SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage: https://jaraset.com/
ISSN: 2462-1943

Securing IoT Environments: A Comprehensive Analysis of Cluster Based Security Mechanism

Rohit Kumar Vyas [1*], Dr. Meghna Dubey [2]

[1] Research Scholar, Department of Computer Science and Engineering, Mewar University, Rajasthan, India
[2] *Associate Professor, Department of Computer Science and Engineering, Mewar University, Rajasthan, India*

ARTICLE INFO

Article history:
Received: 22-08-2024
Received in revised form: 15-09-2024
Accepted: 28-09-2024
Available online: 11-11-2024

Keywords:

Internet of Things, Network Security, Information Security, Privacy of Data, Secure Connections.

ABSTRACT

Sensors, communication networks, and intelligence that control every step of the process and the data produced are the foundation of the Internet of things. Sensors may be utilized in vast numbers since they are the senses of systems. Sensors need to be tiny, inexpensive, flexible, and able to operate in a variety of environments. Consequently, as the number of nodes linked by sensor data develops quickly, the security of these network devices data sensors and other devices become more important. This work provides an overview of papers on the Internet of Things (IoT), security issues, particularly those pertaining to privacy, and access control in this kind of environment from the perspective of a systematic review. In conclusion, it offers a comprehensive examination of security concerns that need to be resolved, spanning several categories and specific domains within the technology's application industries.

Introduction

Internet of things (IoT) is seen as an integrated component of the Internet, which is also described as a dynamic global network infrastructure made up of many items with the ability to interact and communicate with end users [1]. In order to facilitate interaction, these things need to have distinct identities.

The necessity for privacy and data security is significant because of the rapid development of Internet-connected devices and the creation of networks that communicate with them [2]. As a result, information security is a well-known issue since the number of internet-connected devices is increasing quickly, increasing the amount of data that is exposed on the network.

In order to address the excessive number of authentications, this article suggests a security architecture that uses methods like public key infrastructure (PKI) to neutralize vulnerabilities at

the Internet of Things. This problem has a solution provided by [3], who conducted an investigation of fingerprint identification and suggested a three-layer model (sensor, transport, application) that allowed for the examination of each process component. In this project, writers use RFID systems and include a microchip combined memory to develop a system that enables to receive a signal and send it with some extra data (unique serial number). Another security issue is connected to the communication medium; this issue is handled in [4].

The goal of this research is to provide a broad overview of the issues related to IOT security levels. As a result, the state of the art regarding safety in Internet of Things environments is presented, with a focus on the security mechanisms involved. On the other hand, an analysis of the factors pertaining to performance, application, and security is presented, along with a list of security techniques that can be used in IOT environments. To this end, we shall propose the use of categorization as a means of determining which factors, in accordance with the principles of authenticity, access control, and authentication, should be taken into account when flagging safety concerns. In order to facilitate the acquisition of devices to be used in various work environments, such as industrial level, Smart Grid, or home, it is important for this model to characterize the types of RFID devices, work settings, connection types, and security mechanisms that could be applied for the purpose [5].

Literature Review

The Internet of Things, or IOT, has gained popularity in homes recently due to the advancement of mass communications via networks that enable the worldwide interchange of products and services [6]. According to keeping an eye on homes using security cameras, motion detectors, and other Internet-connected sensors makes managing them easier and facilitates the user's access to important data. These things, like having a smart phone that is linked to the Internet and being able to watch your house from anywhere in the globe, may provide you peace of mind. However, a research conducted by [8] claims that these ongoing monitoring levels are exposed to degrees of confidence in order to analyze the hazards, such as the network points and their transmission. The authors ultimately come to the conclusion that this encryption and authentication procedure needs to be reviewed. This implies that the user is no longer the only one who can see and keep an eye on his property, but an intruder may easily do this, making a home's security and privacy insecure.

Wearable's, which are tiny, wearable gadgets that record data from specific activities, are among the most well-liked gadgets driving the Internet of Things' growth. The user may also get additional information from them, such as the time, the weather, or even alerts from a connected mobile phone. They may receive mail, messages, and even calls in addition to syncing their activities with other devices and social media platforms; thus, the majority of the time, the data is kept on cloud storage.

Real time information is made possible by IoT, which uses physical items to connect computer systems to the outside world [7]. As a result, a lot of data must securely go from various sources (sensors, actuators, RFID tags, etc.) to the data centre and from there to devices like PCs and smart phones, which may then use the information to make choices. The growth of IOT is posing new security-related difficulties.

Information technology is developing at a quick pace, and as more is known about Internet security and the Internet of Things, new issues and possible security risks have emerged. As a result, developing a safety and dependability framework for the Internet of Things becomes a priority. This issue has been addressed in a general trust architecture [9], which consists of a trust module (which places users at the centre of the system), a perception of trust module (which performs full authentication), a terminal confidence module (which operates in accordance with control rules), a trusted network module (which is intended to assess, analyze, and manage security situations), and a trusted agent module (which reduces the risks associated with unreliable access terminals). The development process for these modules addressed security concerns and produced a development model, but it did not provide a particular fix for the security issue.

In light of future Internet of Things applications in fields as diverse as health (e.g., remote patient monitoring or control of the elderly) and smart cities (e.g., distributed pollution monitoring, intelligent lighting systems), among many others, appropriate mechanisms will be needed to ensure communications with these devices in the work done by [10]. The endeavors of regulatory bodies like the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE) to develop communication technologies and ensure the security of the Internet of Things also mirror this trend.

Research Methodology

Since the Internet of Things is a vast sector with many different technologies, a categorization of the problems and technologies was created. This categorization serves as the foundation for an analysis of specific security and privacy specifics in the relevant domains. a classification of the problems and corresponding technology employed in every subject that comprises the Internet of Things. The eight key IoT topics that have been identified need a certain degree of security-related research. Below is a detailed description of them:

***Communication*:** Communication protocol research has produced solutions like TLS and IPSec that provide secrecy, integrity, and authenticity. While Onion Routing and Freenet are two examples of routing techniques that have fulfilled privacy demands, they are not commonly employed.

***Sensors*:** The goal of the present study is to ensure the authenticity and integrity of the sensor data, which may be achieved by watermarking, as previously mentioned by [2]. Since data sensors' confidentiality is a very precarious situation, there is no need for it inside the sensor; instead, secrecy depends on communication confidentially. It is crucial to have mechanisms in place that protect people's and things' privacy, such face-blurring video data.

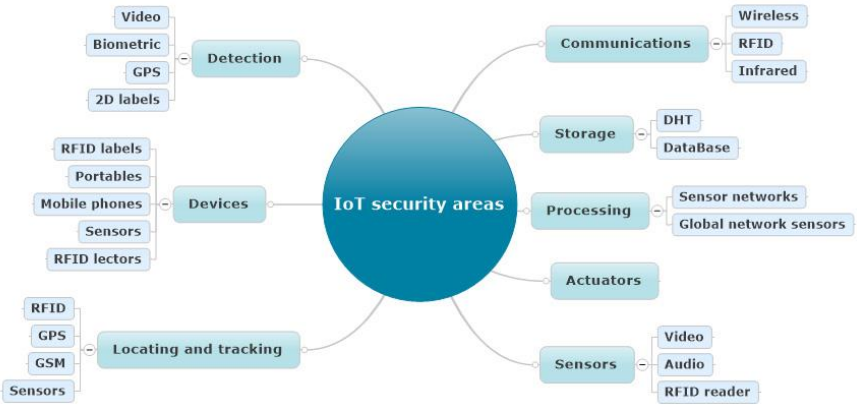

Figure 01: IoT security areas identified

The availability of sensors is mostly dependent on the communication infrastructure. Laws are required to protect the privacy of those who are now most often unaware of the sensors, such video cameras.

- **Actuator:** The security of communications is the primary determinant of the integrity, authenticity, and secrecy of data in an actuator.
- **Storage:** Well-established security protocols are in place for storage devices. Data storage has a high privacy threshold, and there are many instances of privacy laws being broken. These incidents should be publicly publicized in order to adequately address user privacy protection. The availability of redundant storage technologies and the communication infrastructure are the primary determinants of storage availability.
- **Devices:** A device is malware-free as long as it is operating within the parameters of device integrity. This trait has also been referred to as "admissibility" by B. Schneier; it is very sensitive, a Trusted Computing Platform (TPM) research topic that is currently open. A device's authenticity manages every aspect of communication, including invisible components like the connection's endpoint. In order to guarantee that no outside party has access to internal data devices, confidentiality is a device with integrity.

Device privacy is influenced by communication and physical privacy is below as:

Processing: The reliability of communication equipment is the foundation for the integrity of data processing services. It also relies on how well processing algorithms are designed and implemented. The device's and the communication's validity are the only factors that determine the processing's legitimacy. When processing data remotely, the secrecy feature is contingent upon both the communication channel's integrity and the device's integrity. Processing availability is solely dependent on the device and connection availability [5].

Location and Tracking: The reliability of GPS or GSM reference signals utilised in the location, as well as the integrity of communication, are the foundations of location and tracking integrity. Additionally, it is dependent upon the integrity and validity of the communication devices. Ensuring user privacy requires the secrecy of data monitoring and tracing, which makes it very sensitive [4]. In this sense, confidentiality is essentially reliant on the secrecy of communication, meaning that an attacker cannot reveal the location data. When anything is data privacy located, it implies that an attacker cannot identify a person or item, and that tracking and location cannot be done without consent or express knowledge.

Identification: It employs the same levels of sensitivity as tracking and location. The increased sensitivity on the integrity aspect is one distinction [2]. Since it is managing the localization process, it is simpler for an attacker to alter the identifying process. This corresponds mostly to the fact that an attacker is more likely to manipulate location technologies (like GSM) because of the technology utilized, such as RFID or biometrics.

Table 01: Recommendation criteria in security areas

Properties	**Security principles**		
	Integrity	**Authenticity**	**Confidentiality**
Communication	High	Medium	Medium
Sensors	High	High	High
Actuators	Low	High	Low
Storage	High	High	High
Devices	Low	Medium	Low
Processing	Low	High	Low
Location and tracking	High	Medium	Medium
Identification	Media	Baja	Alta

Conclusions

One of the most important steps that have to be done is to safeguard the information that is travelling via IOT devices, since they are primarily focused on transmitting information to and from the Internet. This information is often sent via public or wireless networks, both of which are open to assault. If the data is not encrypted to a sufficient degree, an attacker may find it easier to carry out assaults on the communication channel. In order to function as an intermediary in communications that is invisible to both the source and the destination of traffic, the attacker may intercept customer traffic, modify it to seem as if it originated there, and then transfer it to the genuine server. As a result, anybody may get whatever information they choose and even edit it to change how the device behaves or performs. They can even provide users with

misleading information to prevent them from making the best choices based on the original facts. Research on the availability of communication in the face of DDoS and IP-based services is particularly needed. Considering the need for more study, the devices' integrity must also guarantee that they are free of viruses such spyware and root kits. Lastly, hardly any sector has measures that are relevant to Internet of Things privacy.

Future work is anticipated to characterize these issues so that proper security mechanism identification from the most common issues in IoT application clusters may be accomplished out using an ontological model and intelligent agents. This would make it easier to identify security options and install access models for IoT devices first.

References

1. D. Boyle, R. Kolcun, and E. Yeatman, “Devices in the internet of things,” J. Inst. Telecommun. Prof., vol. 9, no. 4, pp. 26–31, 2015.

2. D. Pavithra and R. Balakrishnan, “IoT based monitoring and control system for home automation,” in 2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 169–173.

3. V. Vujovic and M. Maksimovic, “Raspberry Pi as a sensor web node for home automation,” Comput Electr Eng, vol. 44. pp. 153–171.

4. R. Aggarwal and M. L. Das, “RFID security in the context of internet of things,” in Proceedings of the First International Conference on Security of Internet of Things, 2012, pp. 51-56.

5. W. Huan, “Studying on Internet of things based on fingerprint identification,” in 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), 2010.

6. R. Weber, “Internet of Things–New security and privacy challenges,” Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

7. L. Atzori, et al., “The internet of things: A survey,” Computer networks, vol. 54, pp. 2787-2805, 2010.

8. G. Gang, et al., “Internet of things security analysis,” in Internet Technology and Applications (iTAP), 2011 International Conference on, 2011, pp. 1-4

9. X. Li, et al., “Research on the architecture of trusted security system based on the Internet of things,” in Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on, 2011, pp. 1172-1175.

10. J. Granjal, et al., “Security for the internet of things: a survey of existing protocols and open research issues,” Communications Surveys & Tutorials, IEEE, vol. 17, pp. 1294-1312, 2015.

11. T. Bécsi, et al., “Security issues and vulnerabilities in connected car systems,” in Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2015 International Conference on, 2015, pp. 477-482.