Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

The Security Challenges In The World Of Internet Of Things

D. Janet Ramya[1] , Dr. L. Arockiam[2]

[1]Research Scholar in Computer Science, St. Joseph's College(Autonomous), [Affiliated to Bharathidasan University] Tiruchirappalli, Tamilnadu, India.

[2]Associate Professor in Computer Science St. Joseph's College(Autonomous), [Affiliated to Bharathidasan University] Tiruchirappalli, Tamilnadu, India.

Abstract:

The Internet of Things (IoT) spans a vast network of numerous smart devices be it simple or complex. They regularly exchange data over the Internet. The momentous growth of IoT as a new technological paradigm exposes many secure-critical operations and sensitive data online. So, security of the device, its operations and data are equally at risk. This paper studies the various security issues in the IoT environment. The IoT architecture is prone to many design-level, service-level, network-level and application-level threats. Possible attacks and countermeasures have been summarized layer wise to visualise the big picture. Thus, provides better awareness of the risk of security blemishes and also may protect and safeguard the IoT environment.

Keywords – Security, Internet of Things, Architecture.

I. INTRODUCTION

The Internet of Things (IoT) is a dynamic worldwide network architecture with automatic configuring capabilities based on standard and interoperable communication protocols in which physical and virtual "things" have their own identities, physical characteristics, employ intelligent interfaces, and virtual behaviours and are seamlessly linked into the information network, and frequently transfer data related with users and their environments [1]. It comprises of physical and virtual things or objects which have unique identities when connected to the internet to make a 'smarter' environment. IoT is a fast-growing technology which is gaining momentum day by day and it is driven by many technologies which complement it such as sensor networks, wireless communication, mobile devices, cloud technologies and networking. The Gartner's Hype cycle [2] anticipates that there would be more than 25 billion uniquely identifiable objects in the forthcoming global networking era. IoT is going through the peak of inflated expectations and the need for security of these interconnected devices is also

increasing. IoT is a fusion of heterogeneous networks which involves many kinds of security and privacy issues. When nearly 25 billion devices are connected, this constant exposure of things will divulge security flaws and vulnerabilities to the hackers and the weaknesses may be mistreated in the IoT environment. The world of IoT includes wide range of devices and diverse applications, which are deployed in different scenarios and the security requirements of these devices, differ in each paradigm. Therefore, new security and privacy issues arise and resolving these issues might create a better world for the IoT environment.

II. SECURITY REQUIREMENTS OF IOT [3][7]

A. Confidentiality: Confidentiality ensures that the data is accessible only by authorised users all over the process and not tampered or eavesdropped by unauthorized users. A loss of confidentiality is termed as unauthorised disclosure of information. When large numbers of IoT devices are integrated, Confidentiality of these connected things becomes a major necessity.

B. Integrity: Integrity ensures the data transmitted over networks, is not tampered by any 3rd party and provides data accuracy for authorized users in the long run. If the data transmitted is forged or tampered then the erroneous data will be received and wrong feedbacks will further disrupt the IoT operations. A loss of integrity means that the unauthorised modification or destruction of data.

C. Availability: When the data and devices are available when users request it, availability can be ensured. Services cannot be scheduled if they are not provided to the user in a timely manner. Nowadays, Denial of Service (DoS) is the one of the most common attacks. A loss of availability is when the service access is interrupted and information cannot be obtained.

D. Identification and Authentication:

Identification ensures that only authorised devices and applications can connect to network of things. Authentication assures that the data distributed in the network are genuine to the devices or applications. Cisco[4] has reported that by 2020 there will be 50 Billion devices interconnected in the IoT network. Identifying and authenticating each and every device is a major challenge in the IoT environment. Thus, each input arriving at an IoT device should be from a trusted source.

E. Privacy: Individuals have entire control of the data collected and stored related to them. They are decisive and influential over whom the information must be disclosed to. Privacy ensures full control over data corresponding to user but restricts control over information received. Privacy is one of the key objectives of Security since all the devices existing in the IoT environment share the same communication network.

F. Trust: Trust is the basis of all the above-mentioned security and privacy objectives. This is achieved through all the IoT layers and applications. The End-to-End Trust covering trust between devices, trust between all the IoT layers, trust between devices and applications, and altogether enforces trust as a whole in the IoT environment.

III. IoT SECURITY ARCHITECTURE

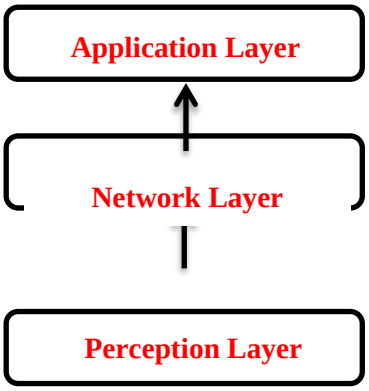

FIG. 1. GENERIC ARCHITECTURE OF IOT

Generally, 3 key layers form the IoT Architecture as given in above Fig. 1, which is described below.[9]

A. Perception Layer:

It is also called as the sensing layer, which is the lowest layer in IoT architecture. The main concern of this layer is to interact with physical devices and components through different kinds of RFID (Radio Frequency IDentification), sensor networks and Barcodes [5][6]. The basic purpose of the layer is the intelligent connectivity between sensor nodes facilitates the exchange of information.

As the perception layer in IoT focuses on collection and processing of data, forging of data is a vital threat which is discussed below in Table I.[8][9]

TABLE I SECURITY ISSUES IN PERCEPTION LAYER.

Security Threats	Description	Countermeasures
Unauthorised Access to the Tags	Lack of proper authentication mechanism of RFID tags or systems, they may be accessed by unauthorised users. The data can be read, altered and even deleted.	Enforce strong Authentication mechanisms.
Tag Cloning/ Node Capture Attacks/ node replication attack	Tags are visible and can be read and modified easily, the attacker creates a replica of the tag and the reader may fail in distinguishing	

	between the original and the compromised tag.	Effective schemes are to be built to monitor & detect malicious nodes.
Spoofing	By broadcasting false information to the systems and making it look like as if it has originated from trusted source and the attacker can gain access of the entire system and makes it vulnerable.	
Eavesdropping	The data flow between the tag-reader or reader-tag is wireless and the attacker sniffs the information such as passwords and attacks the device.	Improvised multi-level secure encryption algorithms and quantum proof key management schemes are required.
Malicious code Injection Attacks	When unauthorised access to node is made the attacker injects malicious code to the memory of the system and gains full control over the system.	Effective code authentication schemes are required.
False Data Injection Attacks	Attacker may inject false data in the place of original data and may transmit the false data and may lead to IoT applications returning false services and erroneous commands.	False data cleaning schemes to sense and drop false information before it reaches the end point devices is required.
Replay Attacks/ Freshness Attacks	The attacker node may transmit false data to the destination host with genuine identity and repeats the same process in the network to obtain trust in the network.	Secure time stamp schemes need to be built in.
Cryptanalysis Attacks	During cryptanalysis, the attacker looks for vulnerabilities and information leaks and uses the cipher text or the plaintext to acquire the encryption key used in the encryption algorithm.	Enhanced end to end security mechanisms for encryption and key management are good alternatives.
Side Channel Attacks	The attacker targets data by exploiting information related to execution and compromises the system.	Eliminating data leaks and unlinking the secrecy in the information.
Sleep Deprivation Attacks	In IoT network, most of the devices are low powered with short lifecycle. So, the devices are	Nodes can be provided with energy from the external

	automated to follow some sleep sequences to lessen the power consumption in order to extend the life cycle. The attacker breaks through these sleep routines and keeps the devices awake so that they can shut down soon.	environment and Duty-cycle mechanisms can be built in.

B. Network Layer:

The network layer comprises of Wireless Sensor Networks (WSN) which transfer data collected from sensor devices to its destination. This is the most targeted layer among the WSN, since they depend mostly on secure routing and privacy of data being transmitted. Threats may compromise the devices in the entire network and this is a major challenge in IoT environment. As the network layer in IoT focuses data transmission, forging of identities, loss of data are major concerns which are discussed in Table II.[4][8][9]

TABLE II SECURITY ISSUES IN NETWORK LAYER

Security Threats	Description	Countermeasures
Sybil Attack	Here the attacker creates many false identities for a single node and the system results in false information about redundancy.	An intelligent identity management mechanism is to be followed.
Sinkhole Attack	The adversary attracts the neighbour nodes and diverts all attention towards the compromised node.	Multiple routing protocols with higher level security needs to be applied.
Denial of Service(DoS)	DoS attacks devour all the available resources in IoT and then attack the network or bombard the IoT network with enormous traffic, making the requested services unavailable to the IoT systems.	The attacking schemes in DoS attack need to be investigated to provide efficient defensive schemes to mitigate the attacks.
Malicious Insider	This attack befalls when someone from the inside tampers with the data seeking some personal benefits or for the benefits of any 3rd party.	Techniques to detect and eliminate nodes whose energy, packet delivery ratio, throughput have sudden fluctuations
Malicious Scripts	Since many IoT applications and devices are always connected to the internet, it is	Effective Script detecting schemes are to be deployed.

	an added advantage to the adversary to run malicious scripts when the user requests for services.	
Man-in-the-Middle Attack	This attack is triggered when the attacker has full control over a malicious device and is found to be located in-between 2 communicating IoT devices[13].	Efficient defence techniques are to implemented to protect against the attack by securing communication protocols and key management schemes in a manner to ensure the identity and key information of resource constrained devices from being leaked to the adversary.
Spoofing Attack	By gaining complete access over the IoT system the adversary sends malicious data into the system.	Trust management, identification and authentication should be strengthened to defend against the such attack.
Wormhole Attack	The attack arises when 2 cooperative malicious devices or IoT nodes, exchange routing related information irrespective of their locations by using private links in order to achieve one-hop transmission between them.	By enhancing the routing protocols in a way to boost the route selection process this attack can be eliminated.
Routing Information Attack	This attack focuses on routing protocols and manipulates the routing information and resends it to create route loops in the data transmission of the network	Secure routing among protocols and trust management is to be established between IoT devices through secure communication links.
Gateway attack	The connection between the sensors and the Internet infrastructure is limited or shut down by this kind of attack. This in-turn would jeopardize the internet infrastructure.	Securing the gateway with intelligent intrusion detection system

Storage Attack	Enormous amount of user data is stored in IoT devices or in cloud storages. When storage attacks take place the user data may be compromised.	Monitor and limit the data transfer from device to device, device to gateway and device.
Selective Forwarding	When an adversary-controlled node is decisive about the packets to forward and sends a few but drops most of the packets from sender to receiver then issues arise on unorganised packet delivery.	To detect the malicious node same packets are sent through multiple paths and ordering the packets in a fashion can be done.
Hello Flood Attack	The attacker's node broadcasts Hello packets to all other nodes in the network and when the nodes receive this hello packet, they assume that the sender is a neighbour node and adds it in its routing table.	This could be prevented by following bidirectional verification and verifying if the sender is in the radio range or not.
Acknowledgment spoofing	When the attacker node spoofs the ACK packet on overhearing packets being delivered to a weak or dead node then the sender assumes the node sending the ACK packet is live and in range.	This can be prevented by encrypting the message and by verifying the packets through sequence numbers.

c. Application Layer:

The responsibility of this layer is to provide all the user requested services on time. Each device has its own software and hardware vulnerabilities which make it prone to attacks. They should be power efficient and should recharge quickly so as to keep the device active.

As the application layer in IoT relies on device constraints and offering user services, delay in rendering the services to all types of devices is a drawback which is discussed in Table III [8][9]

TABLE III SECURITY ISSUES IN APPLICATION LAYER

Security Threat	Description	Countermeasure

Jamming	The adversary interrupts the radio signals and cuts off the communication channel between the devices and network causing congestion in the communication channels.	The spread spectrum techniques can be deployed.
Loss of Power	IoT devices operate on low power environments since they have resource constraints. The battery life is important to keep the device active.	Power saving modes, hibernation modes can be used as an alternative.
Physical tampering	Tampering the devices and causing damage to it by replacing the device physically, extracting essential data and controlling the device is possible.	Self-destructive nodes can be designed to destroy all memory once the device is being tampered.
Malicious Code Injection	The attacker may use all possible hacking techniques and inject malicious code in the end users device.	Restrict access control and validate users' data input
Denial-of-Service (DoS) Attack	Non- encrypted personal data, messages of user can be at risk in the hands of the attacker/hacker.	End to end encryption should be enabled for protecting user info and messages.
Phishing Attack	In the phishing attack the user credentials maybe spoofed by vulnerable site access and emails.	Secure Authentication, identification and Authorization may prevent these kinds of attacks.
Spear-Phishing Attack	The users' email is spoofed when the user logs in to his/her mail, the attacker overhears it and captures the credentials and steals vital data of the victim.	Invalid login alerts and device logged in details are to be provided to the user on each activity.
Sniffing Attack	An attacker forcibly introduces a sniffer into the IoT application and ends up corrupting the entire system.	Enhancing firewalls to block applications that use insecure protocols.
Malicious Virus/worm	The adversary may tamper with the IoT applications by triggering malicious proliferation attacks such as	Firewalls and virus recognition mechanisms should be deployed.

	worms, horse, trojan etc., and alter user's confidential data.	

IV. SECURITY CONSIDERATIONS FOR IOT

There are many solutions available but the most viable and efficient ones will always grow as the trend and new security issues rise. A few specific security considerations to strengthen the IoT devices are given below.[10][11]

a. Identification and Authentication: Global ID schemes which eliminate the traditional centralised nature will be an effective alternate to be considered when intelligent objects and humans interact. Also, effective identity management approaches which are distributed and decentralised should be developed. Further open research challenges exist in areas such as mobility, privacy, pseudonymity, anonymity aspects need deeper.
b. Privacy: Automating key management scheme is very sensitive and still a booming issue when it comes to privacy concern in IoT. It encompasses key provisioning, updating, revocation, transporting and key agreement. Non-cryptographic operations like enrolment, backup and recovery, firmware updates should be addressed to achieve high level of security. Also, open grounds to develop new schemes using blockchain based smart contracts for asymmetric key management including generation, validation and distribution. This in turn will achieve decentralised public key Infrastructure and enhanced CIA (Confidentiality, Integrity, Availability) metrics.

c. Architecture Standards: IoT is in the verge of defining a self-sovereign environment which comprises of data models, interfaces, and protocols which can support a wide range of heterogenous devices, operating systems and languages.

d. New security challenges and applications of lightweight cryptography, threshold cryptography, blockchain solutions for IoT needs to be inculcated further.

From the above study made the conclusive requirements and countermeasures are summarized in the table IV for each layer. [12]

TABLE IV. SUMMARY TABLE OF IOT SECURITY CONSIDERATIONS

IoT Layer	Task Performed	Key Components	Security Issues	Security Requirements	Countermeasures
Perception Layer	Collection of Data from various end devices	Smart Card, RFID tag, Sensor Networks	Security of the sensor networks	• Lightweight Encryption • Access Control • Data structures and format	• Lightweight encryption schemes are to be developed. • Protecting sensor data • Key agreements

Network Layer	Transmission of Data	Wired or Wireless network	Security during data transmission	• Communication, Routing and Connectivity Security • Mechanisms for Cross-domain Data Security Handling • Secure Sensor/Cloud Interaction	• Identity authentication • Encryption mechanism • Anti DDoS measures • Communication security policies
Application Layer	Data Analysis and Decision Making	Intelligent devices and applications	Security while processing data	• Privacy Protection and Policy Management • Application-specific Data Minimization • Authentication measures • Application specific encryption, cryptography. • Authorization, Assurance	• Authentication and key agreement • Privacy protection mechanisms • Security education and management techniques • End to End Encryption.

V. CONCLUSION

Today's IoT devices are insecure and not efficient enough to defend themselves. The hype cycle has created a fast-growing network of IoT devices and as things get smart, ways to secure them needs to be smarter. The huge amount of data being shared among these devices should be preserved with respect to the security considerations of each layer. This paper summarizes most of the attacks which occur at various layers. The countermeasures are not limited but paves way to widen the possible solutions.

REFERENCES

[1] A. Bahga and V. Madisetti, Internet of Things: A Hands-On Approach. VPT, 2014.
[2] CLIENT RESEARCH IoT's Challenges and Opportunities in 2017: A Gartner Trend Insight Report Mark Hung, April 2017. Available online : https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[3] W. Stallings, “Cryptography and Network Security: Principles and Practice”, 8th Edition p. 900.
[4] Cisco, U. "Cisco annual internet report (2018–2023) white paper." Cisco: San Jose, CA, USA (2020).
[5] Khattak, Hasan Ali, Munam Ali Shah, Sangeen Khan, Ihsan Ali, and Muhammad Imran. "Perception layer
security in Internet of Things." Future Generation Computer Systems 100 (2019): 144-164.
[6] V. Adat and B. B. Gupta, “Security in Internet of Things: issues, challenges, taxonomy, and architecture”, Telecommun. Syst., vol. 67, no. 3, pp. 423–441, Mar. 2018.
[7] Čolaković, Alem, and Mesud Hadžialić. "Internet of Things (IoT): A review of enabling technologies,
challenges, and open research issues." Computer networks 144 (2018): 17-39.
[8] Ahmad, Mudassar, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, and Syed Hassan Ahmed. "A
review of current security issues in Internet of Things." Recent trends and advances in wireless and IoT-
enabled networks (2019): 11-23.
[9] Abdullah, Aishah, Reem Hamad, Mada Abdulrahman, Hanan Moala, and Salim Elkhediri. "Cyber Security: a
review of Internet of Things (IoT) security issues, challenges and techniques." In 2019 2nd International
Conference on Computer Applications & Information Security (ICCAIS), pp. 1-6. IEEE, 2019.
[10] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The Effect of IoT New Features on Security and Privacy:
New Threats, Existing Solutions, and Challenges Yet to Be Solved,” IEEE Internet Things J., vol. 6, no. 2,
pp. 1606–1616, Apr. 2019.
[11] B. Javed, M. W. Iqbal, and H. Abbas, “Internet of things (IoT) design considerations for developers and
manufacturers,” in 2017 IEEE International Conference on Communications Workshops (ICC Workshops),
Paris, France, 2017, pp. 834–839.
[12] Bashir, Adil, and Ajaz Hussain Mir. "Internet of things security issues, threats, attacks and counter
measures." International Journal of Computing and Digital Systems 7, no. 02 (2018): 111-120.
[13] Prathibha, L., and Kaleem Fatima. "Exploring Security and Authentication Issues in Internet of Things."
In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), pp.
673-678. IEEE, 2018.