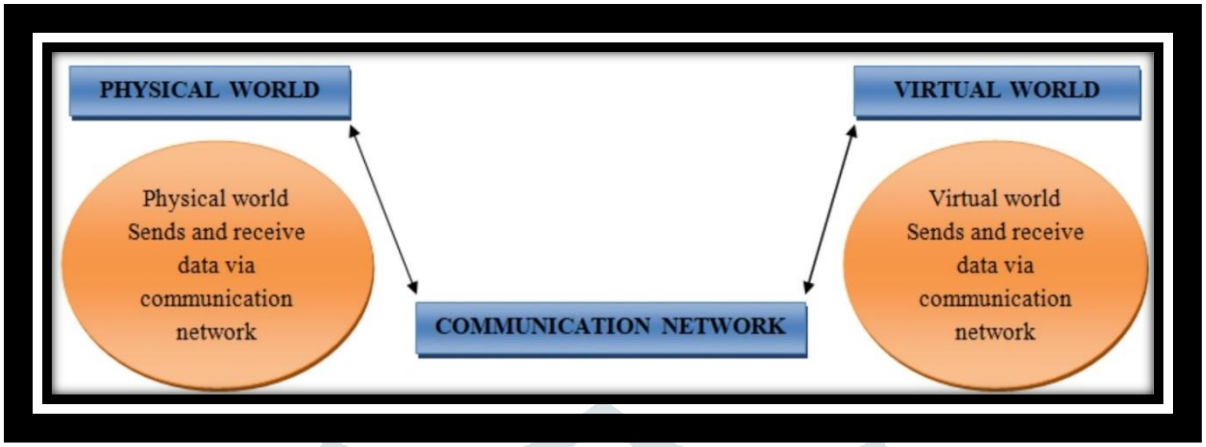

Figure 2 Internet of Things Building Blocks

Internet is the base for supporting IoT, therefore maximum security threats that are linked to internet propagate to Internet of Things as well. The area where threats in IoT may take place are the devices, communication medium, applications and software. Devices are the primary source through which attacks are initiated. Memory, physical and web interface, network services, and firmware can be the parts of device giving rise to vulnerabilities. Attackers can also harm the device via insecure default settings, out of date components etc. Attacks on Internet of Things arise from the channels that link IoT nodes to one another. The security concern in the protocols used in Internet of Things can harm the entire system. IoT systems are susceptible to physical attacks, network attacks, and software attack, harming the different layers of IoT architecture.

The paper is organized into 6 sections where Section-I defines the introduction to IoT. Section-II is literature review which contributes a detailed survey of previous year's research papers and articles regarding IoT attacks, vulnerabilities, security and solutions provided by the researchers. Section-III provides a tabular description of types of attacks with its definition and vulnerabilities associated to it. Section-IV put forward the solutions to IoT attacks. Section-V and VI covers the conclusion and future work corresponding to the subject.

II. LITERATURE REVIEW

The Internet of Things technology is spreading tremendously because of its potentiality to serve better services. IoT technology has been accomplished successfully on numerous devices. However, security is a vital challenge with its massive growth. Attacks are becoming frequent on IoT devices because of limited resources and diverse environment like low computational power and memory. Hence, these restrictions create difficulties in implementing security solutions in IoT devices.

According to [1] the rise of internet access ability and sensing capabilities in sensor nodes has merged WSN's (wireless sensor network) and IoT in internet connected world. IoT is furnishing access to massive amount of data over the web, accumulated by WSN's. Thus, might create an open route for the attackers. Hence, in [1] precise analysis of security attacks concerning IoT and WSN including the methods namely data aggregation, key management, traffic shaping, hierarchical security solutions, for detection, rectification and reduction of attack are mentioned. The attacks are divided into two parts active and passive attacks like jamming-DoS, collision, exhaustion, flooding, routing, de-synchronization and traffic analysis, node destruction respectively with layer wise description and estimation of defending tactics against mentioned attacks.

As mentioned in paper [2] due to the rapid development of IoT many threats in privacy and security exists which restrain its progression. Thus, the paper [2] analyze the security goals essential for a reliable IoT system and also classify the security threat and issues using classification methodology that is dividing attacks into four classes- physical, software, network and encryption attack. Further, the security countermeasures such as secure booting, device and data authentication, confidentiality, anonymity, secure routing, access control lists, anti-spyware, anti-adware etc. are highlighted which are essential for safe and stable IoT systems.

The paper [3] put forward a survey of attacks on wireless sensor network including traffic analysis attack, DoS attack, routing attack, Sybil attack, eavesdropping etc. and highlighted few feasible solutions and strategies such as secure routing scheme, key management, encryption, spread spectrum techniques for diminishing the security susceptibility in wireless sensor network. Thus, the article also includes the vital security concern for WSN.

The author in paper [4] has divided the attacks into two types that is active attack and passive attack to outline valuable countermeasure for making communication safe and secure. Active attacks includes tampering attack, jamming attack, physical attack, DoS attack, routing attack, node replication attack, whereas passive attack includes traffic analysis, camouflage adversaries, homing attack, monitoring and eavesdropping. As defined in the paper [4] the intruder intends to seek and destroy the data on the other hand in passive attack the intruder aims to steal confidential and valuable data like codes and passwords. Thus, the paper recapitulates the security constraints and challenges of numerous security attacks in wireless sensor network. Moreover, the paper [4] encapsulates the security needs as confidentiality, authentication, integrity and authorization of information and network.

Paper [5] includes overview of different IoT attacks on physical, data link, network, transport and application layer of wireless sensor network and challenges faced like unreliable communication, limited power, memory and storage. The paper also discuss the few security requirements as stated integrity of data, survivability, flexibility, secure localization, self-organization etc.

The author of paper [6] explores the layer wise security concern in IoT and aims to acquire the essential security techniques for jamming attack. Thus, the study recommended a multilayer security strategy for DDoS detection in IoT, that secure devices from Distributed Denial of Service attack and also minimizes the computational cost under mobility in the network. The author suggested a threshold based countermeasure (TBC) for reprise attack in every layer. The outcome indicates low energy utilization and low computational cost. Hence, the research resulted in improving the scalability using TBC in sensor network.

Wireless Sensor Network is combined with IoT via sensing ability of internet connected sensor nodes and devices. It is crucial to protect the network from internet attacks by securing the router. The paper [7] objective is to provide an authoritative literature review on prevention and detection system in mobile Ad-hoc network and WSN's for securing IoT applications. The paper [7] emphasizes on numerous attacks with the acceptance of avoidance and alleviation models. Moreover, several deep learning and machine learning models including various implementation tools, types of dataset preferred and performances in every contribution is evaluated. Thus, the survey is concluded with diverse research options in implementing IDS to conserve security features of IoT for mobile Ad-hoc network.

As truly mentioned in paper [8] security is an immensely crucial concern for Internet of Things that requires to be tackled effectively. Heterogeneity being an immanent attribute of IoT cause security concern that is to be undertaken by approaching modern framework like cryptographic algorithm software networking ,edge computing and federated cloud. The paper [8] has organized IoT security using three approaches – three layer security structure, security barrier at every layer and its countermeasure. Thus, explores the prevailing state of art, methodologies and protocols preferred at every layer of the architecture. As per the findings the data swapping, that links the various applications or devices in IoT framework are quite fragile, therefore highlights acute need of designing security strategy and guideline for IoT devices. Hence, the paper [8] accomplishes the comprehensive and substantial research in IoT security domain including the suggestions and countermeasures to alleviate the threat arising at different standard of IoT protocol stack.

The paper [9] recommended that smart device security can be enhanced by restricting direct internet request. Every call must be authenticated via block-chain interface, and in case of accuracy, the request can be approved. A easy interface can be implemented as a security gateway adding on device assignment as one more layer for security shielding of web connections and services. Moreover, the interface will further secure the devices from third party approach to the network. The paper [10] mention Internet of Things as persistent scenario of computing including actuators and sensors merged with internet. As per implementation the integrated methods and procedure of security issue play a vital role. Thus, it explores the IoT background, security issue, open challenges as fault tolerance in the network, network scalability and delay, network agility and privacy features as authentication, data protection, and more, on the existing methodologies for implementing IoT in numerous directions are also emphasized.

According to paper [11] security vulnerabilities are enhancing with the increment in the growth of interconnected devices and IoT. Security features are in associated devices, data transmission procedure and storage method. The advancement of IoT may be affected by security threats like ransomware, viruses, malwares etc. to secure reliable IoT, numerous security programs are being evolved. Proceeding, the paper [11] discusses the latest state of security characteristics of IoT. Thus, the research mentions various probable security threats in IoT environment and also explores the machine learning algorithm beneficial to hinder IoT threats. Hence, the results refine the security network and furnish user with reliable user skills.

The survey paper [12] employs IoT network architecture that is equivalent to traditional network architecture to communicate between numerous devices including the limitations of traditional network architecture. In the evolution of Internet of Things, different attacks have been introduced to harm the security of IoT devices. Many researchers have recommended various solutions to overcome these attacks till date. But implementing these security standards and techniques simultaneously can give rise to excessive battery consumption and computation power of devices. Thus, to resolve maximum security issues a good security mechanism is required and it must be robust, light weight and reliable for IoT devices. This survey [12] classifies and discusses IoT attacks as physical, network, software, encryption attack and mentions the security precautions that need to be taken at the time of application development or device communication to ensure the security.

The paper [13] examines and explores the IoT privacy and security concern using advance approach that is IoT features. Revealing the existing security threat and solution, mentioning the research challenges for future scope related to IoT features. Moreover, specifying the modern security and privacy technologies for further analysis and learning. Thus, after deeply examining many previous studies the author emphasizes the growth trend of current IoT features and security research.

The objective of paper [14] is to direct a comprehensive literature survey regarding privacy enhancing technologies using newly initiated categorization in the IoT applications. The latest privacy enhancing technology employed in the IoT has been drafted and compared with 120 studies and the results are included in the research paper. Moreover, open issues as identification, tracking, profiling, inventory attack, privacy violating interactions, and the privacy policies such as unlink-ability, transparency, usability of data and system, restrictions/ drawbacks and potential progress regarding PETs in the Internet of Things has been identified.

Internet of Things has capabilities to put forward the industrial reorientation which is essential to government, business and consumers, modifying entire sectors incorporating agricultural, automotive, manufacturing infrastructures, automations, electronics and services, medical etc. IoT has an ability to initiate a major transformation in the coming future. The huge amount of data produced by IoT, needs attention on the cryptographic data repository, employed edge computing, artificial intelligence and analytics. The survey paper [15] also comprises research possibilities like self-configuring software's, analysis of complex data and auto-power sensors.

According to the article [16] the Internet of Things affiliates numerous devices in the network with advance and inventive services to secure the privacy of users from attack like jamming, spoofing, eavesdropping and Denial of Service attack. The following research explores the artificial intelligence and machine learning models merged with IoT to emphasize device security, adding on the learning techniques that are supervised, unsupervised and reinforcement learning. The paper [16] also includes access control method, detection of IoT malwares, authentication, secure offloading using machine learning and AI.

Moreover, directs the IoT challenges that are required to be analyzed and examined practically before imposing security in IoT devices. Implementing artificial intelligence principles, techniques and instruments in Internet of Things can solve large number of IoT issues. Thus, also mentions the future research approach to come up with more elaborated solutions to IoT.

The research [17] states a detailed explanation of industrial IoT attacks namely DoS, authentication attack, man-in-the-middle, side channel attack, malware injection, phishing, mobile device attack, etc. including the fundamental characteristics, attributes and vulnerabilities, also mentioning the thorough evaluation of expressive suggestions to the vulnerabilities. Thus the article authenticates the reference statements and suggestive assumptions for recognition and analysis of risk involvement to the developing industrial scenario.

The classification paper [18] contributes a broad and comprehensive classification of numerous attacks on IoT IoT based on connecting protocols, components, architecture, reference model and moreover related to data perception, storage, processing, and transmission, also includes the suggested countermeasure to diminish the consequences of attack. But, simultaneously implementing all techniques and securing methods can lead to excessive computation power consumption of devices which is not at all adequate. Thus, the devices need to be robust, scalable and lightweight with secure mechanism to resolve maximal Internet of Things security issues.

The paper [19] explains the advantages of integrating Internet of Things into human day-to-day life by introducing smart devices and sensors, automations and data analytics. But, these IoT devices are highly vulnerable to attacks and security issues. Thus, the research [19] explores the recent attacks like Man-In-The-Middle attack, injection attack, DNS attack, brute force attack etc. in the IoT environment as well as their countermeasures. Yet the miscellaneous characteristics and limitations of IoT devices can make few findings tactless and unfortunate for Internet of Things. Since, the technology is expected to upgrade day by day and may result in rise of more vulnerabilities and their preventions.

The survey [20] layout a comprehensive classification of Internet of Things attacks into three categories that is passive attacks, service degradation attacks and Distributed Denial of Service attacks respectively. The author analyses the attacks with reference to kill chain and contributes a medium for building more precise AI (artificial intelligence) based paradigm for malware detection.

The author in paper [21] proposed an easy and relevant naming method for classifying IoT threats. The categorization is done on the basis of IoT layers attacked and infected security and privacy goals. The taxonomy is organized into two elemental building blocks that is attack on IoT layers and security concepts. The architecture of IoT is classified in three layers that is cyber physical layer, middleware, and application layer, each layer performing different task like device stimulation and sensing, transferring and addressing information, processing accumulated information for decision making respectively. Thus, the study [21] simplifies the IoT threats using naming scheme typology for IoT attacks.

The paper [22] signify the taxonomy of real world IoT threats mainly cryptanalysis attack, side channel attack, sleep deprivation attack, replay attack, man-in-the-middle attack, social engineering, malwares, Denial of Service attack, eavesdropping, as well as classify and map them to the relevant class of attack. Moreover, revels the security vulnerabilities related to the attacks and provides a dominant countermeasure. The research is explored into three domains named as industrial, consumer and commercial sectors with their functioning goals and limitations. Thus, the author contributes the strategic approach to mitigate and secure the environmental sector from IoT attacks and also recommend policies to handle upcoming IoT threats.

III. TYPES OF IOT ATTACKS AND THEIR VULNERABILITIES

The employment of Internet of Things is growing exponentially, which is consequently leading to a rise of IoT threats and vulnerabilities. These IoT attack targets to destroy, disable, manipulate, block, steal or gain illegitimate access to data and devices causing major harm to the IoT developing network. Thus, this section presents a layer wise detailed description of IoT attacks with its major vulnerabilities as mentioned in table 1. On the basis of layers the attacks are divided into seven groups as physical attacks, data link attacks, network attacks, encryption attacks, software attacks, transport attacks and application attacks accordingly.

Table 1: Types of Attacks with Description and its Vulnerabilities

S.no.	Ref. No.	Attacks on IoT	Type	Description	Vulnerabilities
1	[2], [12], [19], [20]	Malicious Code Injection	Physical Attack	The attacker gets complete control over the IoT devices by manually inserting a malicious code into the nodes of IoT systems.	1) Loss of data or manipulating data. 2) Shortage of accountability or denial of access. 3) Can lead to entire host takeover.
2	[12], [22]	Social Engineering	Physical Attack	The attacker gathers confidential information by physically interacting and manipulating users of IoT systems.	1) Entice unsuspecting users into exposing information. 2) Spread of malware infections. 3) Accessing restricted systems.

3	[1], [2], [4], [12], [20]	Node Tampering	Physical Attack	The attackers physically alters the sensor node and can gain sensitive information like cryptographic key (encryption key).	1) Modifying or replacing sensors with malicious sensors/devices. 2) Extraction of cipher data.
4	[2], [4], [12], [20], [21]	Node Jamming In WSN	Physical Attack	The attacker deliberately attempts to interfere with the communication of signals in a wireless sensor network by using jammers.	1) Refusing the transference of authorized packets in network. 2) WSN are highly vulnerable to network attack.
5	[2], [4], [12], [15], [21]	Physical Damage	Physical Attack	To know the hidden aspects of system the attacker physically damages or stealing the components of IoT devices.	1) Document or record thieving. 2) Identity theft. 3) shadowing or tailgating.
6	[2], [12], [20], [21], [22]	Sleep Deprivation Attack	Physical Attack	The attacker aim is to maximize the power usage of the nodes which results in shutting down the system or minimizing their energy to perform any task.	1) Can lead to battery drainage and it is not possible to restore battery potential of sensor nodes. 2) More of overload can lead to faulty throughput.
7	[1], [17]	Collision	Data Link Attack	Transmitting message by two nodes at the same time of the same frequency. There are 2 types of collision : environmental and probabilistic collision.	1) The PDF records are vulnerable to collision attack using color values which can further be modified to substitute the content of signed document.
8	[1], [17]	Resource Exhaustion	Data Link Attack	The continuous re-transmission and recurrent collision until the sensor node is completely destroyed.	1) Slow going or crashing of software because of unhandled errors. Degradation of service and may even cause total halt if takes place at huge amount.
9	[1], [2], [3], [4], [12]	Traffic Analysis Attack	Network Attack	To identify routing framework, address of key nodes, network information, the attacker determine and examines message and network communication.	1) Intruder can make use of traffic analysis and network pattern as a base for further targeted attack.
10	[2], [12]	RFID Unauthorized Access	Network Attack	The adversary modifies, monitor or delete information stored on nodes. Thus, proper authentication is required in radio frequency identification system.	1) Illegitimate reading or writing of tag data or trigger devices. 2) RFID systems are vulnerable to physical and electronic attack.
11	[3], [15], [17], [21], [22]	Denial Of Service (DoS) Attack	Network Attack	In DoS, the attacker's flood the targeted network with traffic by sending large amount of request so that the verified user cannot access its services.	1) Destabilizing or crashing system. 2) Giving rise to flood attack or buffer overflow attack. 3) Inappropriate use of network or resource connections.
12	[2],	Routing	Network	The attacker makes the network	1) Variability in router software.

	[3], [12], [20]	Information Attack	Attack	complicated by altering, spoofing or communicating routing information, which ends with forwarding inaccurate data, packet falling or splitting the network	2) Lack of authentication. 3) Affect the network utility and business performance.
13	[17],[18], [19], [22]	Man-In-The-Middle Attack	Encryption Attack	When 2 end users exchange keys or transfer data, the attacker interrupts the communication and acquires confidential information.	1) Hijacking Secure Socket Layer (ssl) and Session hijacking. 2) Spoofing Domain Name System. 3) ARP cache corrupting.
14	[2], [12], [20],[22]	Side Channel Attack	Encryption Attack	The side channel data released by encrypting devices is used by the attacker which is neither the plaintext nor cipher-text, it consist of information related to power, fault density, time taken to execute the task etc. Thus, this information is used by the attacker to determine the encryption key.	1) Give rise to a severe threat to modules that integrate the cryptographic systems. 2) Capable of gaining and analyzing the measurements over multiple operations and various physical criterion / parameters.
15	[2], [12], [21], [22]	Crypt-analysis Attack	Encryption Attack	It refers to the analysis of codes by using plaintext or cipher text in order to know the hidden aspects. It is used to gain access to the data of encrypted message even if cryptographic key is not known. Cipher-text only, known plaintext attack, chosen plaintext and chosen cipher-text attack are the different types of cryptanalytic attacks.	1) Total break- detecting secret key. 2) Information deduction- obtaining knowledge related to unknown cipher-text or plaintext. 3)Distinguishing algorithm- intruder has the potential to differentiate the resultant of cipher-text from a random combination of bits.
16	[12], [17], [21]	Phishing Attack	Software Attack	It refers to the practice of hacking personal information like username, password or stealing sensitive data like credit, debit card login information etc or installing malware on victim's system. It is done through emails.	1) Manipulation of link or spoofing. 2) Evading filters. 3) Targeting unsuspected uses.
17	[2], [12]	Malicious Script	Software Attack	It is a type of injurious computer script or web code leading to vulnerabilities like security breaches, data theft, and potential harm to files and system.	1) Account hijacking. 2) Access to clipboard data/ browser history. Spreading web worms. 3) Exploiting and scanning intranet devices and applications.

18	[2], [11], [12], [17], [18]	Virus, Worms, Trojan Horse, Adware Attack	Software Attack	Virus is software's that link itself to other computer programs to harm the system. Worms are computer program which replicate itself to slow down the computer. Trojan Horse are hidden codes which steals confidential information of users or computer network. Adware are pop-up advertisement that flash on computer screen can be malicious and harm the system by hijacking browser and installing viruses or spywares.	1) Immoderate privileges, consent authorization that intensify the probabilities of attack. 2) Hacking of easy and weak passwords, files and unable to install the updates as it holds vital patches that may fix vulnerability.
19	[1], [18]	Flooding	Transport Attack	It refers to the repetitive request of new link or connection till the IoT systems hold out maximum level.	1) Sending huge amount of traffic to a server or network segment and exhausting the resources, and not allowing to execute legitimate request.
20	[1], [17]	De-Synchronization	Transport Attack	The attacker uses fake sequence's and copies the message linking one or more end points of the active link and disturb the existing connection.	1) Can cause loss of synchronization (generally losing image coordinate) 2) Permanently disabling the authentication ability of RFID tags.
21	[1], [25]	Attack On Reliability & Clone Attack	Application Attack	In clone attack a malicious unauthorized node claims the identity of authentic node in the network and ultimately tries to trap the entire network.	1) Reprogramming sensor nodes and joining it to targeted network. 2) Lack of availability and gaining information from unauthorized users can also be vulnerable to clone attack

IV. COUNTERMEASURES TO IOT ATTACKS

Every bit of vulnerability needs a different solution. In case of IoT device security a fusion of detecting, preventing and mitigating the vulnerability is required across the multiple layers of IoT. But, what makes IoT vulnerable to attack? Lack of synchronization and standardization in IoT security is one of the major factor. The unavailability of hardware capacity required to handle robust security is also a major concern. Thus, considering all the factors, following are the possible solutions to IoT.

1) Employing Block-chain Technology

Block-chain technology refers to the decentralized, distributed, efficient, and transparent data performance. These operations can be useful in securing and strengthening diverse communication environment. Block-chain can be deployed as an audit system to support authentication, encryption, de-identification, handle block query, access control and key management. It can also be helpful in preventing IoT attacks because it provides a distributed ledger/ voting system to manage and maintain bandwidth and power requirements of IoT devices.

2) Network and IoT API Security

API (Application Programming Interface) security is crucial for securing the integrity of data transmission between IoT edge devices and back end systems. APIs ensure and verifies that the devices, apps, developers, and communication environment is authorized and authenticated. The network connecting IoT devices must be secured and protected by using anti-malware and anti-viruses security features and intrusion detection and prevention system.

3) Data Encryption and Authentication

Internet of Things collects a huge amount of data. Privacy of data is a big concern to device users. The efficient way to secure data is by using data encryption and authentication in IoT devices. For protecting sensitive and confidential data wireless protocol with built-in encryption is the possible solution. To secure online data SSL(secure socket layer) protocol can be preferred. Moreover, multifactor authentication, digital certificates, passwords and biometrics are other alternative to protect IoT devices from various threats and attacks.

4) Cloud Computing as a Security Solution to IoT

Cloud computing assist IoT in data analysis and storage to gain the maximum profit from IoT infrastructures. Cloud computing enables data transmission and data storage via direct link or through internet which allows uninterrupted transmission and communication of devices, data, applications and cloud services. Cloud provides distribution of resources and miscellaneous data along with the virtual environment and maintaining security using encryption, virtual private network or masking sensitive data in transit.

Table 2 : Countermeasures to IoT attacks

sno.	Ref.	Attacks	Countermeasures
1.	[19], [20]	Injection	Active management of updates and patches, validating user inputs, encrypting and hashing passwords, data monitoring and access control.
2.	[1],[2],[20]	Tampering	Tamper resistant hardware, Camouflaging, changing key regularly, proper key management, disabling JTAG, and secure bootstrap loader.
3.	[1],[4],[17]	Jamming	Use of spread spectrum transmission, wormhole techniques, use of intrusion detection system, re-routing data packets to alternative route.
4.	[2],[4], [15]	Physical Damage	Use of strong key locks and password, encrypting the data of storage devices, use of biometric authentication in devices, and tamper proofing.
5.	[1], [17]	Collision, Exhaustion	Use of Error Correction Codes, Time Division Multiplexing (TDM), FHSS (Frequency Hopping Spread Spectrum) method.
6.	[3], [12]	Traffic Analysis	Network monitoring, Traffic Queue, NAT(Network Address Translation), Encrypting traffic, Padding the traffic by adding fake packet in the traffic.
7.	[2], [12]	RFID-Unauthorized Access	Authorization and authentication using secrets and encryption, employ public key re-encryption, hash chain scheme, and anonymous-ID scheme.
8.	[4], [17]	Denial-of-Service Attack	Ingress and Egress Filtering, use of Encryption algorithm, prioritizing messages, Intrusion Protection System, and monitoring system.
9.	[3], [20]	Routing Information	Use of multiple paths for routing data, integrity and privacy of data, MAC authentication and use of data encryption and cryptography.
10.	[17], [19]	Man-in-the-Middle Attack	Semi state Address Resolution Protocol (ARP) cache, Use of system logs modeling, Encrypting web traffic using VPN (virtual private network), and maintaining a reliable and decentralized peer to peer network for data communication.
11.	[2], [12], [20], [22]	Side-Channel Attack	Blinding techniques and Masking Implementation to remove the link between secret data and leaked information. To eliminate the release of information analyze and evaluate systems with TVLA methodology (Test Vector Leakage Assessment), employ silicon based hardware root of trust.
12.	[21], [22]	Cryptanalysis	Maintaining integrity and privacy during sensitive information transmission, keeping secrecy in data storage, and identity authentication.
13.	[12], [17], [21]	Phishing Attack	Implementing IWAF (Intelligence Web Application Firewall), Applying Associative Classification data mining approach, Protecting the accounts by Multifactor Authentication, URL Embedding.
14.	[2], [12]	Malicious Script	Ensuring input validation on server and client side, limiting cookies utilization, validating data, use appropriate encoding/escaping technique.
15.	[11], [17], [18]	Virus, worms, Trojan Horse, and adware attack	Secure the routers and network, install antivirus protection software, secure the data transmission using encryption, implement access control and multifactor authentication, keep the software and firmware updated.
16.	[1], [18]	SYN-Flooding	Restricting the total number of link connections, client puzzles, firewall filtering, SYN-Cookies, install commercial tools to obtain entire network visibility, and set-up latest

			networking tools with rate limiting capability.
17.	[1], [17]	De-Synchronization	Use of authentication incorporating header of transport layer protocol, reliable transmission of MAC layer frames, 6TiSCH (IPv6 over the Time Slotted/ Synchronized Channel Hopping mode).
18.	[1], [25]	Clone attack	Public keys based on ID, Multilevel clustering, and key management on the basis of location.

V. CONCLUSION

The aim of IoT is to enrich the value of life using automation technology and smart applications. IoT contributes a lot of benefits but there are few drawbacks associated with Internet of Things. The security and privacy are the major concern related to IoT. Thus, it is mandatory to secure and protect the security environment of IoT persistently. A thorough and appropriate security evaluation on every layer of IoT should be carried out consistently. Most of the attack emerges due to the absence of complete knowledge and proper awareness concerning cyber-attacks or IoT attacks. Therefore, it is necessary to understand that the continuous progression of technology is concurrently leading to the huge evolution of IoT devices hacking and threats. The majority of population still rely on primary security techniques to stay protected from IoT threats. This survey paper encapsulates the persistent IoT attacks on application, encryption, software, network, data-link, and physical layers of IoT, their vulnerabilities and relevant mechanism to protect and secure systems, IoT devices. Thus, the study is profitable for upcoming researchers in numerous possible modes. Hereafter, it is essential to secure and protect IoT devices and data from all types of attack and maintaining complete security as per latest technology.

VI. FUTURE WORK

The IT and IoT departments are spreading and growing more and more covering majority of sectors and turning the world to be digital with automation. Thus, introducing the devices supporting wireless networks. For security and efficiency of data and transaction processing, block-chain technology is the most secure and trusted technology currently. Thus, in coming future it is expected to merge Internet of Things and block-chain technology together to gain privacy and secure transmission of data on devices.

REFERENCES

[1] Butun, Ismail, Patrik Österberg, and Houbing Song. "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures." IEEE Communications Surveys & Tutorials 22, no. 1 (2019): 616-644.

[2] Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges." In 2015 IEEE symposium on computers and communication (ISCC), pp. 180-187. IEEE, 2015.

[3] Ekong, V. E., and U. O. Ekong. "A survey of security vulnerabilities in wireless sensor networks." Nigerian Journal of Technology 35, no. 2 (2016): 392-397.

[4] Keerthika, M., and D. Shanmugapriya. "Wireless Sensor Networks: Active and Passive attacks-Vulnerabilities and Countermeasures." Global Transitions Proceedings 2, no. 2 (2021): 362-367.

[5] Sehrawat, Harkesh, and Vikas Siwach. "Security vulnerabilities in Wireless Sensor Networks." (2021).

[6] Khan, AB Feroz, and G. Anandharaj. "A Multi-layer Security approach for DDoS detection in Internet of Things." International Journal of Intelligent Unmanned Systems (2020).

[7] Pamarthi, Satyanarayana, and R. Narmadha. "Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms." International Journal of Intelligent Unmanned Systems (2021).

[8] Yousuf, Omerah, and Roohie Naaz Mir. "A survey on the internet of things security: State-of-art, architecture, issues and countermeasures." Information & Computer Security (2019).

[9] Šarac, Marko, Nikola Pavlović, Nebojsa Bacanin, Fadi Al-Turjman, and Saša Adamović. "Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture." Energy Reports 7 (2021): 8075-8082.

[10] Neeli, Jyoti, and Shamshekhar Patil. "Insight to security paradigm, research trend & statistics in internet of things (IoT)." Global Transitions Proceedings 2, no. 1 (2021): 84-90.

[11] Podder, Prajoy, M. Mondal, Subrato Bharati, and Pinto Kumar Paul. "Review on the security threats of internet of things." arXiv preprint arXiv:2101.05614 (2021).

[12] Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 32-37. IEEE, 2017.

[13] Zhou, Wei, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved." IEEE Internet of things Journal 6, no. 2 (2018): 1606-1616.

[14] Cha, Shi-Cho, Tzu-Yang Hsu, Yang Xiang, and Kuo-Hui Yeh. "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges." IEEE Internet of Things Journal 6, no. 2 (2018): 2159-2187.

[15] Kakkar, Shyna, and Vishal Monga. "A SYSTEMATIC LITERATURE SURVEY: INTERNET OF THINGS."

[16] Surya, Lakshmisri. "IoT Security Techniques Based On Machine Learning: How IoT Devices use AI to Enhance Security." International Journal of Computer Trends and Technology (IJCTT)-Volume 67 (2019).

[17] Tsiknas, Konstantinos, Dimitrios Taketzis, Konstantinos Demertzis, and Charalabos Skianis. "Cyber threats to industrial IoT: a survey on attacks and countermeasures." IoT 2, no. 1 (2021): 163-188.
[18] Damghani, Hamidreza, Leila Damghani, Heliasadat Hosseinian, and Reza Sharifi. "Classification of attacks on IoT." In 4th International Conference on Combinatorics, Cryptography, Computer Science and Computation. 2019.
[19] Rajendran, Gowthamaraj, RS Ragul Nivash, Purushotham Parthiban Parthy, and S. Balamurugan. "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures." In 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1-6. IEEE, 2019.
[20] Mudgerikar, Anand, and Elisa Bertino. "IoT Attacks and Malware." In Cyber Security Meets Machine Learning, pp. 1-25. Springer, Singapore, 2021.
[21] Wüstrich, Lars, Marc-Oliver Pahl, and Stefan Liebald. "Towards an extensible IoT security taxonomy." In 2020 IEEE Symposium on Computers and Communications (ISCC), pp. 1-6. IEEE, 2020.
[22] Xenofontos, Christos, Ioannis Zografopoulos, Charalambos Konstantinou, Alireza Jolfaei, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. "Consumer, commercial and industrial IoT (in) security: attack taxonomy and case studies." IEEE Internet of Things Journal (2021).
[23] Kathrine, G. Jaspher Willsie, and C. Willson Joseph. "Attacks, Vulnerabilities, and Their Countermeasures in Wireless Sensor Networks." In Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks, pp. 134-154. IGI Global, 2020.
[24] Jaitly, Sunakshi, Harshit Malhotra, and Bharat Bhushan. "Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey." In 2017 International Conference on Computer, Communications and Electronics (Comptelix), pp. 559-564. IEEE, 2017.
[25] Dora, Jean Rosemond, and Karol Nemoga. "Clone Node Detection Attacks and Mitigation Mechanisms in Static Wireless Sensor Networks." Journal of Cybersecurity and Privacy 1, no. 4 (2021): 553-579.
[26] Xiao, Liang, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." IEEE Signal Processing Magazine 35, no. 5 (2018): 41-49.
[27] Sharma, Gaurav, Stilianos Vidalis, Niharika Anand, Catherine Menon, and Somesh Kumar. "A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues." Electronics 10, no. 19 (2021): 2365.
[28] Istiaque Ahmed, Kazi, Mohammad Tahir, Mohamed Hadi Habaebi, Sian Lun Lau, and Abdul Ahad. "Machine learning for authentication and authorization in IoT: Taxonomy, challenges and future research direction." Sensors 21, no. 15 (2021): 5122.
[29] El Mouaatamid, Otmane, Mohammed Lahmer, and Mostafa Belkasmi. "Internet of Things Security: Layered classification of attacks and possible Countermeasures." electronic journal of information technology 9 (2016).
[30] Strous, Leon, Suné von Solms, and André Zúquete. "Security and privacy of the internet of things." Computers & Security 102 (2021): 102148.
[31] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and security: Challenges and solutions." Applied Sciences 10, no. 12 (2020): 4102.
[32] Resul, D. A. S., and Muhammet Zekeriya Gündüz. "Analysis of cyber-attacks in IoT-based critical infrastructures." International Journal of Information Security Science 8, no. 4 (2020): 122-133.