A Review on Architecture and Security of Internet of Things

Sudeshna Das, Chinu Mog Choudhari, Jhunu Debbarma
Tripura Institute of Technology,Tripura, India
jsudeshnadas@gmail.com, mogchinu03@gmail.com, jhunudb@gmail.com

Abstract

The use of Internet give rise to another area called as Internet of Thing. Use of Internet of Things (IoT) increasing day by day in people's daily life as well as in the industry. IoT devices are connecting us with the things and with the world around us. The devices used in IoT are varied in types, sizes and resources. In this paper, an overview has been given about architectures of IoT, technologies used in IoT and different attacks in IoT are discussed. A review has been done on various IoT attack detection techniques.

Keywords: Internet of Things (IoT), IoT architectures, IoT devices, security attacks

1 Introduction

The Internet of Things (IoT) is anticipated to grow swiftly as a result of the extensive usage of communication technologies, device accessibility, and the advancement of computing systems. The Internet of Things (IoT) enables connections and communication between machines and things through the use of the Internet. Kevin Ashton coined the phrase "IoT" for the first time in 1999. After some time, this word began to catch on. IoT is becoming more and more prevalent in both industry and people's daily lives. It is an essential component of your existence. IoT devices send the data they collected to the Internet. People may synchronise and communicate with others around the globe via the Internet. IoT devices come in a variety of processing capacities, and the environments in which they are situated may be remote. By allowing them to effortlessly communicate with one another, IoT connects a variety of objects, people, data, and processes. IoT may therefore aid in enhancing numerous processes by collecting and analysing a lot of data to make them more quantifiable and measurable. A few areas where IoT may enhance quality of life include healthcare, smart cities, the building and construction industry, agriculture, water management, and the energy sector. This is made possible by facilitating tools for real-time decision optimization and enabling a greater level of automated decision making.
The lack of security features in IoT devices makes it easier to attack. Therefore, IoT security is an issue that needs to be considered to protect the hardware and network of the IoT system. Security, however, has not been taken into account in the development of these appliances because the concept of networking appliances is still somewhat new.

2 Literature Survey

The first IoT monitoring system based on energy audits and analytics is proposed in the paper [1]. The dual disaggregation and aggregation deep learning models learn the typical IoT system performance indicators and, if necessary, can additionally offer in-depth analytics of specific system performance metrics. A dual deep learning model system is developed using the energy metre readings, and it adaptively learns the behaviours of the system under normal conditions. Data from energy audits are less vulnerable to hacking than data from other sources. To detect cyber attacks, the disaggregation model examines the energy usage of system components such as the CPU, network, disc, etc. The aggregation model characterises the difference between measured power consumption and predicted results to identify physical attacks.

In order to determine the device performance and identify variations that are anomalous, Paper [2] proposes to use statistical learning methods. Recommended framework is platform and device independent, because of system statistics like CPU usage cycles, memory usage etc. can be accessed through the IoT API (Application Program Interface). To evaluate their viability and applicability, several machine learning models are trained. Typical system performance can be well modeled for the target autonomous IoT devices, implementing well-planned processes. Anomalous behaviors can be easily identified using time series analysis techniques such as suggested adaptive online threshold (AOT), cumulative sum (CUSUM), and local outliers (LOF). We draw the conclusion that relatively basic machine learning models are better suited for IoT security and the recommended data-driven anomaly detection method after comparing their performance on anomaly detection. as well as the necessary computational resources. Paper[3] put the emphasis on network intrusion detection systems (NIDS). Reviews of free and open-source network sniffer software as well as current NIDS implementation tools and datasets. The paper covers both conventional and machine learning (ML) network intrusion detection systems and considers possible future developments. Given that learning algorithms have an excellent track record for security and privacy, the survey should concentrate on IoT NIDS deployed via machine learning. A machine learning strategy to identify routing threats for the Internet of Things has been proposed in the paper [4]. In IoT networks with 10 to 1000 nodes, the Cooja IoT simulator was used in the study to generate highly accurate attack data. They have developed a highly scalable, deep learning-based attack detection method to detect version number change, hello-flood and low rank attacks on IoT routing systems. .

In paper [5], the author provides a summary of several IoT layered architectures and security attacks from a layered perspective. A overview of the procedures that address these problems is also provided, along with a discussion of their shortcomings.

A breathing acoustics-based authentication method for secure access has been proposed in paper [6]. They are testing the effectiveness of the breath acoustics terminal system on three different types of smart devices: smartphones, smartwatches, and Raspberry Pi, for tasks like user identification and verification. They compare system performance when using shallow classifiers (such as SVM, GMM and logistic regression) with classifiers based on deep learning (e.g. LSTM, MLP). They found that of all the classifiers compared, the LSTM models for audio classification were the most accurate, had the fastest inference time, and were the most compact.

3 IoT Architecture

The abstraction of many layers of hierarchy can be observed in the architecture of the Internet of Things. The application layer, middleware layer, the network layer, and the perception layer are the main layers of the abstraction. Despite the fact that a device from the same layer may use a variety of technologies, each layer's technologies are distinct. A variety of services with unique needs, limitations, and trade-offs are offered using the devices and technologies in the Internet of Things. The technologies and equipment themselves are also very diverse. Because of this, managing them is a challenging and complicated endeavour. In order to overcome this difficulty, middleware layers are occasionally introduced to control various service kinds while hiding the implementation's inner workings. The role of the middleware layer is to gather data from network layer and store them in the cloud and database. The middle layer also provides data processing capabilities. A four-layer IoT architecture, which includes the aforementioned components, is used in this work and can be used to build real-world applications. The four-layer architecture of IoT is shown in Figure 1. To emphasize specific security requirements, we test the functionality of these layers in this section.

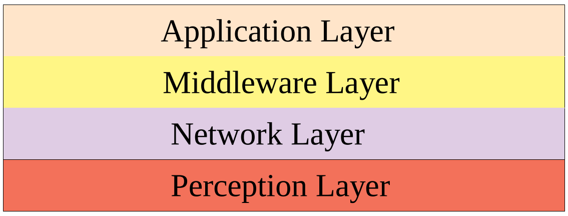

Figure 1 IoT architecture

3.1 Application Layer

The social component of the Internet of Things, the application layer combines with industry demand to realise significant intellectualization. For various contexts, this layer implements various applications. The middleware layer's data is managed and processed by this layer, which also offers the end user a high-quality service. Application layer issues, including as unauthorised access to data, malicious data modification, and permissions that are granted for an extended period of time, mostly arise when sensitive data is used. In order to attack systems and steal or alter sensitive data, attackers can take use of coding flaws.

3.2 Middleware Layer

Data from the community layer is processed and saved withinside the middleware layer, which also hyperlinks the device to databases and the cloud. Middleware layer may also offer extra effective compute and storage capabilities. This layer offers APIs to provide help to the software layer. Database and cloud safety are issues on the middleware layer that have an effect on the extent of provider on the software layer.

3.3 Network Layer

This layer manages the connectivity of the IoT infrastructure. Moreover, it collects and transmits data from the cognitive layer to the higher layer. Wi-Fi, Bluetooth, ZigBee and 3G are the main transmission media technologies. Wired or wireless media available. Attacks on the network layer frequently complicate task coordination and information sharing for devices.

3.4 Perception Layer

The perception layer aims to recognise objects and collect relevant data before turning it into digital signals. The primary technologies of this layer are wireless sensor networks (WSN), RFID tags, cameras, and sensors. Technologies used in perception layer have an impact on energy and computing power. Additionally, a sensor device may be used in an environment that is hostile and vulnerable to destruction (intentionally and unintentionally). The effectiveness of the entire system is directly impacted by this. The largest challenge for this layer is the malicious attacks on the identification and sensor technology that prevent data collection.

4 IoT Technologies

Radio frequency identification (RFID), Bluetooth, near field communication (NFC), wireless sensor network (WSN), and ZigBee are the communication technologies that are utilised to realise the idea of IoT.

4.1 Radio frequency identification (RFID)

RFID connects two devices using frequency waves. Tags, a database, and a reader make up its components. The tags are attached to the objects and read their status while a reader is used to read the information from the tags. Data is stored in a database, which is regarded as the third component. Numerous Internet of Things (IoT) applications, including ones for tracking people, gesture recognition, and health care, use RFID technology. Working of RFID is depicted in Figure 2.

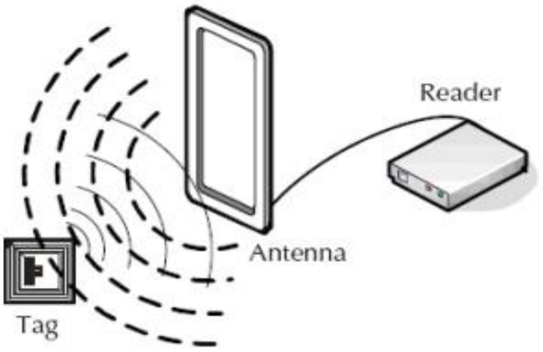

Figure 2 Context of RFID

4.2 Bluetooth

Bluetooth is used for applications that require close-proximity communication. It provides a range of security mechanisms to guarantee secure communication between the sender and the receiver. Among the Internet of Things (IoT) applications that make use of Bluetooth technology are traffic monitoring systems, smart home automation, and human traces.

4.3 Near field communication (NFC)

A close-range wireless communication method is NFC. Near-field communication transmits data via electromagnetic radio signals between two connected devices. Both devices must have NFC chips for the system to work because transactions take place over a relatively short distance. NFC-enabled devices can only send data when they are physically contacting or a few centimetres apart.

4.4 Wireless Sensor Network (WSN)

A node in a WSN is made up of four parts: a sensor, a battery, a microcontroller, and memory. It is straightforward to understand how the network works after reading this explanation of how sensors are used to collect data and store it in the WSN's memory for later use. All information is sent to the server. Additionally, batteries that allow for continuous operation are used. Smart grid, environmental monitoring, and an intrusion detection system are a few IoT applications that use a wireless sensor network. Working of sensing node is depicted in Figure 3.

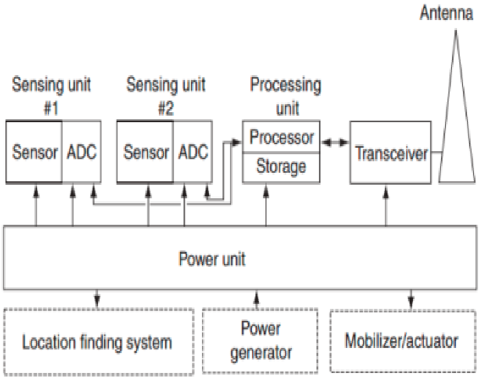

Figure 3 Working of a sensing node

4.5 ZigBee Technology

ZigBee is a PAN (personal area network). It offers minimal power consumption at a reasonable price to win the trust of as many customers as possible. It offers wireless connectivity for short-range data transmission. Application, network, Media Access Control (MAC), and physical layers make up this structure. ZigBee technology is employed in a variety of IoT applications, such as home energy monitoring and control systems, fingerprint-based attendance systems, and greenhouse monitoring systems. A MAC layer provides encryption. To prevent man-in-the-middle attacks, the MAC layer offers facility of integrity as a service. With ZigBee technology, each device is given a network key, which adds security. Having a network key is required for every device.

5 Applications of IoT

IoT applications in the areas of smart traffic systems, smart environments, smart homes, smart hospitals, smart agriculture, and smart retailing and supply-chain management are just a few of the numerous possibilities.

Based on an intelligent traffic monitoring system, the smart traffic system We require IoT solutions for accurate automatic recognition of vehicles and numerous traffic parameters. By reducing congestion, the intelligent traffic monitoring system offers an excellent transportation system. Other advantages include the ability to detect parking plots, traffic accidents, reduce environmental pollution, detect theft, and determine the best route in the event of a roadblock. The development of cutting-edge IoT technologies has made it feasible to foresee a variety of natural calamities, including floods, earthquakes, rain, and water logging. For noise, air quality, and other environmental pollutants, there exist effective monitoring systems.

IoT offers remote home automation in smart homes based on requirements. Saving resources is possible with proper energy and water supply monitoring. A reliable incursion detecting system exists.

Smart hospitals have flexible smart wearables loaded with RFID tags that enable doctors to keep an eye on patients' vital signs whether they are inside or outside the hospital's walls. Soil nutrition, light, and humidity may all be monitored in smart agriculture. Through automatic temperature change, it enhances the sensation of being in a greenhouse. If there are bad weather conditions, it maximises production. Saving water and fertilisers is made possible by using the right amount of each.

By using RFID-equipped products, a store may keep track of its inventories in smart retailing and supply-chain management. It also aids in the detection of shoplifting. It keeps track of every item in a store and places orders for products in lower quantities on its own. Retailers can create sales charts and graphs to help them come up with successful tactics to boost sales.

6 Security in IoT devices

IoT devices are open to numerous attacks. There are many reasons why IoT device security is disregarded, including IoT devices typically have very basic operating systems, which leaves less room for security measures like auditing, which allows attackers to hack and abuse the devices covertly. In IoT development, there is a lot of hardware and software reuse, which results in a lot of security-critical components being shared between devices. Malware can be simply developed for the target architecture because the operating system of IoT devices is typically a simplified version of Linux. Peer-to-peer is a common technology used by IoT devices, enabling consumers to connect to their gadgets as soon as they go online. Without the owner's knowledge, hackers can identify susceptible cameras quickly using faults in these features, then launch attacks to gain access to them. P2P is a feature that many devices have that enables access to them without the need for human setting. Users are able to instantaneously connect to their device from their phone or computer by using a unique serial number known as a UID. P2P devices can be accessed without port forwarding or dynamic DNS. Additionally, these devices have the ability to automatically overcome NAT and firewall situations.

6.1 Attacks associated with each layer of IoT

Various attacks are associated with each layers in IoT devices. These attacks are discussed briefly.

6.1.1 Perception Layer

Replay attacks and side channel attacks occur in the perception layer. Attackers eavesdrop on conversations between the two parties during a replay attack to gather information. Repeated transmissions of the received messages between communication pairs deplete communication resources. This attack frequently takes place in the communications between the RFID reader and RFID tag in RFID technology. This kind of attack uses up the resources in the back-end database in addition to the computational resources between the reader and tag. In addition to the aforementioned outcomes, attackers can gain reader give access using radio signal broadcasting. A side-channel attack [10][11][12][13] uses a computing system's or implementation's information leak to infer sensitive data. With side-channel attacks, the attacker had to physically own the target device in order to see and discover the information that was leaking. There are two different kinds of side channel attack: active and passive. In an active side channel attack, the attacker directly modifies the device's behaviour. Additionally, in a passive side channel attack, the attacker merely watches information leak.

6.1.2 Network Layer

Attacks on the network layer, such as DoS, DDoS, Man-in-the-Middle, Sinkhole, Sybil, Sniffing, and Trace Analysis are briefly described in this section.

A denial of service (DoS attack) attack against the network is done by bombarding the target with requests, which generates a lot of network traffic. This type of attack can deplete all resources. It leaves the users unable to access network resources. In addition, a lot of unencrypted user data can also be leaked. Additionally, a distributed denial of service (DDoS) attack can use a computer network as the attack platform to launch DDoS attacks against one or more targets. A man-in-the-middle attack takes place in real time between two victim nodes that are communicating. In order to communicate with the two victim nodes, the attacker poses as a valid node on one of the nodes. Two nodes trust the attacker, who then learns details about two victim nodes.

Attackers exploit a compromised node to draw data flow from surrounding nodes in a sinkhole attack.

The system believes that the data has already arrived at its destination because it has been tricked. In a WSN, an attacker could

employ a malicious node to draw in network activity before operating at will with the sensor data.
In Sybil Attack, a system node gives multiple identities to the victim node. It allows the victim node to perform an operation multiple times, eliminating redundancy. In a Wireless Sensor Network (WSN), the attacker has multiple identities. The victim node can pass information through the compromised node, resulting in longer routing distances. In a sniffing attack, the attackers gather network information using sniffer tools and software before extracting vital information for further attacks.
In trace analysis, by examining the quantity and size of transferred data packets, attackers can infer communication load and pattern. More useful information is available the more packets that can be processed and evaluated. This kind of assault can be used against encrypted packets, and its communication pattern can be examined. Through traffic analysis, WSN may provide three different types of information. An attacker may start by noticing network activity. The physical location of wireless access points can also be obtained by an attacker. A hacker can even discover information on the protocol type utilised in the communication.

6.1.3 Middleware Layer

Information can be transmitted wirelessly or wired from the middleware layer to the network layer via this media. DoS attacks and illegal access by malicious insiders are only two examples of the many threats that might impact this layer.
The network layer and the DoS attack in a support layer are connected. To flood the network with data, an attacker sends a lot of it. The IoT is therefore exhausted as a result of the heavy system resource use, and the user is no longer able to access the system.
An IoT environment is the target of a malicious insider attack, which allows access to users' private information. An authorised user does it in order to access information belonging to another user.

6.1.4 Application Layer

Malicious code attack and cross-site scripting are two examples of assaults that can impact this layer. A form of injection attack is cross-site scripting. A client-side script, such as java script, can be inserted by an attacker and placed on a reliable website that is accessed by other users. The contents of the application can be entirely altered by the attacker to suit his purposes.

Any code in a piece of software that is designed to harm the system or have unwanted effects is known as a malicious code attack. The usage of anti-virus software might not be able to stop it or manage it. It could turn on by itself or behave like a programme that demands the user's attention before acting.

7 Challenges

Although the IoT has a huge impact on our daily lives, there are also many obstacles to overcome. Poor management plagues IoT-based applications. Sensors assemble information. The method of information gathering and storage is less important to developers. Attackers have simple access to user information. Developers should concentrate on secure information collection methods as a result of this vulnerability. Another significant challenge that needs to be actually resolved is giving IoT devices a sense of trust and privacy. IoT devices encounter issues as a result of their proliferation. It is now difficult to assign identities to the devices. There are many gadgets connected to the Internet of Things (IoT). The amount of information produced by these gadgets is immense. An IoT challenge is how to transmit and process such large amounts of data.
There are difficulties with authentication and authorization. In a classical system, users can be authenticated in a variety of methods. The network has grown sophisticated as a result of the high number of connected devices. As a result, standard methods of authentication and permission are completely ineffective in large networks.
Some of the difficulties are highlighted in the study. The problems at hand must be resolved soon.

8 Conclusion

The Internet of Things (IoT) is advancing into daily life. By connecting multiple smart applications, it is utilised to improve quality of life. IoT aims to enable universal automation. An overview of IoT security technologies was provided in this study. We have provided a brief overview of IoT's layered structures. Additionally, the topic of security attacks based on layering is covered. We reviewed the available research on security risks to existing systems as well as to safeguard IoT infrastructure. The IoT technology's open research issues have also been suggested as potential future directions. These issues must be resolved and implemented right away.

Reference

References

[1] Li, Fangyu, et al. "Enhanced cyber-physical security in internet of things through energy auditing." IEEE Internet of Things Journal 6.3 (2019): 5224-5231.

[2] Li, Fangyu, et al. "System statistics learning-based IoT security: Feasibility and suitability." IEEE Internet of Things Journal 6.4 (2019): 6396-6403.

[3]Chaabouni, Nadia, et al. "Network intrusion detection for IoT security based on learning techniques."IEEE Communications Surveys & Tutorials 21.3 (2019): 2671-2701.

[4]Yavuz, Furkan Yusuf, Ü. N. A. L. Devrim, and G. Ü. L. Ensar. "Deep learning for detection of routing attacks in the internet of things."International Journal of Computational Intelligence Systems 12.1 (2018): 39.

[5]Burhan, Muhammad, et al. "IoT elements, layered architectures and security issues: A comprehensive survey."Sensors18.9 (2018): 2796.

[6]Chauhan, Jagmohan, et al. "Performance characterization of deep learning models for breathing-based authentication on resource-constrained devices."Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2.4 (2018): 1-24.

[7] Muna AL-Hawawreh, Nour Moustafa , Elena Sitnikova"Identification of malicious activities in industrial internet of things based on deep learning models"Journal of Information Security and Applications 2018

[8] Ren-Hung Hwang , Min-Chun Peng, Van-Linh Nguyen and Yu-Lun Chang"An LSTM-Based Deep Learning Approach for Classifying Malicious Traffic at the Packet Level"Applied sciences,2019

[9]Sutharshan Rajasegarar , Alexander Gluhak , Muhammad Ali Imran , Michele Nati ,Masud Moshtaghi , Christopher Leckie , Marimuthu Palaniswami "Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained znetworks"Pattern Recognition,2014

[10] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in Advances in Cryptology – CRYPTO 1996, ser. LNCS, vol. 1109. Springer, 1996, pp. 104–113.

[11]P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Advances in Cryptology – CRYPTO 1999, ser. LNCS, vol. 1666. Springer, 1999, pp. 388–397.

[12]J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards," in Smart Card Programming and Security – E-smart 2001, ser. LNCS, vol. 2140. Springer, 2001, pp. 200–210.

[13]S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks Revealing the Secrets of Smart Cards. Springer, 2007.
[14]L.Xiao, Z.Wang, "Internet of Things: A New Application for Intelligent Traffic Monitoring System," in JOURNAL OF NETWORKS, 2011

[15]Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Proceedings of Frontiers of Information Technology (FIT), 2012, pp. 257-260

[16]P.Fuhrer, D.Guinard, "Building a Smart Hospital using RFID technologies,"

[17] F.TongKe, "Smart Agriculture Based on Cloud Computing and IoT," in Journal of Convergence Information Technology (JCIT), Jan'13

[18]Farooq, M. Umar, et al. "A review on internet of things (IoT)."International journal of computer applications13.1 (2015): 1-7.

[19]Anzelmo E, Bassi A, Caprio D, Dodson S, van Kranenburg R: Matt Ratto (Internet of Things, Discussion/Position Paper. 2011, Institute for Internet and Society, Berlin, commisioned.