Received: Dec '22
Revised:
Accepted: Jan '23

SECURITY AND PRIVACY ARE OBSTACLES IN IOT DEVELOPMENT & DESIGN

Dr. Vishal Pareek[1] and Mr. Ram Kumar Vyas[2]
[1]Associate Professor, Department of Computer Science, Tantia University, Sri Ganganagar (Raj.), India
[2]Research Scholar, Department of Computer Science, Tantia University, Sri Ganganagar (Raj.), India

ABSTRACT

The concept in the back of the Internet of Things (IoT) is that ordinary items may want to hook up with the net and have interaction with each other to shape intelligent, self-configuring systems. Security and privateness are nevertheless regarded as widespread barriers to the variation and development of IoT strategy, regardless of the blessings of IoT development. Safety and privateness matters are the maximum widespread impediment that desires to be resolved at every IoT layer however hasn`t been. Security-associated problems had been addressed with the aid of using several studies. A suitable safety framework ought to cope with IoT layer-safety problems to shield the technology. This article presents a top-level view of IoT privateness and safety problems. Additionally, it emphasized some of advised answers and safety necessities which might be applicable to the IoT context.

INTRODUCTION

The Internet of Things (IoT) is essentially a network of a number of interconnected things (nodes) that can communicate with one another and exchange data in order to perform common tasks. An object could be a person, a phone, a door, a car, an animal, or anything else you can think of. A sensor is attached to each object, enabling it to communicate with its surroundings. In order to organize, process, and store data, IoT connects devices from the consumer, commercial, industrial, and government sectors. It can be used for energy, healthcare, and transportation in multiple ways. The Internet of Things (IoT) is defined by the ITU-T as "global infrastructure for society, allowing improved services by linking (physical and virtual) things based on existing and emerging interoperable information and communication technologies." The Internet of Things (IoT) is a new Internet revolution that will alter our daily lives. It makes it possible for the intelligent devices that are all around us to do the things we normally do.

Almost the entirety we engage with could be capable of talk and connect with the net way to destiny technology. New phrases like "clever city," "clever home," and "clever workplace" have emerged due to the Internet of Things (IoT).

Gartner predicts that there will be more than 50 billion connected IoT devices by 2020, up from about 25 billion today. The diverse makeup of this huge network creates new security risks and challenges that make it easier for attackers to gain access to more sensitive IoT network data and expand the area of attack. IoT nodes talk with each other and hook up with the net without following any predetermined policies or regulations. This increases several privateness and safety concerns. However, proposed solutions face even greater challenges because of the enormous size and diversity of the problem.

The IoT ecosystem's security and privacy concerns are the subject of this research. Using the keywords "internet of thing challenges," "internet of thing issues," "internet of thing security issues," "internet of thing security solutions," and "internet of thing security and privacy," we searched the Saudi Digital Library, Google Scholar, and IEEE library for articles published between 2011 and 2017 that addressed the privacy and security concerns associated with IoT.

The idea of the Internet of Things (IoT) and its structure are in brief mentioned with inside the following segment, and segment three affords a top-level view of IoT safety at every tier of the structure. Section four highlights the requirements, difficulties, and a few counseled answers for IoT safety concerns. Section five affords a top-level view of the IoT privateness issue, observed through a dialogue and conclusion.

IOT OUTLINE

Progression

Kevin Ashton at the Massachusetts Institute of Technology first used the term "Internet of Things" in 1999, and while it quickly gained traction in the market, the poor performance of the network limited its application. ***Sristava*** stated in 2011 that merchandise may be marked with different technology like close to discipline communiqué

(NFC) and QR ciphers similarly to RFID. By 2020, there might be over 50 billion IoT devices. The Internet of Things (IoT) is a brand new form of the net wherein communiqué among machines takes the location of human-to-human communiqué. Televisions, automobiles, doors, wearable technology, and mobile phones are all part of the network. Each device comes equipped with technologies like radio frequency identification (RFID).

The Internet of Things is the writer of the M2M verbal exchange model. The Internet of Things (IoT) modified business, healthcare, industry, and our everyday activities. The modern-day business goal is to "join the disconnected," or to allow each tool in our surroundings to attach and proportion information. However, the various nature and excessive processing electricity of many IoT gadgets lead them to smooth prey for hackers. Safety is one of the major troubles with the IoT`s development. 71% of respondents to a survey agree with that safety issues have encouraged customers' choices to buy IoT products.

IoT Architecture

A flexible layered architecture is required for the Internet of Things (IoT) because it connects a variety of heterogeneous items.

The fundamental IoT model has a three-tier structure consisting of the application coating, the network coating, and the perception coating, despite the fact that there is no standard IoT design. Security concerns arise because each IoT layer differs from the others in terms of the functions and technology it integrates with. Layers consist of:

Layer 1 of Perception

This layer is referred to as the "sensors layer." Before sending the data to the network layer, this layer finds, gathers, and prepares it.

It also shows how IoT nodes cooperate in close-proximity networks and a sensor network. Sensors, GPS, and Radio Frequency Identification (RFID) technologies are its primary means of operation.

Layer 2 of the Network.

The Internet of Things and data forwarding to various hubs are handled at Layer 2 of the Network. Routers, switches, cloud computing platforms, and net gateways are crucial elements of the community layer. It uses 2G, 3G, LTE, WiFi, Bluetooth, ZigBee, and different technologies. Gateways at this accretion act because the hyperlink among nodes through collecting, filtering, and transmitting records among sensors.

Level 3 of Application

At this layer, the Internet of Things genuinely accomplishes what it got down to do with the aid of using offering a huge variety of clever surroundings applications. Smart cities, clever homes, clever offices, and clever transportation are all examples of IoT applications. The Internet of Things (IoT) has each private and business application, together with independent motors and cell apps.

IOT SECURITY QUESTIONS

The IoT and other systems are subject to the general security objectives of availability, integrity, and confidentiality. Security is difficult to achieve in the Internet of Things due to a number of restrictions, such as the variety of nodes with internet access and the absence of embedded security devices. This phase presents an outline of safety troubles at every IoT layer, accompanied with the aid of using a dialogue of IoT safety requirements, threats, and a few recommended solutions.

A. Security Concerns at Each Layer

1. Perception Layer

The IoT lumps are generally set up outdoors, wherein they may be susceptible to each human assaults and herbal disasters. Because of those factors, IoT nodes are getting easy goals for bodily attacks. For instance, if an attacker has bodily get admission to a tool element, he might also additionally tamper with it. Additionally, due to the fact IoT gadgets have to be cell for lots applications, the risk of such attacks is increased. Additionally, this residue generally includes wi-fi sensor networks and sensors with RFIDs, that have some of safety troubles such records leakage, replay assaults, clone assaults, and man-in-the-center assaults.

Additionally, those nodes are susceptible to numerous kinds of attacks due to the fact to their low garage area and constrained compute power. Examples of such assaults consist of replay assaults, which with the aid of using faking or replaying tool records identification, might also additionally conveniently take benefit of the secrecy of this residue. A timing assault is every other option, wherein the attacker determines the encryption key with the aid of using tracking the encryption time. Attacker nodes might also

additionally create malicious facts on this layer, endangering facts integrity and elevating the opportunity of a DoS assault. Encryption, stenography, get admission to control, and authentication to confirm sender identification can all be used to cope with the bulk of safety vulnerabilities at this tier.

2. Network Layer

This coating is regularly a goal for records theft, denial-of-carrier attacks, unauthorized get right of entry to, records destruction, virus attacks, man-in-the-center attacks, etc. Attackers can goal the community`s secrecy and privateness via eavesdropping and visitor's analysis.

The probability of such attacks is accelerated through IoT's far flung get right of entry to strategies and records interchange. To save you such attacks, the important thing alternate technique wishes to be noticeably secure. New protection issues which can be unusual at the Internet are added up through conversation in an IoT setting. While with IoT, conversation is simply among machines, conventional net conversation is among people and computers. These gadgets proportion lots of non-public records with out adhering to time-honored protection rules. Through his IoT gadgets, community attackers can research extra approximately the customers and make use of that records for unlawful purposes. In the Internet of Things, each community and item safeties are crucial. Although modern-day community protocols create powerful protecting measures, they do now no longer deal with the various nature of the IoT. The modern-day community kingdom ought to be recognized through objects, and that they ought to be capable of react to any uncommon moves that would jeopardise their protection. This degree of safety can be attained with the usage of powerful protocols and software.

3. Application Layer

Due to the lack of standards governing application development and interaction, there are several issues with application security. Identity and information privateness are tough to make sure in packages with a couple of authentication systems. This layer is accountable for coping with the traffic, making it prone to DoS attacks. In addition, the huge quantity of information generated and related gadgets can overload information evaluation software, thereby decreasing provider availability. When developing packages for the Internet of Things, special consumer interactions and the quantity of information as a way to be generated need to be taken into account.

B. IoT Security Needs and Challenges in General

The predominant safety necessities of IoT are mentioned from exceptional components by. IoT safety necessities may be summarized in 5 predominant necessities as proven with inside the table1. Satisfying those necessities is a large mission because of the restrictions related to IoT gadgets with reference to heir potential and functionality to put in force conventional safety solutions.

TABLE I. SECURITY REQUIREMENTS IN IOT

Confidentiality	Information transmission between objects must be protected from attackers [11].
Authorization	Object privileges should be restricted where they can access the resources they need for specific tasks only [12].
Authenticity	The access to the system and sensitive information is allowed for legal users only [4].
Integrity	Ensuring data accuracy and completeness and keep it from any tampered [13].
Availability	To avoid any possible operational interruptions or failures, the availability and continuity of the security service must be increased [12].

In addition, there are extra demanding situations going through the success of IoT protection necessities cited in and summarized as follows:

Date Capacity

Although the bulk of Internet of Things (IoT) packages rent constrained communique channels, many IoT structures have the capacity to want a considerable quantity of facts on the principal network.

• Resource limitations

Since the majority of Internet of Things (IoT) nodes have constrained storage and processing power, they regularly have low-bandwidth communication channels, which restricts the implementation of numerous protection functions much like the general public key encryption method.

• Defense

Since the bulk of RFID structures use a shoddy certification method, it is informal to hint tags and perceive things. Data may be accessed, modified, or even deleted through the intruder.

• Scalability

The Internet of Things (IoT) has a big variety of nodes and maintains to develop over time. As a result, its safety machine need to be scalable.

• Autonomic control

Nodes with inside the Internet of Things must have the ability to connect to each other and set themselves as much as extrade in line with the platform. Therefore, it should use self-configuring, self-managing, and self-recuperation strategies and techniques when you consider that automation necessitates extra safety and control.

C. Several suggested IoT security measures

Studies have been conducted with the aim of improving IoT security and providing solutions to security related problems. ***Tahir*** and his colleagues presented the ICMetric outline for safeguarding the Internet of Things with cryptographic keys. To solve the problems of key theft and prevent unwanted access, ICMetric technology adds a second layer of encryption algorithms. A key necessity of IoT-based healthcare applications, ICMetric technology is integrated into the healthcare environment to provide encryption that enables safe and secure use of electronic devices. In addition, ICMetric technology protects data stored and sent between devices. IoT security is solved by the method proposed by Liu et al, based on biological immune system. While static security solutions may not be appropriate, the recommended approach uses a dynamic defense outline for Internet of Things security. The proposed circular defense includes five relations: safety risk identification, risk calculation, security response, safety protection, and lastly protection plan development. When it comes to IoT security, the link in the framework is correlated. The researchers used immunity-based antigens and a actual IoT indicator to recreate the real IoT platform. They simulate the techniques used by biological systems to identify infections. ***Zhou*** and ***Chao*** created and evaluated a traffic management strategy while creating security architecture for media-aware traffic. The Media-Aware Traffic Security Architecture (MTSA) addresses the security requirements of media computing, communications, and Internet of Things services. Rose used Physical Non-Replicable Functions (PUFs) to illustrate how to implement security protocols and prototypes for IoT devices. He explains how PUF is capable of providing security upgrades through strong authentication or secret key generation in the IoT context. ***Lessa dos Santos*** creates a construction that allows IoT-restricted devices to interact with other devices on the Internet using authenticated "Data Transport Layer Security (DTLS)". IoT Security Support Providers (IoTSSPs), third-party devices, and two 6LoWPAN Edge Router (6LBR) mechanisms form the basis of this security architecture. They are used to direct the DTLS handshake to IoTSSP. ***Zegzhda*** and ***Stepanova*** suggest a method to deal with security attacks that attempt to disrupt, degrade, or destroy IoT components or services by leveraging topology durability. By maintaining an adaptive d-regular graph topology and taking into account various Internet of Things constraints, such as computational resource limitations on IoT devices, the goal is to ensure security of IoT through topology durability. Scalable Security with Symmetric Keys, advanced via way of means of ***Raza,*** introduces an extraordinarily adaptable and scalable key control method for the DTLS safety well known for restricted IoT gadgets aid regulation.

TABLE II. PROPOSED SOLUTIONS FOR IOT SECURITY

Author	year	Methods for achieving security	Main Security Requirements covered			
			Confidentiality	Integrity	Authentication	Availability
Tahir et al. [15]	2016	ICMetric coupled with CRRP	Yes	Yes	Yes	Yes
Liu et al. [16]	2013	IoT dynamic security based on immune system principles	No	No	No	No
Zhou et al. [17]	2011	Key management, watermarking	No	No	Yes	No
Lessa dos Santos [19]	2015	ECC cryptography	Yes	Yes	Yes	Yes
Rose [18]	2016	Nano-electronic security primitives	Yes	No	Yes	Yes
Zegzhda and Stepanova [20]	2015	Graph topology	No	Yes	No	No
Raza et al. [21]	2016	shared keys	Yes	Yes	Yes	Yes

Table 2 lists all solutions that have been suggested along with the security need they addressed.

D. Privacy Issues in IoT

The Internet safety word list defines privateness in IoT as "the proper of an entity (usually a person), appearing in its very own behalf, to decide the volume to which it'll have interaction with its environment, along with the volume to which the entity is inclined to proportion data approximately itself with others."

In the Internet of Things, a community of gadgets seeks to accumulate records from their environment and broadcast it together with a few occasions to a server that hosts apps. Privacy have to be managed in the course of every stage, along with inside the device, storage, communication, and processing. One of the vital worries that should be resolved with inside the IoT is the privateness and safety of touchy records.

1. Device Privacy

When unlawful get admission to happens in hardware or software, touchy data with inside the IoT is probably targeted. For instance, a digital digicam that has been reprogrammed via way of means of an interloper to broadcast data to invaders in addition to the legal server.

There are many troubles that want to be resolved so that you can offer tool privacy, together with defensive the identification of the character of the tool via way of means of including noise, defensive the touchy data even with inside the occasion that the tool is stolen via way of means of the usage of Quick Response Code technique, and defensive the tool region privacy.

2. Data Confidentiality

During Communication Data confidentiality is often accomplished via encryption techniques when data is sent across network channels. In some circumstances, data is added to packets after encryption to give them tracing properties. Some answers for privateness may be determined in verbal exchange protocols for security. Using pseudonyms for verbal exchange encryption can also additionally help to lessen the risk. Devices must simplest speak whilst certainly important to lessen privateness exposure. In order to reduce location monitoring, devices must have the ability to detach from the network while inactive. Only approved devices are permitted to interact, and even after being curved on, they must re-authenticate with the system before handling any data.

3. Storage Privacy

The least amount of statistics that may be stored at the same time as but retaining privateness protections is what must be done. Transport of statistics best takes place in "need-to-know" situations. The saved statistics' identification is probably hidden thru anonymization. Access to a database should be confined to simply statistical data. Differential privateness or the including noise technique may be applied to assure the output's independence from different database entries.

4. Processing Privacy

Personal and sensitive data must be treated appropriately and solely for the intended purpose. Before disclosing personal information to other parties, acceptance and data owner confirmation must be obtained. A useful way to manage transferred data rights and protect against improper processing is to utilize a digital rights management (DRM) system.

Personal and touchy statistics should be dealt with as it should be and totally for the supposed purpose.

Before disclosing private records to different parties, attractiveness and statistics proprietor affirmation should be obtained. A beneficial manner to control transferred statistics rights and guard towards wrong processing is to make use of a virtual rights management (DRM) system.

DRM is predicated on reliable, stable gadgets to characteristic properly. Before processing or really managing private statistics, consent from the statistics proprietor and understanding of the scenario should be sought. User notification aids in stopping unauthorized use of touchy statistics and personal records.

DISCUSSION

IoT adoption is notably impacted with the aid of using protection and privateness issues. The protection and privateness desires at every layer and every improvement factor have to be taken into consideration and addressed with inside the increasing studies on this field. The issue of enforcing protection answers is turning into greater hard because of the speedy boom with inside the variety of heterogeneous related nodes and the truth that almost all of the facts with inside the Internet of Things is touchy or non-public information. The ease with which IoT can be breached at every layer makes protection a critical problem for investigation. Confidentiality, authorization, authenticity, integrity, and availability are a number of the number one desires for IoT protection. IoT protection issues encompass carrier quality, confidentiality and dependability, handling and safeguarding big facts, software program and hardware vulnerability, and growing pertinent requirements are nonetheless unresolved and unaddressed. In order to shield IoT facts privateness, which is likewise a main protection situation in IoT, authentication and identification are essential. Although it has to be maintained in each IoT component, it regularly is going unnoticed. IoT layer-protection issues have to be protected with the aid of using ok protection frameworks for protection.

To create and enforce suitable protection answers for IoT that keep in mind the restrictions of its equipment, greater observe is required. Additionally, there's a want to create complete protection and privateness frameworks that deal with the troubles at every tier and take influencing variables into consideration.

CONCLUSION

This article offered a short creation to the Internet of Things (IoT) and its three-layer layout, evaluated the principle IoT safety wishes and issues, highlighted numerous cautioned IoT safety solutions, and tested the IoT`s privateness challenges. Problems with safety and privateness would possibly gradual the adoption of IoT.

It is important to layout complete safety and privateness frameworks that keep in mind the problems with inside the IoT surroundings and critical influencing variables. The aid constraints of IoT gadgets ought to additionally be taken under consideration at the same time as growing safety solutions.

REFERENCES

1. E. Leloglu, "A Review of Security Concerns in Internet of Things," Journal of Computer and Communications, vol. 5, pp. 121-136, 2017.
2. "Gartner Inc. Press Release," 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2905717
3. J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-supported Internet of Things," IEEE Internet of things Journal, vol. 3, 2016.
4. XHuang, P. Craig and H. Y. Lin, "SecIoT: A Security Framework for the Internet of Things. Security and Communication Networks," vol. 9, pp. 3083-3094, 2015.
5. "Capgemini Consulting and Sogeti High Tech Interview, Available at: http: www.capgeminiconsulting.com".
6. M. Mohammadi, M. Aledhari, A. Al-Fuqaha, M. Guizani and M. Ayyash, "Internet of Things: A Survey on Enabling," IEEE, 5 NOV 2015.
7. L.Atzori, A. Iera, G. Morabito and N. M, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, no. 3594-3608, 2012.
8. R. Zejun, L. Xiangang, Y. Runguo and Z. Tao, "Security and privacy on internet of things," in Electronics Information and Emergency Communication (ICEIEC), 2017 7th IEEE International Conference, July 2017.
9. Zhang, Q. Wen and X. D. R, "Application of dynamic variable cipher security certificate in

internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 2012.
10. K. Zhao and LGeo, "A survey on the internet of things security," in Int'lConf. on Computational Intelligence and Security (CIS)," pp. 663-667, 2013.
11. H. Suo, Zou, W. J and J. C.Liu, "Security in the Internet of Things: A Review," IEEE International Conference on Computer Science and Electronics Engineering,, Vols. 648-651, pp. 23-25, March 2012.
12. "Wind River Systems Security in the Internet of Things," 2015. [Online]. Available: http://www.windriver.com/whitepapers/security-in-theinternet-of-things/wr_security-in-the-internet-of-things.pdf.
13. Nguyen, K. Laurent and O. M, "Survey on Secure Communication," Protocols for the Internet of Things. Ad Hoc Networks, vol. 32, pp. 17-31, 2015.
14. Arseni, S. Halunga, S. Fratu, O. Vulpe and S. A., "Analysis of the Security Solutions Implemented in Current Internet of Things Platforms," IEEE Grid, Cloud & High-Performance Computing in Science, Romania, pp. 28-30, 2015.
15. Tahir, McDonald-Maier and A. Fernando, "A novel ICMetric based framework for securing the Internet of Things," IEEE International Conference on Consumer Electronics, pp. 469-470, 2016.
16. Zhang, C. Liu and Z. H, "A Novel Approach to IoT Security Based on Immunology," in Ninth International Conference on Computational Intelligence and Security, 2013.
17. C. L. and Zhou, "Multimedia traffic security architecture for the internet of things," vol. 25, no. 3, pp. 35-40, 2011.
18. Rose, "Security meets nanoelectronics for Internet of things," in International Great Lakes Symposium on VLSI, 2016.
19. L. Santos, Guimarães, d. C. Rodrigues, Granville and Tarouco, "A DTLSbased security architecture for the Internet of Things," in IEEE Symposium on Computers and Communication, 2015.
20. Stepanova and Zegzhda, "Achieving Internet of Things security via providing topological sustainability," in Science and Information, London, 2015.
21. Raza, L. Seitz, D. Sitenkov and G. Selander, "S3K: Scalable Security with Symmetric Keys—DTLS Key Establishment for the Internet of Things," IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, 2016.
22. "RFC 2828, Internet Security Glossary," May 2000. [Online]. Available: https://www.ietf.org/rfc/rfc2828.txt.