Webology, Volume 19, Number 1, January, 2022

A Survey on IoT Security: Attacks, Challenges and Countermeasures

H.J. Felcia Bel
Research Scholar, Department of Computer Science, SRM Institute of Science and Technology, Kattankulathur, Chennai, India.
E-mail: fh4219@srmist.edu.in

S. Sabeen
Assistant Professor, Department of Computer Science, SRM Institute of Science and Technology, Kattankulathur, Chennai, India.
E-mail: sabeens@srmist.edu.in

Received September 20, 2021; Accepted December 17, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19246

Abstract

IoT technology grows enormously now-a-days in various fields and it is a need to achieve high security requirements. IoT produces more amounts of data to communicate to each other which may undergo various issues like low processor speed, power, and memory. The IoT devices undergoing these barriers along with crucial information will get into different types of security attacks in IoT layers. An outline of IoT, it's architecture, state-of-the-art technologies, security attacks in layers and analysis of security threats are studied and the countermeasures have been reported in this survey. The challenges and goals facing IoT security have also been discussed. The security threats on the IoT devices have been briefly introduced. The security challenges, giving research directions and finding security solution for each and every challenge have been also discussed.

Keywords

Internet of Things (IoT), Architecture, Security Threats, Attacks, Countermeasures.

Introduction

Internet of Things (IoT) is a connection between objects and devices to communicate among them without human intervention. Internet of Things (IoT) is to extend traditional lifestyle of society into smart lifestyle. All humans and 'things' are connected with networks in this pandemic era. Internet plays a vital role among domestic purposes as well as in every field of day to day life. Moreover, Internet of Things is defined as the internet connected devices and objects embedded with sensors, softwares for transferring information through wireless networks without human intervention. Internet of Things security is an important aspect to concentrate as the entire globe is connected with massive networks. As per the IoT Statistical research, the number of IoT devices in 2021 will reach around 46 billion as per the report of Jupiter Research. Identifying the threats, attacks, new challenges, limitations and countermeasures in this mass device networks is a challenging task from the recent existing literatures and come out with an open discussion and future IoT in our proposed research.

A. Related Work

Kevin Ashton in 1999 introduced the term IoT (Mohamed Litoussia et al., 2020). IoT is connected with billions of devices such as sensors, Radio-Frequency Identification (RFID), wireless networks to transform the things into automated smart devices (L. A. Amaral et al., 2011). The various sensors in smart devices will sense the objects, devices and environment to transfer data in networks and communicate to each other (Z. Yan et al., 2014). Moreover, the devices, sensors, networks and things are well designed to have an efficient security system, it should be highly maintained by humans from all types of attacks (G. Svensson, 2013). It is a need to secure all the devices and objects from severe security threats by further security challenges (E. D. Frangopoulos et al., 2013). IoT applications consists of smart home, smart city, intelligent transportation system, smart agriculture, healthcare, earthquake detection, Smart parking and smart grid (K. Mohanta et al., 2020). IoT security data security challenges will be met unexpectedly (Zhi-Kai Zhang et al., 2014). In organizations, the worms and viruses may attack. In May 12, 2017, the systems and networks affected by the WannaCry Ransomware Attack over the globe and it was described as the massive attack among humanity. The customers privacy, IoT security requirements and security framework will establish the services provided by the IoT Environment (Nabil Kannoufb et al., 2020). Reports on the most advanced security countermeasures within the areas of autonomic, encryption, and learning-based approaches (S. Khanam et al., 2020). Security attacks which will influence on each IoT Architectural layers (S. Khanam et al., 2020). Evaluative look of security requirements must be noticed in IoT (Suha Ibrahim Al-Sharekh1 et al., 2019).

B. Work Flow

The work flow has been structured as follows. Section II offers Threats, IoT design, application domains for IoT. Section III provides all types of attacks in IoT. Section IV provides challenges and goals. Section V offers security countermeasures of IoT attacks in layers. Section VI provides limitations in devices, software, protocol and networks. Section VII provides open issues and research directions. Section VIII concludes the study.

Overview

The internet of things can have massive economic opportunities for various application domains like, healthcare, Industries, Education. As work from home is implemented in this pandemic era, the remote monitoring, future maintenance and connected devices with organization and home enables to have customer interactive technologies more with mobile apps and wireless gadgets which can reduce operational complexity, lower costs and increase the market time. IoT Security has a major concern in the business field with unique security and privacy. As the traditional IoT security have to concentrate more in operational and maintenance of end to end connectivity of devices environments to interact, login, send or receive data. Data breaches over the network connected devices, compromised by attackers become the interrupted services in case of video baby monitors and it is very much unreliable on things for the humans to trust in networks.

A. Threats

a. Botnet

IoT Botnets are compromised networks to inject malicious codes to the victim devices to make them bots by the bot herders. Security cameras are among the most concentrated and least protected IoT devices. Dark Reading's Ericka Chickowski said "2016 is going to be the year that attackers make a concerted effort to turn the Internet of Things (IoT) into the Botnet of Things." Internet of Insecure Things is providing for malicious actors who are always looking for new ways to break into networks to defraud organizations of their cash and valuable assets, or to harm opponents and competitors with a glimpse of various opportunities. As (R. Gurunath et al., 2018) various botnet attacks are phishing, sending span delivery, DDoS attacks, Identity theft which is compromised widely by IoT devices enormously. Hence, (J. Sathish Kumar & Dhiren Patel, 2014) the cyber criminals attack the IoT device due to default software configuration, irregular software updates and of outdated products.

b. Denial of Service (DoS)

Denial of Service will overload the target system with multiple requests send by attackers. DoS has not an aim to steal credential data like phishing and Brute – force attacks.

Attackers will simply slow down or disable the service provided by the organization to deactivate the process of the devices to extend the denial of their work to affect the revenue.

c. Remote Recording

Cybercriminals will record the conversations of IoT users. For example, an attacker will attack the smart camera in an organization and record video of everyday activities. They can obtain confidential information of an organization secretly. To mitigate this threat, the organizational leaders should create a cybersecurity policy before implementing the IoT ecosystem in their organization. For eradicating this kind of threat, the organization can ensure that the confidential datas are encrypted and the systems are audited regularly. Block chain, big data and AI could be extended to enhance the cybersecurity efforts of these kind of threats.

d. Ransomware

Ransomware has become one of the most crucial cyber threats. In this the hacker uses the malware to encrypt the data required and the attacker will decrypt data after receiving ransom.

e. Social Engineering

Hackers will access a system for installing malicious software. These types of attacks are accomplished using phishing emails where the attacker has to evolve persuasive emails. This is very easy to implement in IoT devices. Personally Identifiable Information (PII) is to collect in a massive amount especially in IoT wearable devices. Thus, in social engineering, the user data could be accessed illegally.

f. Man in the Middle

The hacker will intercept the messages communicated between two individual IoT devices. Attackers gain control over their communication and send unauthorized information to that particular IoT devices. In fact, these attacks are most common in industrial and medical instruments.

g. Identity and Data Theft

Hackers attack the confidential information such as personal details, credit and debit card credentials, and email addresses were stolen. Attackers can execute this kind of identity theft in organizations where smart watches, smart meters and smart home devices are being used. Data breaches are more now in business systems.

h. Advanced Persistent Threats

This kind of threat is a targeted cyber-attack in various organizations. The attacker will do illegal access to a network and will be there undetected for prolonged period of time. The aim of the attacker of this kind of threat is to monitor the network activity and steal the credential data. This type of threat is very difficult to prevent, detect or mitigate. Cybercriminals will target the IoT devices to gain personal or corporate networks. They can steal the confidential information of the organization.

B. IoT Architecture

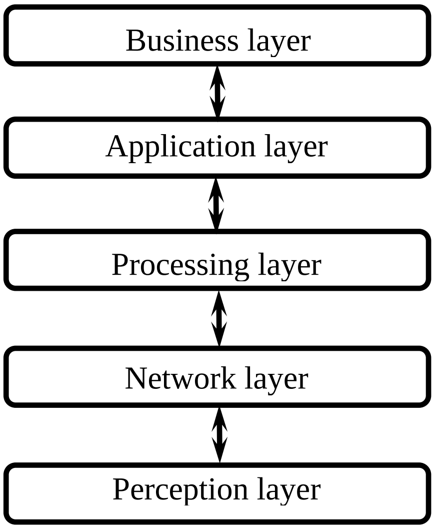

Fig. 1 Layers of IoT Architecture

a. Layers in IoT

The IoT architecture is made up of five layers. Perception, network, middleware, application, and Business layer is shown in figure 1.

i. The Perception Layer

It is also known as the physical layer, and it is made up of sensors that sense and collect data about the environment. It detects certain physical parameters or recognizes other smart objects in the environment.

ii. The Network Layer

The network layer serves as a link between the hardware and application layers, allowing devices to communicate with one another.

iii. The Processing Layer

A processing layer is also known as a middleware layer. It is constructed on top of the network layer. It has an API (Application Programming Interface) that can be used to create applications. Furthermore, it offers a variety of services to be accessed in this layer.

iv. The Application Layer

This layer has a user interface for the program. Web resources are consumed by applications in the application layer.

v. The Business Layer

It is the charge of all IoT systems. That layer is emerging and promoting the evolution of IoT applications. It should also manage and protect users' privacy in which the internet of things needs it.

b. Application Domains

Figure 2 represents the various application domains were IoT systems are implemented.

IoT suites have become an indispensable component of our everyday lives. This plug-ins is quickly evolving. IoT systems are susceptible to a variety of security, privacy, and agreement issues, which can affect everything from applications to the atmosphere and commerce. Actual security results must be implemented on each IoT domain, and they should be primarily based on functions.

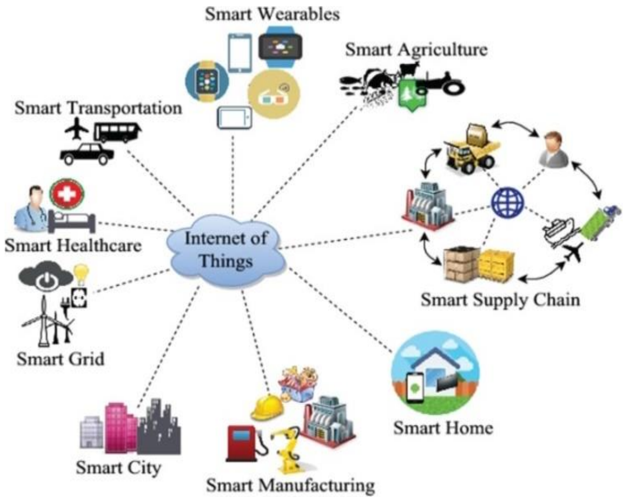

Fig. 2 Application Areas

i. Smart Home

A lot of the recent houses are outfitted with smart and programmed home hardware, along with brilliant lighting, fridge, washer, cool, electric meter, alert device and CCTV. For guaranteeing assurance and wellbeing, those houses are fuelled through smart cameras, sensors, smart bolts and caution frameworks. This home hardware might be worked from very large distance through internet. The various devices mounted in exciting houses would be secret word secured, and buyer login ought to be private.

ii. Industrial IoT

IoT that allows for remote monitoring, diagnosis, and control of physical processes and show output in real time. Industrial IoT and its goods, on the other hand, are closely linked to the internet of things. Many security issues affect digital entities, including confidentiality, anonymity, and trust. They also pose problems such as output standardization of the structure and public aspects. Due to a scarcity of resources the industrial IoT design necessitates low-cost, low-power infrastructures that are completely integrated.

iii. Smart City

IoT technologies in various sectors give rise to the idea of a smart city. Nevertheless, ensuring confidentiality and trust among stakeholders in this field is still a major concern.

iv. Health care IoT

In recent years, the treatment in hospitals and the facilities in remote healthcare have become increasingly common. There is a chance that the number of applications will increase. A patient's private and confidential details, on the other hand, may be stolen or exploited. Personal information about patients is private, so it's important to keep it safe from unauthorized access. If a patient's medical report is leaked and changed, the doctor can handle the patient incorrectly, which can be deadly and dangerous to the patient. The security and confidentiality of a patient's data are critical.

v. Smart Traffic

The IoT devices like sensors and RFID are most useful to make driving in enjoyable and traffic management system is more effective. An IoT-enabled traffic system may provide all traffic information. Passengers' data is at risk of being compromised when smart vehicles, buses, and trains, among other things become linked to the internet.

vi. Smart Grid

Smart grid is a smart electrical supply system that consists of a network of electric transmission lines, transmitters, and substations that deliver electricity from a power plant to homes and businesses. The main areas of concern that should be addressed are verification, privacy, confidence, reliability, and availability.

vii. Smart Farming

Consolidating different sensors and RFID advances, conventional horticulture, animals, and fish cultivating will get more intelligent in smart cultivating. Smart cultivating, then again, is helpless against various security concerns. On the off chance that the assurance of such applications isn't ensured, agricultural items might be harmed or fish and animals might be trucked away**.**

Classification of IOT Attacks

The IoT attacks for hardware, software, data and protocols are represented as given in figure 3.

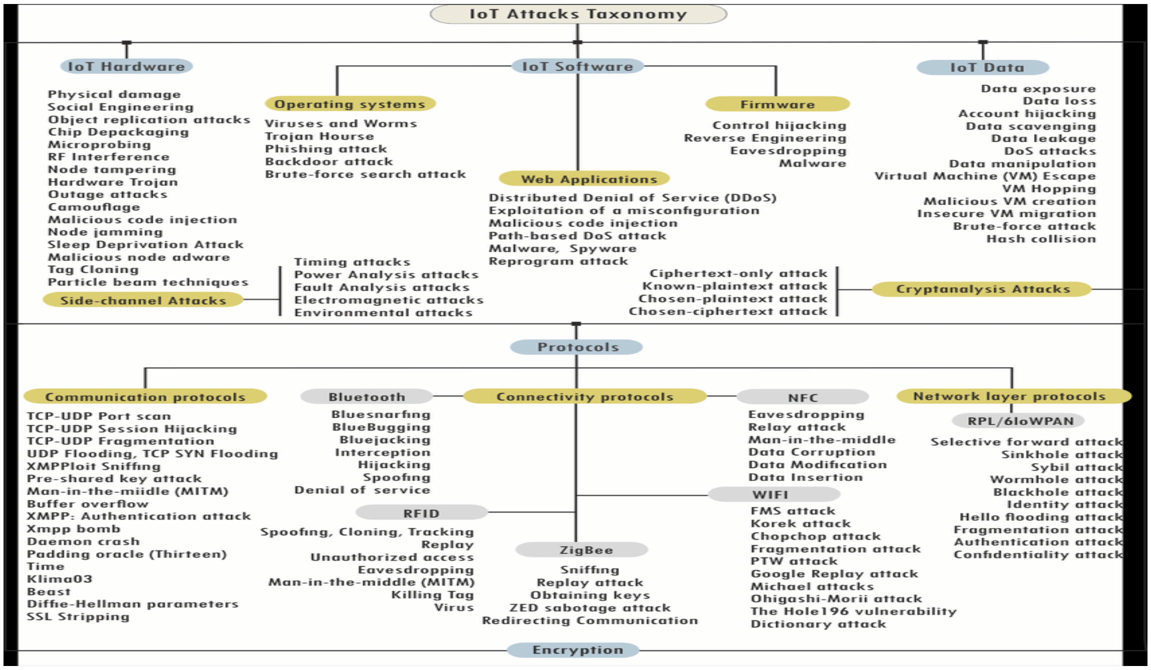

Fig. 3 Classification of IoT attacks

A. Hardware

Heterogeneous IoT devices are associated together among the framework. Based on the characteristics of the devices, the attacker may compromise it. Two such schemes for these devices are

a. Low Configured Device Attack

Devices with less memory storage, energy and computational abilities are considered as low-end configured devices. Using these low configured devices, the attacker uses other IoT devices.

b. High-End Device Attack

A very good quality device indicates to a potent and totally useful tool. An attacker may pose attacks to the high end devices (i.e., PC, laptop) with the expectation of causing damage to other devices and networks to provide a great loss ultimately.

B. Software

Some of the various software attacks in IoT are given below.

i. Botnets
ii. Man in the middle
iii. Data and Identity theft
iv. Social Engineering
v. Denial of Service

C. Protocols

The various devices in IoT may also have protocol attacks which may also disturb the devices by Malignant attackers.

a. Protocol Abnormality

A rival disruptions and merges from notable discussion or programmable protocols transform into an insider to have the option to report various bots.

b. Protocol Distraction

An attacker may likewise disturb boundless rules alongside synchronization, information collection or key management protocols from internal or external devices.

D. Networks

IoT System undergoes the various network attacks such as denial of service (DoS) and spoofing.

a. Denial-of-Service/Distributed (DoS) attack

This may not allow to work in devices, network or software and make provider unreachable to its operators. This can also additionally ascend in lot of forms. The attack could occur with the help of generating vast network traffic and propagation.

b. Spoofing

Spoofing is the communication from an unknown network as being from a known, depended on source. Spoofing can practice to emails, telecell smartphone calls, and websites, or technical, consisting of a pc spoofing such as IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

IoT Security

A. Goals

The principle security goals which plays a major role in existing systems are Confidentiality, Integrity (Q. M. Ashraf & M. H. Habaebi, 2015) which focus on securing keys, maintaining software integrity. Another important security goal is privacy (P. Vijayakumar et al., 2020) which provides location and data privacy. It also provides device privacy (Y. Kortesniemi et al., 2019) and Non- link- Ability (L. Garms & A. Lehmann, 2019).

Countermeasures of IoT Attacks in Layers

Countermeasures of IoT security attacks for various IoT layers could be explained in the table below.

i. Learning Method

Table 1 Various state of art learning based methods

Layers	Ref.	Learning method & type	Dataset	Objective	Advantage	Performance Accuracy	Limitations
Application	(H.-S. Ham et al., 2014)	SVM algorithm	-	Detect malware detection	Can outperforms well than other algorithms	-	-
	(A. Abeshu & N. Chilamkurti, 2018)	Deep Learning Methods	-	Detect Fog to things computing	-	Can have better than in shallow models in discovering precision, false alarm rate, and change of size	-
	(W. Fang et al., 2020)	Elman Neural Networking and the Support Vector Machine introduced (BPTT)	-	Time processing could be transformed.	-	-	-
	(M. E. Aminanto et al., 2018)	Three layered architecture	AWID	Impersonation attacks to be detected	The features preprocessing maybe done by SVM, DT, Artificial Neural Network.	SVM had better accuracy.	Longest training time.
Network layer	(G. Thamilarasu & S. Chawla, 2019)	Deep Neural Network (DNN)based Deep Belief Network (DBN) Method	Cooja simulator	Sinkhole attack, DDoS, Black hole, and Wormhole to be detected	Proposed Intrusion-detection system to monitor real-world intrusions	Precision 95% and recall 97% could be evaluated.	-

	(F. Y. Yavuz et al., 2018)	DL algorithm	Cooja developed IRAD dataset	Version number, Black hole, and Hello Flood attacks to be detected.	-	Accuracy 99.5% and F1-scores up to 99%	-
	(K. Alrawashdeh & C. Purdy, 2016)	Boltzmann machine (RBM) algorithm	-	DoS and probing attacks to be detected.	A softmax activation function performed to detect Multi-class intrusion detection	High accuracy of 97.9%	-
Physical layer	(T. Erpek et al, 2019)	Q-learning and Dyna-Q-based on RL	-	Physical-layer spoofing detection	A zero-sum spoofing detection game is used.	Environmental changes in which Spoofing detection is robust.	-
	(R. Vinayakumar et al., 2019; F. Y. Yavuz et al., 2018)	DNN	-	Jamming attack	The Protection system does not apply the information of the jammer.	-	-
	(W. Fang et al., 2020; M. Hasan et al., 2019)	Dynamic watermarking	-	Cyber attacks could be detected and prevented	A set of stochastic properties could be extracted from their IoT devices.	-	Authentication requires high computational resources.
	(N. Shone et al., 2018)	Channel-based machine learning	-	Clone and Sybil attacks to be detected.	-	Accuracy rate 84%	-

	(W. Fang et al., 2020)	An algorithm based on learning method	-	Side-channel attacks to be detected.	-	For high end detection the accuracy rate is 82% and for low end devices the detection accuracy is of 90% for IoT devices	-

ii. Autonomic Method

Researches proposed self-secure/autonomic approaches. Autonomous means 'self-sufficient' or 'self-healing' which prevent from random attacks. State of art autonomic methods for various security attacks in IoT system are discussed below.

Table 2 Existing state-of-the-art using autonomic methods

Layers or types	Reference	Title/ Intro	Aim/Objective	Explanation	Merits	Drawback
Application layer	(P. Kaur & S. Sharma, 2015)	MAPE design	Classification of Viruses or malware outlines.	By executing the mitigation service(s) it could be executed.	-	-
	(H. Alnabulsi, 2018)	Manufacturing mobile-IoT malware recognition	It could be analyzed based on Static, dynamic and hybrid methods	-	-	-
	(D. I. Wolinsky et al., 2013)	Hybrid method	Using various antivirus software the spyware could be identified.	Recognized on three factors: description mapping, interface study and source code analysis	Describe the malicious movements of an presentation .	-
	(J. Yang Koh et al.,	ELSA	Spoofing attacks	-	Uses statistical	-

	2013)				decision theory	
	(H. Alnabulsi, 2018)	GMSA	Program injection attacks	-	99.45% of Accuracy rate.	-
	(K. Bu et al., 2015)	Time-sensitive statistical relationship technique	Brute Force attacks	Pattern and its configuration to be analysed.	-	-
Network Layla	(M. N. Napiah et al., 2018	Compression header analyzer intrusion detection system (CHA-IDS)	-	Inspects compression header facts.	Eliminating attacks in 6LoWPA.	-
	(A. Le et al., 2016)	On behalf of Intrusion Detection System Partial-auto profiling RPL condition could be recognized		Secured from sinkhole attack	Low power consumption if the IDS executive shuts down	
Physical Layer	(A. Elngar, 2018)	Tamper Detection (TD) tool	-	Healthcare IoT requirements	Security damages to be disturbed	-
	(Q. M. Ashraf & M. H. Habaebi, 2015)	Autonomic system	-	Duty cycling and cognitive adjustment	Increase the lifetime of networks and secure the availability.	-

iii. Countermeasures based on Encryption

The countermeasures for securing IoT could be done using Symmetric and Cryptographic solution. For an encryption based countermeasure the three layered architecture of IoT is not applicable.

a. Cryptography based on Symmetric Key

Single key is shared for both sender and receiver for both encryption and decryption in secret key encryption process. There are various encryption distributions are obtainable.

b. Cryptography based on Asymmetric Key

AKC is an eminent, effective and protected method between nodes and similarly accepted as PKC. The sender encodes a message and receiver decrypts the message done by the use of his private key. It is a very dominant device to protected statement over the internet.

c. Cryptography based on Hybrid Key

The combination of both Symmetric and asymmetric cryptograms joined to form a cryptographic method denoted to as Hybrid Key Cryptography (HKC). Surviving hybrid systems are profitable for massive categorized networks that may consume the profits of both public and secret key patterns.

Limitations

IoT devices deals with many challenges and each challenge is mitigated in the manufacturer phase and the user phase. The following are the various limitations faced in software, hardware etc.

A. Networks

a. Multi-Protocol Networking

IoT devices use network protocols (comprising of non-IP protocol) to impart between close by networks. Simultaneously, it can state with a web provider by means of IP. These are numerous highlights of the communication protocols on the web of things, making customary security plans unseemly for IoT devices.

b. The Diversity of Devices

IoT devices are an assortment in the IoT networks, going from full PC to low radio frequency identification. Thus, it is elusive a solitary security device that can oblige any remaining devices.

c. Dynamic Network Topology

IoT devices can be a portion of network. These temporal and spatial gadgets make the network topology a unique one. Hence, the modern security of the network doesn't manage this abrupt kind of topological changes, and this model doesn't agree with the IoT smart devices and doesn't correspond to its security.

d. Mobility

The most obvious highlights and attributes of IoT devices is the versatility include that suggests these devices be a portion of close and proximal group without past setup. As a result of this nature of portability, we need to raise flexible security designs and works in IoT devices.

B. Software

a. Active Security Patch

The way toward declining and lessening the flaws of the IoT devices, and the way toward introducing viable security programming on IoT devices is definitely not a direct errand. Distant reinventing may unrealistic for the devices of IoT because of protocols and operating systems, so it's anything but ready to get codes and another library.

b. Embedded Software Limitation

Operating systems of IoT that implanted in IoT devices have thin network protocols and may lack entity security. The security module should be for insufficient protocols.

C. Hardware

a. Tamper Resistant Packaging

IoT devices may be installed in isolated areas and it was not used, the attacker may inject the malicious programs to make it tamper the devices also extract encryption secrets.

b. Memory Restriction

IoT devices have RAM and flash memory which is limited in contrast with customary devices like PC frameworks and utilized as a light-weight model of General-Purpose Operating System. Consequently, protection plans ought to be unbelievably productive for memory. In any case, conventional security algorithms are not intended for memory productivity in light of the fact that customary frameworks utilize huge RAM. Therefore, in IoT devices security plans might not have sufficient memory space because of their little size. Accordingly, conventional traditional plans can't be utilized to consistent the IoT devices.

D. Communication Devices

IoT devices are things indulged and consequently, customary security systems are not exact in Internet of Things.

a. Memory Dimensions

Limited devices utilize Random Access Memory (RAM) to save information and skill among a couple of kilobytes and 12 kilobytes. Information storing in the IoT devices is restricted, and a couple of devices can't save or send data.

b. Energy Capacity

It is the amount of energy the devices have to maintain itself over a specified period. The energy sources in the devices are limited and need to be replaced after a particular time. Some IoT devices consume large amounts of power and are not rechargeable. Therefore to save the battery in limited devices, low-bandwidth connections are being used.

c. Processing Limit

The processing limit alludes to the measure of energy in the devices. Numerous IoT devices are tiny, minimal expense with low processing limit. Accordingly, these devices require lightweight protocols to work competently.

Discussions

In this section, the discussions could be analyzed in the countermeasures of security measures addressed in the key security issues and point out the domain that demand further research. Also this section presents the discussion on implementation challenges and recommends upcoming research guidelines for future scientists.

A. Countermeasures Methods

The existing countermeasures discussed about the advantages and its commutations are:

a. Learning Measures

This techniques mainly based on performance matrix. Machine learning and Deep learning algorithms are used to perform the high accuracy rate. Some of the algorithms like Decision tree, SVM and Naïve Bayes classifiers are used to classify the intrusions incorrect manner. Mostly Deep learning algorithms are mainly used to train the massive datasets to find out the hidden layers accurately with high performance than machine learning algorithms. The dataset used to train the ML and DL algorithms should be realistic otherwise will produce massive false-positive rates.

b. Autonomic Approaches

An autonomic architecture is an advantage of an autonomous approach in which the different tasks are to be accomplished to discover and diminish attacks. Human physical intervention is low in this approach. In CIA triad to achieve this self-security is integrated between software and network of an IoT environment. For self-repairing mechanism some complex cognitive structures are provided. It is a biggest challenge among researchers to automate the system completely.

c. Encryption Algorithms

The light duty nodes of asymmetric cryptography will provide the performance inefficiency. More research is undergoing to improve energy supply among IoT devices. To make the IoT stronger, security by encryption techniques is a major research direction for heterogeneous environments.

B. Challenges in Implementation

In remote areas, IoT devices are deployed which may undergo physical layer attacks. To implement complex and robust communication protocols among these devices is not possible. It is incredible to implement the securing and autonomic security architecture due to the limited resources characteristics of IoT features.

C. Open Issues and Research Directions

The state of art presents major issues in IoT which might be very complex to find solutions. In fact, usage of devices is massive in this pandemic era. Attacks could be reduced and produce a unified security system or an integrated security model as a future scope. Our findings and future directions could be outlined below.

- Security concern is a vital role while manufacturing the devices which has weak, speculate or Embedded Credentials, hardware problems, Insufficiency in secure upgrade technique, old and repaired embedded operating systems and software, uncertain information transfer and storage could be highly concentrated in research.
- Lack of user knowledge and Awareness about the IoT devices and its functionality is still more concentrated to have better insights among the users.
- Device management is one of the security issue. Manufactures will install the device with software update before selling the product. The need of the software updates can run automatically in devices. As per the literature some of the old IoT devices are not automatically updated which will perhaps enter into a security issue. A hacker can steal the information if the connection is unencrypted and updated files are unprotected. It will also suffer a short downtime of the device as after the update. To overcome this issue in future it should reach the cloud to retain backup of communications between devices.
- IoT devices can run automatically without human intervention. Some of the devices could be kept in remote locations which will undergo threat. This issue could be concentrated by the manufacture to ensure the physical security. Perhaps, users could also have to secure some smart devices with proper insights about the devices and functionality of IoT systems.
- The single IoT devices affected with malware will not have real time threat. When this botnet attack happens it will inject malware to all devices in that network. IoT devices are highly vulnerable to malware attacks. The devices all turned into infected zombies which will send multiple requests and respond to the network in which the IoT devices are connected. To mitigate this issue in future, proper detection model should be implemented with suitable machine learning and mining based techniques.
- As per literature, it was found that Spying and Intruding the IoT devices is a vital issue as much information may be compromised and employ against the owner. Many IoT devices record user information it could be spied and hacked by hacker to expose the secret information of an organization. Proper security solution could be implemented to eradicate this issue to safeguard the organization devices and information from hackers in a most appropriate way as a future research.
- Rouge devices are malicious IoT devices which can steal credential information, also will damage permanently the IoT system. To overcome this issue in future, researchers could find proper detecting tool to implement with care in an organization.

- Crypto-mining is a type of bot which involves infected botnets aimed at IoT devices, with the goal not to create damage, but mine crypto-currency. Researchers doing research in this issue to stop crypto-miners. Lopez-Penalver says it would be something like a well-trained neural network, some security vendors are using machine learning and other artificial intelligence (AI) technologies to spot the behaviors that indicate crypto mining as a future research.

Conclusion

An IoT security, it's allowing technologies, and comparing the elements associated with employing a widespread security method in IoT with conventional internet have been discussed. The main aspect of this survey is primarily based on IoT design. Attack classification and evaluations have also been furnished. Moreover, the various factors associated with the ability and difficulties of IoT have been analyzed. The security goals of the existing system also been implemented.

In contrast to different existing research, various innovative security countermeasures are being guaranteed for high protection for IoT which will bring novelty to the future research work. This survey could be very much useful for the researchers to understand the various attacks existing in IoT. An existing techniques, execution tasks and upcoming investigation guidelines can also be poured in this survey. Several researchers have seasoned modelled trivial arrangements for IoT, yet further research effort is required to plan universal, integrated, and well matched security countermeasures for IoT.

References

Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A., & Fartitchou, M. (2020). IoT security: challenges and countermeasures. *Procedia Computer Science*, *177*, 503-508.

Amaral, L.A., Hessel, F.P., Bezerra, E.A., Corrêa, J.C., Longhi, O.B., & Dias, T.F. (2011). eCloudRFID–A mobile software framework architecture for pervasive RFID-based applications. *Journal of Network and Computer Applications*, *34*(3), 972-979.

Yan, Z., Zhang, P., & Vasilakos, A.V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications*, *42*, 120-134.

Svensson, G. (2013). Auditing the human factor as a part of setting up an information security management system. KTH, Stockholm, Sweden, Tech. Rep., 2013.

Frangopoulos, E.D., Eloff, M.M., & Venter, L.M. (2013). Psychosocial risks: Can their effects on the security of information systems really be ignored?. *Information Management & Computer Security*, 21(1), 53-65.

Mohanta, B.K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*.

Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K., & Shieh, S. (2014). IoT security: ongoing challenges and research opportunities. *In IEEE 7th international conference on service-oriented computing and applications*, 230-234.

Nabil Kannoufb, Khalid El Makkaouic, Abdellah Ezzatia, Mohamed Fartitchouc, Mohamed Litoussia, “IoT security: challenges and countermeasures”, The 7th International Symposium on Emerging Information, Communication and Networks (EICN 2020) Madeira, Portugal, Nov. 2 - 5, 2020.

Khanam, S., Ahmedy, I.B., Idris, M.Y.I., Jaward, M.H., & Sabri, A.Q.B.M. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. *IEEE Access*, *8*, 219709-219743.

Al-Sharekh, S.I., & Al-Shqeerat, K.H. (2019). Security challenges and limitations in iot environments. *IJCSNS International Journal of Computer Science and Network Security*, *19*(2), 193-200.

Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018). An overview: security issue in IoT network. *In 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 104-107.

Kumar, J.S., & Patel, D.R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, *90*(11).

Ashraf, Q.M., & Habaebi, M.H. (2015). Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, *49*, 112-127.

Vijayakumar, P., Obaidat, M.S., Azees, M., Islam, S.H., & Kumar, N. (2019). Efficient and secure anonymous authentication with location privacy for IoT-based WBANs. *IEEE Transactions on Industrial Informatics*, *16*(4), 2603-2611.

Kortesniemi, Y., Lagutin, D., Elo, T., & Fotiou, N. (2019). Improving the privacy of iot with decentralised identifiers (dids). *Journal of Computer Networks and Communications*, *2019*.

Garms, L., & Lehmann, A. (2019). Group signatures with selective linkability. *In IACR International Workshop on Public Key Cryptography*, *Springer*, 190-220.

Ham, H.S., Kim, H.H., Kim, M.S., & Choi, M.J. (2014). Linear SVM-based android malware detection for reliable IoT services. *Journal of Applied Mathematics*, *2014*.

Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine*, *56*(2), 169-175.

Fang, W., Tan, X., & Wilbur, D. (2020). Application of intrusion detection technology in network safety based on machine learning. *Safety Science*, *124*.

Aminanto, M.E., Choi, R., Tanuwidjaja, H.C., Yoo, P.D., & Kim, K. (2017). Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. *IEEE Transactions on Information Forensics and Security*, *13*(3), 621-636.

Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors*, *19*(9).

Yavuz, F.Y., Ünal, D., & Gül, E. (2018). Deep learning for detection of routing attacks in the internet of things. *International Journal of Computational Intelligence Systems*, *12*(1), 39-58.

Alrawashdeh, K., & Purdy, C. (2016). Toward an online anomaly intrusion detection system based on deep learning. *In 15th IEEE international conference on machine learning and applications (ICMLA)*, 195-200.

Erpek, T., Sagduyu, Y.E., & Shi, Y. (2018). Deep learning for launching and mitigating wireless jamming attacks. *IEEE Transactions on Cognitive Communications and Networking*, *5*(1), 2-14.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, *7*, 41525-41550.

Yavuz, F.Y., Ünal, D., & Gül, E. (2018). Deep learning for detection of routing attacks in the internet of things. *International Journal of Computational Intelligence Systems*, *12*(1), 39-58.

Fang, W., Tan, X., & Wilbur, D. (2020). Application of intrusion detection technology in network safety based on machine learning. *Safety Science*, *124*.

Hasan, M., Islam, M. M., Zarif, M.I.I., & Hashem, M.M.A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, *7*.

Shone, N., Ngoc, T.N., Phai, V.D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), 41-50.

Fang, W., Tan, X., & Wilbur, D. (2020). Application of intrusion detection technology in network safety based on machine learning. *Safety Science*, *124*.

Kaur, P., & Sharma, S. (2015). Spyware detection in android using hybridization of description analysis, permission mapping and interface analysis. *Procedia Computer Science*, *46*, 794-803.

Alnabulsi, H., Islam, R., & Talukder, M. (2018). GMSA: Gathering multiple signatures approach to defend against code injection attacks. *IEEE Access*, *6*, 77829-77840.

Wolinsky, D.I., Syta, E., & Ford, B. (2013). Hang with your buddies to resist intersection attacks. *In Proceedings of the ACM SIGSAC conference on Computer & communications security*, 1153-1166.

Koh, J.Y., Ming, J.T.C., & Niyato, D. (2013). Rate limiting client puzzle schemes for denial-of-service mitigation. *In IEEE Wireless Communications and Networking Conference (WCNC)*, 1848-1853.

Bu, K., Xu, M., Liu, X., Luo, J., Zhang, S., & Weng, M. (2015). Deterministic detection of cloning attacks for anonymous RFID systems. *IEEE Transactions on Industrial Informatics*, *11*(6), 1255-1266.

Napiah, M.N., Idris, M.Y.I.B., Ramli, R., & Ahmedy, I. (2018). Compression header analyzer intrusion detection system (CHA-IDS) for 6LoWPAN communication protocol. *IEEE Access*, *6*, 16623-16638.

Le, A., Loo, J., Chai, K.K., & Aiash, M. (2016). A specification-based IDS for detecting attacks on RPL-based network topology. *Information*, *7*(2), 25.

Elngar, A.A. (2018). IoT-based Efficient Tamper Detection Mechanism for Healthcare Application. *Int. J. Netw. Secur.*, *20*(3), 489-495.

Ashraf, Q.M., & Habaebi, M.H. (2015). Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, *49*, 112-127.