Analysis of IoT Security, Privacy, Threats, and Future Directions

Saad Rehman Babary[1], Hamza Mashhood Elahi[2], Hamza Arif[3], M. Junaid[4]
[1-4]Department of Computer Science & Engineering, University of Engineering and Technology, Lahore
[1]saadbabary97@gmail.com, [2]hm868050@gmail.com, [3]mianhamza2326@gmail.com

***Abstract*—Explores the key aspects of security, privacy, dangers, and future prospects in the Internet of Things (IoT). It investigates the issues and implications for security and privacy in modern IoT networks. Various dangers to IoT systems are investigated, along with their consequences. It also analyses new trends and techniques for improving security. The abstract continues by highlighting future prospects in IoT security, emphasising the continuous growth and adaptability necessary to adequately protect IoT infrastructure.**

***Keywords*– IoT, Smart Home, Layers, Security and DoS**

I. INTRODUCTION

THE Internet of Things (IoT), which has come to the front line of present-day innovation, has altogether adjusted our communications with innovation and our current circumstance. IoT environments — a perplexing trap of connected gadgets and sensors — have acquired conspicuousness lately as a wellspring of development and examination. Two basic parts in this steadily changing climate are working framework (operating system) backing and organization improvement.

This examination researches the cooperation between working frameworks and organization streamlining in the always changing Web of Things, reaching out past the customary limits of innovation. Solid operating system establishments are basic to the fruitful and secure activity of Web of Things gadgets, which range in size from little sensors to strong entryways. Besides, network foundation streamlining is expected to empower a smooth, continuous information stream with low dormancy.

We start by taking a gander at the particular operating system support that upholds this game-evolving innovation, as we concentrate on the harmonious connection between working frameworks and the Web of Things. We talk about the exceptional attributes of Constant Working Frameworks (RTOS), which are basic for guaranteeing convenient and reliable reactions in applications, for example, telemedicine, brilliant manufacturing plants, and self-driving cars. Linux-based working frameworks end up being flexible workhorses, fit for overseeing entryways that coordinate a large number of gadgets and administrations. Wearables, home robotization, and accuracy agribusiness all advantage from IoT-explicit working frameworks that upgrade asset usage. These arrangements are explicitly custom-made to the attributes of IoT gadgets.

Besides, our journey investigates the labyrinth of organization streamlining strategies that permit IoT organizations to make due. Edge figuring, as shown by arrangements like Microsoft Sky blue IoT Edge, alters information handling by bringing down idleness and data transfer capacity needs. Zigbee and other lattice organizing conventions are utilized to make independent organizations, which are basic for Industry 4.0 applications and brilliant homes. MQTT is an illustration of QoS improvement, which guarantees predictable message conveyance, which is expected for remote observing and control frameworks.

As IoT research progresses, it presents both extraordinary open doors and difficulties. Online protection is essential, and to make preparations for weaknesses and new dangers, network streamlining and working framework support should be incorporated and consistently refreshed. Versatility is a major test since IoT networks are quickly growing and require consistent mix across a different arrangement of gadgets and conventions. Our review is directed by late examinations and contextual analyses that show how these standards may be utilized in a unique climate.

This article investigates the confounded trap of working frameworks and organization enhancement inside the Web of Things, drawing motivation from state of the art disclosures and exploration. It comprehends that the field is ceaselessly adjusting to the most recent innovative revelations and current difficulties, thinking about the consistently changing IoT working frameworks and organization enhancement strategies. Through this investigation, we give specialists, developers, and powerful people with an exhaustive comprehension of the basic undertakings given by working frameworks and organization streamlining inside the flourishing field of Web of Things research.

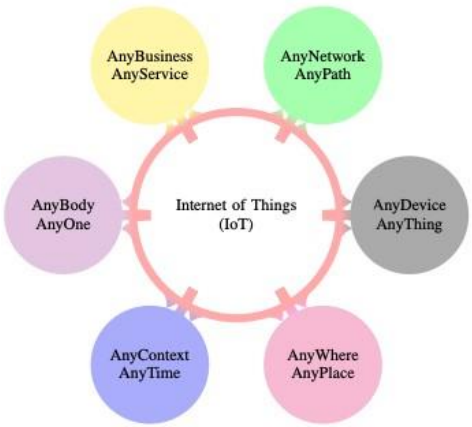

Fig. 1. Definition of IoT

II. EMERGING RESEARCH IN OPERATING SYSTEMS SUPPORT FOR IOT AND NETWORK OPTIMIZATION

Older operating systems are unable to handle the various demands of these networked nodes due to the Internet of Things' rapid proliferation. The goal of current research is to create specialized operating systems that meet the unique needs of the Internet of Things. To support an array of devices ranging from tiny sensors to powerful gateways, these systems need to be flexible, light, and energy-efficient. Thanks to recent developments in this area, new operating systems that are optimized for resource-constrained environments can now function well while using less energy. IoT systems are vulnerable to hacking, making security a major concern. Research projects have produced strong security features like intrusion detection systems, secure boot processes, and authentication protocols integrated into IoT operating systems, which have improved the security of IoT networks against emerging threats. For applications using the Internet of Things, efficient data transmission is essential. In order to ensure scalability, low latency, and reliability with the increasing amount of data generated by Internet of Things devices, network optimization is key. MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) are two new network protocols that researchers are investigating to improve communication in Internet of Things environments. Integration is an additional field where research is progressing rapidly.

III. INTERNET OF THINGS (IoT) ARCHITECTURE

The foundation for developing and deploying IoT systems is IoT architecture. The structure, components, and interactions of an Internet of Things ecosystem are specified to guarantee that devices, networks, and applications operate together smoothly to acquire, process, and exchange data. Data management, security, scalability, and communication protocols are all critical components of an effective Internet of Things architecture. An outline of the essential features and tiers of a typical Internet of Things architecture is presented here [2]:

A. Device Layer

The Internet of Things devices, comprising of sensors, actuators, and diverse endpoints, are situated at the base of the architecture. These gadgets interact with or gather data from the real world. Their talents and levels of intricacy could differ. Micro-controllers and embedded systems are frequently found in devices, allowing them to process data locally before transferring it.

B. Communication Layer

Data communication between devices and the upper tiers of the Internet of Things architecture is facilitated by this layer. It covers both wired and wireless communication technologies. In the Internet of Things, common communication protocols include cellular networks, Bluetooth, Wi-Fi, Zigbee, and LoRaWAN. A number of variables, including data speed, power consumption, and range, influence the protocol chosen.

C. Edge Computing Layer

In order to reduce latency and bandwidth utilisation, edge computing, an optional layer in IoT architecture, processes data closer to the source. Gateways and edge servers may make up this tier. Data preparation, aggregation, and basic analysis are handled by edge devices. They preserve network resources by filtering and sending to the cloud only pertinent data.

D. IoT Platform Layer

By serving as a bridge, the IoT platform links devices to services and applications. It oversees data storage, device authentication, and device registration. Device management, data management, and application enablement features are frequently included at this layer. Depending on the needs, it may be hosted on-premises or in the cloud.

E. Data Processing and Analytics Layer

Large volumes of data are produced via IoT. This data must be processed in order for the data processing and analytics layer to produce insights. Data is processed, stored, and analysed using databases, machine learning algorithms, and analytics tools. Depending on the application, both batch and realtime processing are frequently used.

F. Application Layer

End-user or business applications are developed at the application layer. These apps make use of the processed data to deliver actions, alerts, and insights. Simple dashboards and alarm systems to intricate AI-driven decision-making systems are examples of applications.

G. Security Layer

A crucial element of the IoT architecture is security. It includes threat detection, access control, data encryption, and device authentication. This layer protects data from harmful assaults and unauthorised access by guaranteeing its confidentiality and integrity [3].

Fig. 2. OSI Model

IV. IoT SECURITY REQUIREMENTS

In IoT, all the devices and people are connected with each other to provide services at any time and at any place. Most

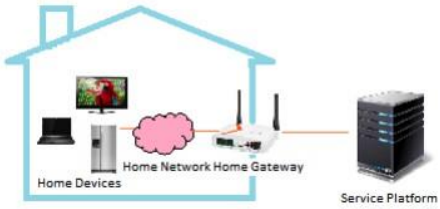

Fig. 3. Elements of a smart home in IoTs

Many internet-connected devices lack effective security features, leaving them open to different privacy and security risks, such as those involving confidentiality, integrity, and authenticity, among other concerns. A few security standards must be met for the Internet of Things in order to shield the network from malicious assaults. Here is a quick rundown of some of the most important features of a secure network.

A. Resilience to attacks

The system should be able to restore itself if it crashes during data transfer. For example, a server running in a multiuser environment must be clever and robust enough to defend itself against intruders or eavesdroppers. If it is down, it will recover without notifying users.

B. Data Authentication

The data and any accompanying information must be authenticated. An authentication technique is used to ensure that data is only transmitted from legitimate devices.

C. Access control

Access control is limited to authorised individuals. The system administrator must manage the users' usernames and passwords and define their access privileges so that different users may only access the necessary portions of the database or programs.

D. Client privacy

Ensuring data and information security is essential. Personal data should only be accessible by authorised individuals in order to protect the client's privacy. The technology ensures that no unauthorised users or clients may access the client's confidential information.

V. IOT SECURITY, PRIVACY, THREATS AND CHALLENGES

The Internet of Things has altered our lifestyles. Although the Internet of Things offers several benefits, it is vulnerable to a variety of security vulnerabilities in our daily lives. The most common security threats are information leaks and service disruptions. In IoT, security threats directly influence the physical security risk. The Internet of Things is made up of several devices and platforms, each with its own set of credentials, and each system requires security based on its unique characteristics. A user's privacy is also very crucial because a lot of personal information is transferred between various sorts of gadgets.

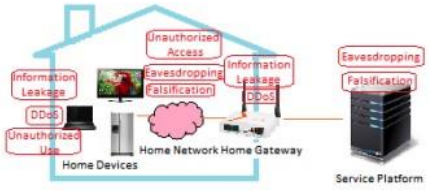

Fig. 4. Threats in smart home in IoTs

Thus, a secure technique is required to protect personal information.

Furthermore, for IoT services, there are several types of devices that communicate via different networks. There are significant security concerns about user privacy and the network layer. User privacy can also be compromised through other methods. Some security risks in the Internet of Things are as follows:

A. E2E Data life cycle protection

To ensure data security in an IoT context, endto-end data protection is given across the whole network. Data is collected from several linked devices and instantaneously shared with other devices. Thus, a framework is required to safeguard data, ensure data confidentiality, and manage information privacy across the data life cycle.

B. Secure thing planning

The connections and communication between IoT devices varies depending on the scenario. As a result, the devices must be capable of maintaining the required security level. For example, when local devices and sensors in a home-based network connect properly, their communication with external devices should follow the same security standard.

C. Visible/usable security and privacy

The majority of security and privacy vulnerabilities are caused by user misconfigurations. Implementing complicated security mechanisms and privacy regulations is challenging for users. It is necessary to pick security and privacy rules that may be implemented automatically.

D. Security Threats in Smart Home

Smart home services are vulnerable to cyber assaults since the bulk of service providers do not address security criteria in the early phases. Possible security dangers in a smart home include eavesdropping, Distributed Denial of Service (DDoS) attacks, and information leaking, among others. Unauthorised access poses a hazard to smart home networks.

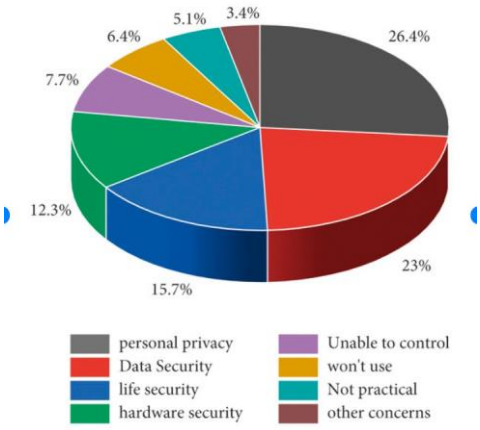

Fig. 5. IoT security worry statistics results graph

1) Trespass: Malicious codes or unauthorised access to smart door locks can allow attackers to enter a smart house without physically breaking the door.This impact might lead to the loss of life or property. To prevent such assaults, it is recommended to change passwords periodically. Passwords with at least 10 characters are more difficult for attackers to break. Similarly, authentication mechanisms and access controls may be used.

2) Monitoring and personal information leakage: One of the primary goals of a smart home is to ensure its safety. As a result, there are several sensors that are utilised for fire detection, infant monitoring, housebreaking, and other applications. If an attacker hacks these sensors, he will be able to monitor the residence and acquire personal information. To prevent this attack, consider using data encryption between the gateway and sensors or user authentication to detect unauthorised parties.

3) DoS/DDoS: Attackers may get access to the smart home network and send mass messages to smart devices, such as Clear To Send (CTS) and Request To Send (RTS). Malicious software can be used to attack specific devices and cause DoS assaults on connected smart home devices. As a result of the strain on resources caused by such assaults, smart gadgets are unable to execute full functionality. To avoid this attack, use authentication to restrict and detect unauthorised access.

4) Falsification: An attacker can collect packets from smart home devices that connect with the application server by changing the gateway's routing table. Despite the usage of SSL (secure socket layer), an attacker can still exploit the false certificate. In this strategy, the attacker may misinterpret the content of data or jeopardise its confidentiality. To secure the smart home network from this attack, an SSL method with a strong authentication mechanism should be employed. Unauthorised devices attempting to connect to a smart home network should also be refused access.

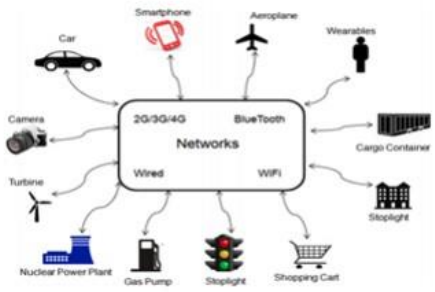

Fig. 6. Example of IoT system

a) The Internet of Things aided in the establish-ment of links between humans, physical items, and physical objects themselves. According to IDC, there will be 30 billion internet-connected gadgets by 2020. The growing expansion of internet data necessitates a more useful and secure network.:

b) The most hard part of IoT is security. Theapplication data for IoT might be industrial, corporate, consumer, or personal. This application's data should be kept private and confidential to avoid theft and tampering. For example, IoT apps might preserve a patient's health or improve purchase outcomes. Although the Internet of Things enhances device connection, scalability, availability, and reaction times remain concerns. When data is safely sent via the internet, security concerns arise. When data is sent over international boundaries, regulatory rules such as the Health Insurance Portability and Accountability Act (HIPA) may be enforced. Among various security issues, the most important IoT difficulties are addressed.

5) Data Privacy: Some smart TV makers gather client data to analyse watching habits, which may pose privacy concerns during transmission.

6) Data Security: Data security is also a significant concern. While delivering data effortlessly, it is critical to avoid being seen by internet devices.

7) Insurance Concerns: Insurance firms that install IoT devices on automobiles collect data on a driver's health and driving history before making insurance judgements.

8) Lack of Common Standard: There are several standards for IoT devices and industrial enterprises. As a result, distinguishing between approved and non-permitted devices linked to the internet presents a significant issue.

9) Technical Concerns: As the number of IoT devices grows, so does the amount of traffic they create. As a result, there is a need to enhance network capacity, which makes it difficult to store the massive amounts of data for processing and final storage.

10) Security Attacks and System Vulnerabilities: There has been a lot of effort done in the area of IoT security up until now.

Table I. A Summary of Different Types of Attacks and their Threat Levels, Their Nature & Suggested Solutions

Type	Threat level	Behavior	Suggested Solution
Passive	Low	Usually breach data confidentiality. Examples are passive eavesdropping and traffic analysis. Hostile silently listen the communication for his own benefits without altering the data.	Ensure confidentiality of data and do not allow an attacker to fetch information using symmetric encryption techniques.
Man in the Middle	Low to Medium	Alteration and eavesdropping are the examples of this attack. An eavesdropper can silently sense the transmission medium and can modify the data if encryption is not applied and steal the information that is being transmitted. Hostile may also manipulate the data.	Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission.
Eavesdropping	Low to Medium	The information content may be lost by an eavesdropper that silently senses the medium. For example in medical environment, privacy of a patient may be leaked.	Apply encryption on all the devices that perform communication.
Gathering	Medium to High	Occurs when data is gathered from different wireless or wired medium. Examples are skimming, tampering and eavesdropping. Data is being collected to detect messages. Messages may also be altered.	Encryption can be applied to prevent this kind of attack. Identity based method and message authentication code can also be applied in order to prevent the network from such malicious attacks.
Active	High	Effects confidentiality and integrity of data. Hostile can alter the integrity of messages, block messages, or may re-route the messages. It could be an internal attacker.	Ensure both confidentiality and integrity of data. To maintain data confidentiality, symmetric encryption can be applied. An authentication mechanism may be applied to allow data access to only authorized person.
Imitation	High	It impersonate for an unauthorized access. Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning can re-write or duplicate data.	To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack.
Privacy	High	Sensitive information of an individual or group may be disclosed. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy.	Apply anonymous data transmission. Transmit sample data instead of actual data. Can also apply techniques like ring signature and blind signature.
Interruption	High	Affects availability of data. This makes the network unavailable.	Applying authorization, only authorized users are allowed to access specific information to perform certain operation.
Routing diversion	High	Only the route is diverted showing the huge traffic and the response time increased.	Ensure connectivity based approach so no route will be diverted.
Blocking	Extremely High	It is type of DoS, jamming, or malware attacks. It sends huge streams of data which may leads to jamming of network, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network.	Turn on the firewall, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks.
Fabrication	Extremely High	Affects the authenticity of information. Hostile can inject false data and can destroy the authenticity of information.	Data authenticity can be applied to ensure that no information is changed during the transmission of data.
DoS	Extremely High	Malicious user may modify the packets or resend a packet again and again on network. User can also send bulk messages to devices in order to disturb the normal functionalities of devices.	Apply cryptographic techniques to ensure security of network. Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage.

There are three types of related work: system security, application security, and network security.

a) System Security: System security primarily focuses on the whole IoT system, identifying various security difficulties, designing various security frameworks, and providing adequate security guidelines in order to preserve network security.

b) Application security: Application Security addresses security challenges in IoT applications based on specific scenario needs.

c) Network security: Network security ensures secure communication between IoT devices.

VI. ANALYSIS OF DIFFERENT TYPES OF ATTACKS AND POSSIBLE SOLUTIONS

The Internet of Things is subject to a wide range of aggressive and passive attacks, which may swiftly interrupt operations and erase the benefits of its services. A passive assault happens when an invader just touches the node or takes data without physically harming it. Aggressive attacks, on the other hand, can interfere with physical performance. These active attacks are further classified into two types: internal and external attacks. Such vulnerable attacks can prevent devices from communicating successfully. To protect devices from harmful attacks, security measures must be applied.This section examines many types of assaults, their nature/behavior, and the threat level of such attacks.

1) Low-level attack: If an attacker attempts to attack a network but is unsuccessful,

2) Medium-level attack: If an attacker/intruder or eavesdropper is only listening to the medium without altering the integrity of the data.

3) High-level attack: An assault on a network can cause data integrity or modification.

4) Extremely High-level attack: An intruder/attacker may acquire unauthorised access to a network and undertake unlawful operations such as making it inaccessible, sending mass messages, or jamming it.

Table I displays several sorts of assaults, their danger levels, nature/behavior, and potential solutions to deal with these attacks.

VII. FUTURE RESEARCH DIRECTIONS

The Internet of Things (IoT) relies heavily on energy efficiency due to the limited resources of its devices, often powered by batteries or other constrained energy sources. Deployment scenarios for IoT are diverse, ranging from numerous and complex setups to remote locations. Given the vast scale of IoT networks, energy-efficient operating systems are crucial for their sustainability. Reduced Data Copying (RDC) is utilized to enhance energy efficiency, requiring precise synchronization of devices. Real-time capabilities of IoT devices are essential for meeting strict deadlines, especially in applications like the Internet of Body (IoB), necessitating

support for RealTime Operating Systems (RTOS) within IoT operating systems. Network connections are vital for both incoming and outgoing data traffic, often employing multiple interfaces for communication across different spectrum's. Continual development of industrystandard protocols at various levels is necessary to facilitate seamless integration and networking in IoT environments. Security and privacy are paramount, particularly in critical systems such as healthcare, smart homes, and smart cities, and should be ensured by IoT operating systems.

VIII. HOW TO PROTECT IOT SYSTEMS AND DEVICES

Businesses can enhance their data security stance by utilizing the following technologies and tools:

1) Ensuring IoT security is integrated throughout the entire design process is crucial. This comprehensive approach can effectively address various risks and challenges associated with IoT devices, particularly during the research and development phase. Implementing secure operating systems and hardware, along with default security settings, is essential. IoT developers should remain vigilant about cybersecurity risks at every stage of development, not just during the initial design phase. For instance, storing key fobs in a secure location can prevent hacking incidents while driving. 2) Employing infrastructure equipped with public keys and digital certificates is essential. Public Key Infrastructure (PKI) can safeguard clientserver communications across multiple networked devices. By utilizing digital certificates and a two-key asymmetric cryptosystem, PKI facilitates secure encryption and decryption of private exchanges. These measures are critical for protecting sensitive user data entered into websites for private transactions, ensuring the functionality of e-commerce platforms. 3.Securing networks is paramount in protecting IoT devices from remote exploitation by threat actors. It's imperative to incorporate both digital and physical components into network defenses to fully safeguard on-premises IoT devices against potential threats. Defending IoT networks effectively requires a multilayered approach.

IX. CONCLUSION

The main topics of discussion in this article are significant IoT security threats and countermeasures. Many IoT devices become soft targets due to a lack of security mechanisms, even when the victim is not aware that the device is infected. Confidentiality, integrity, and authentication are a few of the security requirements covered in this article. Twelve primary assault types are categorized by this poll. The nature, behavior, and suggested strategies for handling low-, medium-, high-, and extremely high-level assaults are all covered in this article.

IoT devices and communication networks must incorporate security measures due to the significance of security in IoT applications. Additionally, to safeguard. Additionally, users are advised to research the security requirements before utilizing a device's default password and to avoid using them altogether. Security risks can be decreased by turning off unused functionality. Additionally, it's imperative to look into the different security techniques used in IoT networks and devices.

REFERENCES

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, pp. 1497-1516, 2021.

[2] M. Zhang, F. Sun , and X. Cheng, "Architecture of Internet of Things and Its Key Technology Integration Based-On RFID," presented at the Fifth International Symposium Computer Intelligence Design, 2022.

[3] S. Santhi, P. Rajendra, and Y. Vijayalakshmi, "A review on the state of art of Internet of Things," International Journal of Advanced Research in Computer and Communication Engineering (IJARCEE), vol. 5, July 2020.

[4] L. Yan, The Internet of things: From RFID to the nextgeneration pervasive networked systems. New York: Auerbach Publications, 2012. S. Das, K. Kant, and N. Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure: Morgan Kaufmann, 2022..

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey,"Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2020.

[6] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey onInternet of Things from industrial market perspective," IEEE Access,vol. 2, pp. 1660–1679, 2021.

[7] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing andits role in the Internet of Things," in Proc. 1st Ed. MCC WorkshopMobile Cloud Comput., Helsinki, Finland, 2023, pp. 13–16.

[8] F. Wang, L. Hu, J. Zhou, and K. Zhao, "A survey from the perspectiveof evolutionary process in the Internet of Things," Int. J. Distrib. SensorNetw., vol. 11, Jan. 2019, Art. no. 9.

[9] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet ofThings: Vision, applications and research challenges," Ad Hoc Netw.,vol. 10, no. 7, pp. 1497–1516, 2022.

[10] D. Uckelmann, M. Harrison, and F. Michahelles, Architecting theInternet of Things. Heidelberg, Germany: Springer, Jan. 2023,pp. 1–353.

[11] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey,"IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2233–2243, Nov. 2021.

[12] R. H. Weber, "Internet of things–new security and privacy challenges," Computer law security review, vol. 26, no. 1, pp. 23–30, 2020.

[13] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot),"in International Conference on Network Security and Applications. Springer, 2020, pp. 420–429

[14] Y. H. Hwang, "Iot security privacy: threats and challenges," in Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. ACM, 2023, pp. 1–1.

[15] M. A. Qureshi, A. Aziz, B. Ahmed, A. Khalid, and H. Munir, "Comparative analysis and implementation of efficientdigital image watermarking schemes," International Journal of Computer and Electrical Engineering, vol. 4, no. 4, p. 558, 2022.

[16] M. Abdur Razzaq, R. A. Sheikh, A. Baig, and A. Ahmad, "Digital image security: Fusion of encryption, steganography and watermarking," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 5, 2021.

[17] S. Singh and N. Singh, "Internet of things (iot): Security challenges, business opportunities reference architecture for e-commerce," in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2023, pp. 1577–1581.

[18] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," The Internet Society (ISOC), pp. 1–50, 2021.

[19] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer, vol. 46, no. 4, pp. 46–53, 2023.

[20] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233– 2243, 2021.

[21] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M.. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2022, pp. 6121–6125.

[22] A. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2023, pp. 372–374.