RESEARCH ARTICLE

SAMRIDDHI Volume 14, Issue 2, 2022 Print ISSN: 2229-7111 Online ISSN: 2454-5767

Comparative Analysis of Security Issues and Trends in IoT and WSN

Vishal Choudhary, Animesh Srivastava, Anoop Kumar, Sunil Taruna

Banasthali Vidyapith, Tonk, Rajasthan, India

Abstract

Recent advancements in the field of wireless sensor networks and the internet of things market give rise to security concerns. While using the application of these technologies in the real world, many security issues have emerged. There are security risks involved in using IoT and WSN devices in areas such as financial, health, and business, as well as in industry. Security requirements are exponentially increasing with the demand for IoT devices in the market around the world. The trends have shown that the WSN field is slowly merging into the IoT ecosystem. Another factor that encourages the integration of the WSN field in IoT is advancements in addressing and the internet of everything. If we study both technologies in minute detail, we will find that although both technologies are interrelated, there is a huge difference in application areas, connectivity issues, routing issues, security issues, etc. WSN gives great importance to the efficient management of constrained resources. On the other hand, security, scalability, quality of service, and heterogeneity are the main concerns in IoT systems. In this paper, there is a detailed analysis of several factors, requirements, and trends in the advancement of both technologies.

Keywords: Internet of Things, Intrusion, Security, Security Issue, Wireless Sensor Networks.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2022); DOI: 10.18090/samriddhi.v14i02.00

Introduction

The main function of the WSN is to collect and transmit the data in a suitable format to a sink node. On the other hand, the Internet of Things is a combination of technologies and protocols to collect, process, and transmit the data for the appropriate application or decision-making process over the computer network. Moreover, IoT devices that are directly connected to the Internet use traditional communication protocols, but wireless networks need innovative methods for routing the information within the network. The data within the sensor network is routed to a particular node, also known as a sink node. WSN is an integral part of the IoT infrastructure in the process of connecting everyday things. Security and safety are important areas in both technologies. The encryption, authentication, and freshness of data originating from sensor nodes is a prominent issue for the correct operation of any application in WSN and IoT. For WSN, the security level differs based on the area of applications, e.g., military and critical infrastructure monitoring applications. The security of WSN is at the highest level. On the other hand, for IoT, there is a need for integrating different security policies and techniques to ensure integrity, authenticity, and confidentiality. All these requirements make the implementation of security in IoT devices more complex. In WSN, the unique identification of each node is not required, whereas, for IoT, each node or device needs a unique identification to ensure proper communication and control of IoT devices follows the proper addressing scheme. In WSN, data processing is limited to data aggregation for reducing network congestion,[3] whereas in IoT, data processing is not only limited to data aggregation and filtration but also includes applying data analytics techniques for transforming the data into information and information into knowledge in all IoT applications. In WSN, internet connection is not the basic requirement as all nodes are interconnected through wireless channels.[8] The sink nodes can receive aggregated data from all the nodes in the network, which in turn sends data towards the server. In IoT, the Internet connection is a mandatory characteristic. Other mandatory requirements for IoT applications are location-aware service, dynamic network

Corresponding Author: Vishal Choudhary, Banasthali Vidyapith, Tonk, Rajasthan, India, e-mail: vishalhim@yahoo.com

How to cite this article: Choudhary, V., Srivastava, A., Kumar, A., Taruna, S. (2022). Comparative Analysis of Security Issues and Trends in IoT and WSN. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 14(2), 1-7.

Source of support: Nil

Conflict of interest: None

configuration, interoperability compliance with rules and regulations, etc.

In an IoT system, all sensors directly send their information to the internet. in a WSN, there is no direct connection to the internet. Instead, the various sensors are connected to some kind of router or central node. A person may then route the data from the router or central node as they see fit.

WSN: sensor nodes connected without a wire to gather some data.

IoT: WSN+ Any Physical object (Thing)+IP address+ Internet + App + Cloud computing+ etc.

Security Threats in IoT

IoT devices encounter many security threats. Some of them are as follows.

Wrong Access Control

Services that are offered by IoT devices should only be accessed by the owner and the people for whom it is made. However, access control is insufficiently enforced in the security system of any IoT device. IoT devices when connected to the Internet then everyone in the world can access the functionality offered by the device if access control is not enforced efficiently. Also, one common problem is universal username and password for hardware devices.

Use of Outdated Software

Many IoT devices auto-update is not possible, the outdated software has many vulnerability issues that are discovered after the deployment of the devices in fields. There is a need for auto-update functionality on the IoT hardware.

Bugs in Application Software

Bugs in the application software of IoT devices are another security issue, during the development phase it is impossible to find all vulnerabilities. So, there is a need for consistent testing to avoid the possible vulnerabilities in application software.

Weak Encryption

Many IoT applications transmit the data without any encryption to reduce the complexity, even if data is encrypted still weakness may be present due to strong encryption methods like authentication cannot be put into operation on low-power IoT devices. So, it is easy to perform a Man-in-the-middle attack. There is a need for strong lightweight cryptographic algorithms[9] for IoT devices.

Weak Intrusion Detection

Most IoT devices don't have logging or alerting capabilities to warn owners of any security problems.[5] As result owners are hardly able to discover that their device has been compromised or attacked. There is a need for efficient intrusion detection methods for intrusion detection in IoT systems.

Security Threat in WSN

The WSN is integrated with next-generation IoT technologies and has gained enormous attention. But in the present scenario, the system is implemented without sufficient security requirements.[7] The WSN and IoT applications that don't consider security requirements may provide hackers or attackers a window for attacks and crack the system. The essential security threats in any WSN environment are as follows.

Physical Layer Attacks

Attacks on the physical layer[2] are directly related to a disturbance at the hardware level of a device, the physical attacks range from the attacks that damage the nodes to jamming of the radio channels with different frequencies. Physical layer attacks are hard to avoid but strong encryption methods can secure the data in case of node tempering. An efficient frequency hopping technique can avoid channel jamming.

Datalink Layer Attacks

The data link layer plays a major role in channel access as well synchronization of nodes with neighboring nodes. This layer is more prunes to attacks like traffic analysis, collisions, exhaustion, etc. if intruders deduce the communication patterns of nodes by eavesdropping then significant information can be leaked, which can lead to compromise of the entire system. In case, if few nodes get compromised in the system, then compromised nodes don't follow the MAC protocols and cause the collision in the transmission system of sensor networks. If the collision attacks continue then the energy of nodes is exhausted also known as exhaustion attack.

Network Layer Attacks

The network layer is prone to denial-of-service attacks and replays attacks. The main purpose of these attacks is to create disruption in network operation or to destroy the integrity of data. The ad-hoc nature of WSN makes it more vulnerable to such kinds of attacks.

Transport Layer Attacks

The attacks on the transport layer[2] are generally used to disrupt the connection by continuously requesting a new connection. The attack exploits the characteristics of resource-constrained sensor nodes. The communication between the sensor nodes is desynchronized by changing the order in which nodes access the shared resources. The flooding at the transport layer causes the disruption in legitimate requests until resources are exhausted.

Application Layer Attacks

There are various applications of WSN, where nodes are deployed in a hostile environment and are remotely managed. There is a strong probability that intruders can reprogram the deployed nodes. If the intruders are successful in re-programming the nodes, then they may hijack the system and take control of the network.

Key Requirements in IoT Security

The IoT devices that are produced through weak and insecure manufacturing processes provide intruders an opportunity to change production parameters as well as an opportunity to clone the device. The Foundation of security requirements in IoT applications depends on ensuring that each connected device must have unique identification and the manufacturer of the device must equip the device with a unique ID using the efficient cryptographic technique so that it cannot be tempered at a later stage. A strong policy must be implemented for end-to-end encryption of data and communication.[10] There is a need for a strong authentication procedure to ensure that the connected /connecting device can be trusted. The IoT device market must be regulated in such a way that no device rolls out in the market without a security benchmark. It is hard for consumers to test whether a device is secure against attacks. The security regulations that are presently followed by some organizations are:

- Strong passwords
- Multifactor authentication
- Unique device password
- No method to reset the device password to the default factory setting
- Guidelines for configuration management for IoT devices.
- Use of Public key infrastructure (PKI) technology

Key Requirements in WSN Security

WSNs are low-powered devices, have limited storage and processing capability, these limitations cause security-related issues.[4] In a wireless sensor network, there is a requirement that the data should not be revealed to an unauthorized party, there should be a mechanism for differentiating the authorized and non-authorized users/devices in the network, there should be a mechanism to ensure that data should not be altered on any stage. Data should not be duplicated or replicated within the sensor network, based on the analysis we have found the following requirement for WSN security.

- Access control
- Authentication
- Data availability
- Data confidentiality
- Data freshness
- Data integrity
- Quality of service
- Secure Localization
- Self-organization
- Time synchronization

The key requirements in both areas are similar.[6] The difference in the security requirement based on relevance is shown in the Table 1

IoT Challenges

IoT devices are designed to assist humans with different tasks that are not easy to perform manually. But there are many risks involved in using these devices. Cyber attacks on IoT applications are emerging. a major challenge due to the complexity of protocols, devices, and topologies. IoT systems interacting with each other need to be trustworthy to prevent various forms of security negligence attacks.

The manufacturing of various kinds of IoT devices is increasing rapidly. And there is a lack of experts to handle

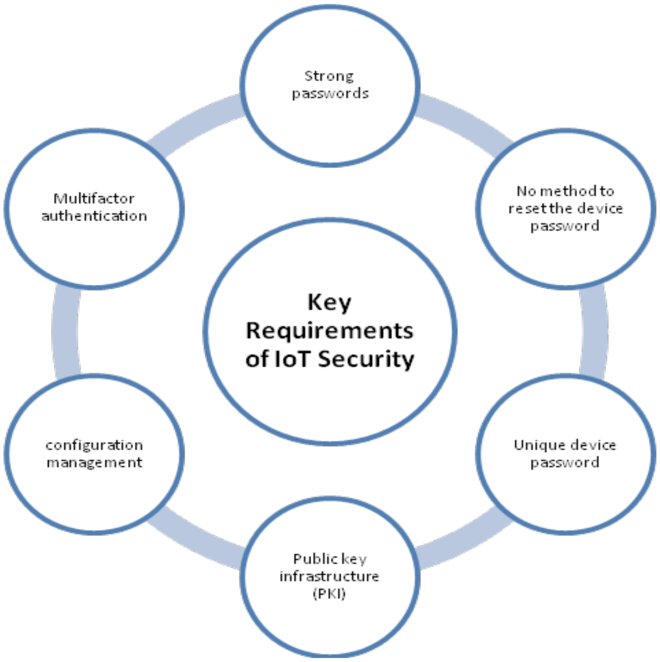
Strong passwords
No method to reset the device password
Unique device password
Public key infrastructure (PKI)
configuration management
Multifactor authentication
Key Requirements of IoT Security

Figure 1: Key Requirements in IoT Security

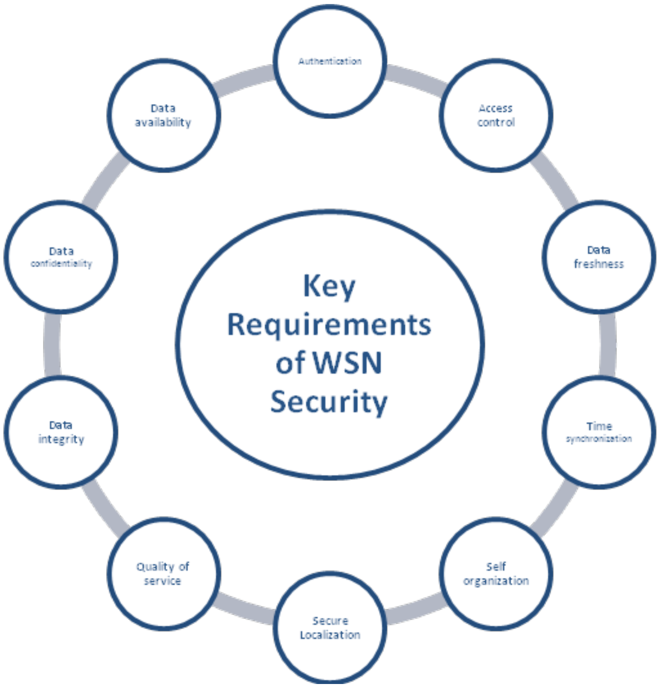

Figure 2: Key Requirements in WSN Security

Table 1: Potential security requirements for the IoT Vs WSN

Parameters	*WSN*	*IoT*
Internet Connectivity	Low	High
Communication	High	High
Data Processing	Low	High
Node identity	Low	High
Node density	High	Low
Power Management	High	Low
Mobility	Medium	Medium
Heterogeneity of component	Low	High
Scalability	Medium	High
Security	High	High

such devices. So, the skill gap induced the security challenge to handle IoT devices. Right now, in this field, humans are not aware of how to handle or not aware of the lack of security. So, we also need to make people aware of this fact.

AI and Automation

For enterprise applications there is a huge amount of data generated as the number of devices increases rapidly there is a challenge to handle such data based on the security front. There is difficulty in detecting an anomaly in data. When this data is applied for the autonomous decision-making process, then the single error in code can bring down the entire infrastructure.

Insufficient Testing and Updation

There are many players in the IoT market and most IoT products don't get sufficient updates or no updates at all. The device which is considered secure may become insecure when flaws are discovered in the future. Also, there is no robust testing procedure followed by the manufacturer of the IoT device.[17] This exposes the customers to potential attacks as a result of outdated hardware and software.

WSN Security Challenges

WSN poses different types of challenges related to addressing, scalability, reliability, SDN integration, and virtualization. Some of the security challenges in WSN are as follows.

Wireless connectivity

Wireless signals are easy to tap in contrast to wired signals. So, it is a weak point in front of security. Wireless channels are the most compromised transmission medium. Wireless infrastructure provides mobility, convenience low-cost, and remote access control. But it poses the challenges of security and reliability.[18]

Key Management and Distribution

Key distribution and management is another challenge in WSN.[11] There is communication overhead during the authentication phase and searching phase. Also, there are limitations in both public-key cryptography and secret-key cryptography. There is a trade-off among cryptographic techniques in front of sensor processing capabilities, power, and applications requirements.

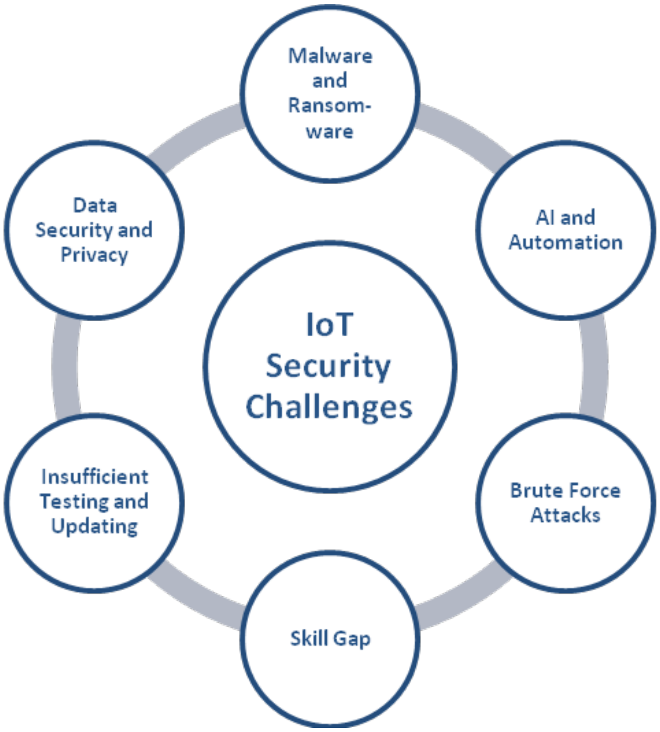

Figure 3: IoT Security Challenges

WSN Virtualization

The wireless sensor network hardware is difficult to virtualize. The separation of services and infrastructure provides many flexibilities and ease of deployment. The virtualization of WSN hardware is another challenge in the industry.

Integration

The hardware and software used in sensor networks are purchased from different manufacturers, integrating these heterogeneous nodes leads to compatibility problems. These issues lead to further challenges in scalability, synchronization, and maintainability.

Programming WSN

WSN contains many heterogeneous protocols, resource-constraints devices. To program the network with such constrained is another challenge the WSN experts are facing.[15]

Intrusion Detection

Intrusion detection creates extra complexity to WSN.[5] The integration of an intrusion detection system with a wireless sensor network is a complex task. The process of intrusion detection consumes network resources and the energy of resource constrained WSN.

Security Defence In WSN

There is a need for a robust security mechanism at each level of WSN. The different layers architecture is designed in such a way that different types of security attacks must be detected and appropriate defense mechanisms can be applied on time.[13] Link layers architecture must be designed in such a way that it can detect unauthorized packets when they are first injected into the network. Jamming attacks at different layers may be prevented using code spreading, spread-spectrum using frequency hopping. Collision attacks at link layers can be avoided by error-correcting codes as well as using media access control. A defense against spoofing and alteration is to append message authentication code at the end of each message.[12] At transport layer flooding using DoS attacks can be countered by using the client puzzle technique. Sybil attacks can be countered with the help of identity-based encryption techniques. Several intrusion detection techniques can be applied in the network to check the abnormal behavior within the network. Temper-resistance hardware is the technique to avoid physical layer attacks. Lightweight encryption techniques are generally used to protect the data during transmission within wireless sensor networks. The key points that must be dealt with at each layer are described in the Table 2.

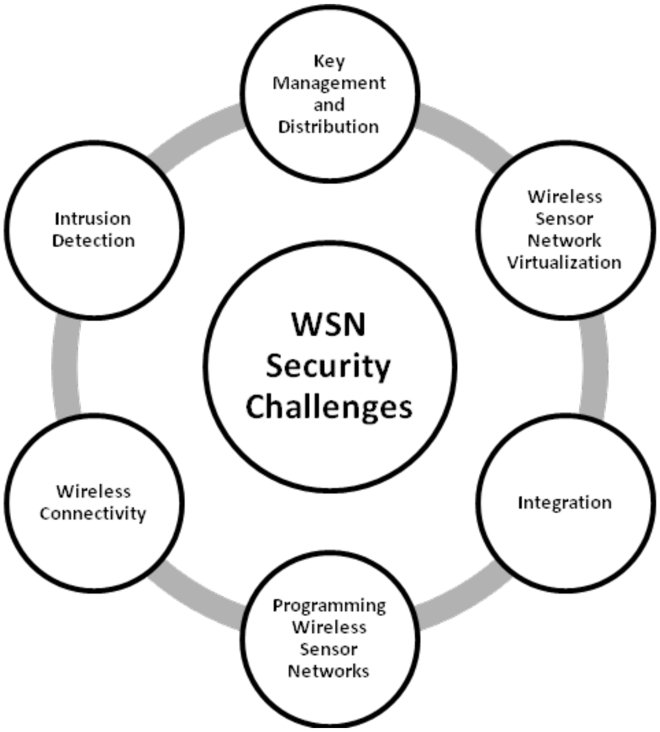
WSN Security Challenges
Key Management and Distribution
Wireless Sensor Network Virtualization
Integration
Programming Wireless Sensor Networks
Wireless Connectivity
Intrusion Detection

Figure 4: WSN Security Challenge

Security Defence in IoT

In IoT devices, most of the security threats,[1] originate from the device itself. Threats also originate from wireless communication media. There is a need for proper cryptographic techniques that must be implemented in

Table 2: Layer wise attacks and security defense mechanism in WSN

Layers in WSN	*Types of Attacks*	*Security defense*
Application Layer	Node cloning, Re-programming	Data encryption techniques, authentication, and authorization, Multipath routing
Transport Layer	Flooding, de-synchronization, Path-based DOS attack	Authentication techniques, anti-replay protection
Network Layer	Jamming, Sybil attack, sinkhole, Hello flood, Node Capture, selective forwarding, Blackhole attack, wormhole attack, spoofed	Counters, timestamps, encryption, Multipath routing, Geo-routing protocols, public-key cryptography, and digital signatures.
Data Link Layer	Jamming, Collision, Exhaustion, unfairness, interrogation, Sybil attack	Error-correcting code, Rate limitation,
Physical Layer	Jamming, Tampering	Frequency-hopping spread spectrum, Priority messages, Tamper proofing

Table 3: Layer wise attacks and security defense mechanism in IOT

Layers in IoT	*Types of Attacks*	*Security defense*
Business Logic Layer	Business Logic Attack, Zero-Day attack	Access Control Mechanisms, Authentication
Application Layer	Malicious Code Attack	Authentication, Privacy protection, Information Security Management
Processing Layer	Exhaustion attacks, Malware	Antivirus, firewall
Network Layer	Man-in-The-Middle Attack, Denial of Service Attack,	Intrusion Detection, Routing Security, Authentication, Key Management
Perception Layer	Eavesdropping, Node Capture, Fake Node and Malicious node, timing attacks	Lightweight-Encryption, authentication, Key Agreement, Data Confidentiality

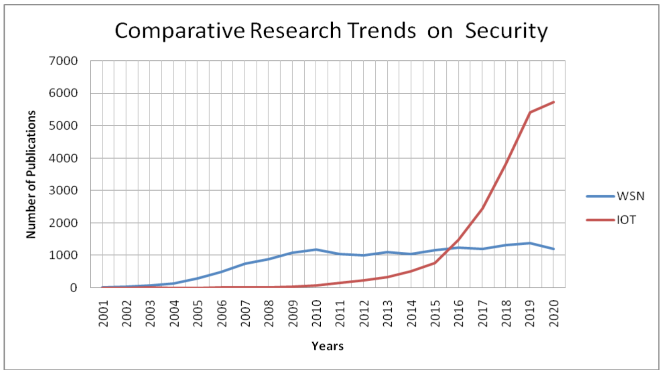

Figure 5: Comparative Research trends in IoT Vs WSN

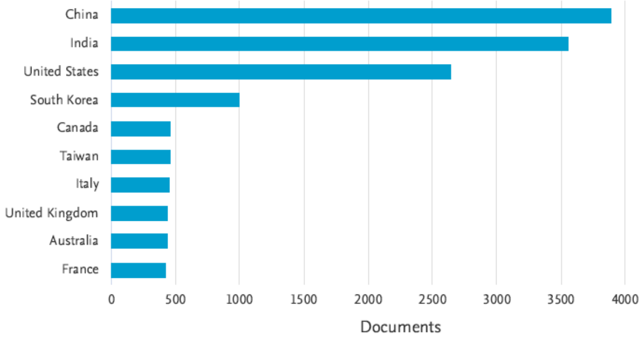

Figure 6: Research publication country wise

IoT infrastructure. All the communication entities must have strong authentication and encryption mechanism. The business layer is used in IoT architecture to perform data analysis and modeling, in this layer there is a need for a robust access control mechanism. The application layer generally deals with application logic, so at this layer, there is a need for strong security management protocols. Network layers need secure routing protocols. The perception layer contains hardware devices that must be temper resistant. Few security defense techniques at each layer are highlighted in the Table 3.

Research Trends on Security Issues

The Scopus database analysis for research trends on the security issues in both IoT and WSN in the last 20 years has shown that until 2010 there was low importance for security in IoT and thereafter there is a drastic increase in security issues in IoT devices. Whereas for wireless sensor networks there is a linear approach to security issues. As we have seen that the IoT product market has shown enough progress in the last 10 years, consequently there is demand for security in IoT devices. As per the Scopus database repository, the top three countries working on security issues are china, India, and the USA respectively. Around 65% of research is going on in the domain of Computer science and Engineering and around 7 % in the field of mathematics.

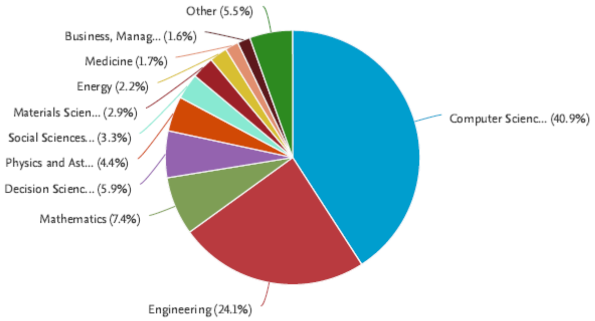

Figure 7: Research Publication in key domains.

Conclusion

IoT and WSN devices are highly vulnerable to various security attacks, ranging from hacking to cracking. Traditional security protocols need high-end devices to have those must-have capabilities for data processing, storing, analysis, encryption, and decryption. There are risks involved in using IoT and WSN devices in areas such as financial, health, and business, as well as in industry. Security requirements are exponentially increasing with the demand for IoT devices in the market around the world. The trends have shown that the WSN field is slowly merging into the IoT ecosystem. Another factor that encourages the integration of the WSN field in IoT is advancements in addressing and the internet of everything. If we study both technologies in minute detail, then it is found that although both technologies are interrelated, there is a huge difference in the application areas where they are applied. WSN gives great importance to the efficient management of constrained resources. On the other hand, security, scalability, quality of service, and heterogeneity are the main concerns in IoT systems. Sensor networks need to satisfy the constraints introduced by factors such as fault tolerance, power consumption, routing, and QoS provisioning. The data collected by the IoT is susceptible to different types of attacks. An attack can happen to the data in different circumstances, either at rest on an IoT device or during transmission.

References

[1] Alharbi, R., & Aspinall, D. (2018). An IoT Analysis Framework: An Investigation of IoT Smart Cameras' Vulnerabilities. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. https://doi.org/10.1049/cp.2018.0047

[2] Choudhary, V. (2017). Fuzzy Analysis for Nodes Deployment Strategies in Wireless Sensor Network. *International Journal on Recent and Innovation Trends in Computing and Communication*, *5*(6), 852–855. https://doi.org/10.17762/ijritcc.v5i6.866

[3] Choudhary, V., & Taruna, S. (2018). A Distributed Key Management Protocol for Wireless Sensor Network. *Communications in Computer and Information Science*, 243–256. https://doi.org/10.1007/978-981-13-3143-5_21

[4] Choudhary, V., & Taruna, S. (2020). The highly secure polynomial

pool-based key pre-distribution scheme for wireless sensor network. *Journal of Discrete Mathematical Sciences and Cryptography*, *23*(1), 95–114. https://doi.org/10.1080/09720529.2020.1721880

[5] Choudhary, V., & Taruna, S. (2021). An Intrusion Detection Technique Using Frequency Analysis for Wireless Sensor Network. *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. https://doi.org/10.1109/icccis51004.2021.9397076

[6] Choudhary, V., Taruna, D. S., & Purbey, L. B. (2018). A Comparative Analysis of Cryptographic Keys and Security. *2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)*. https://doi.org/10.1109/icraie.2018.8710431

[7] Gupta, S., Bharti, P. K., & Choudhary, V. (2011). Fuzzy Logic Based Routing Algorithm for Mobile Ad Hoc Networks. *High Performance Architecture and Grid Computing*, 574–579. https://doi.org/10.1007/978-3-642-22577-2_76

[8] Kavak, A., & Kucuk, K. (2009). On connectivity analysis of smart antenna capable wireless sensor networks. *2009 6th International Symposium on Wireless Communication Systems*. https://doi.org/10.1109/iswcs.2009.5285278

[9] Li, Y. X., Qin, L., & Liang, Q. (2010). Research on Wireless Sensor Network Security. *2010 International Conference on Computational Intelligence and Security*. https://doi.org/10.1109/cis.2010.113

[10] Manrique, J. A., Rueda-Rueda, J. S., & Portocarrero, J. M. (2016). Contrasting Internet of Things and Wireless Sensor Network from a Conceptual Overview. *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2016.66

[11] Mohammed, A. F., & Qyser, A. A. M. (2020). A Survey on Security Mechanisms in IoT. *2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE)*. https://doi.org/10.1109/ic-etite47903.2020.172

[12] Mohammed, S., & Al-Jammas, M. H. (2020). Data Security System for IoT Applications. *2020 International Conference on Advanced Science and Engineering (ICOASE)*. https://doi.org/10.1109/icoase51841.2020.9436579

[13] Sun, Y., Guo, S., Cheung, S. C., & Tang, Y. (2019). Analyzing and Disentangling Interleaved Interrupt-Driven IoT Programs. *IEEE Internet of Things Journal*, *6*(3), 5376–5386. https://doi.org/10.1109/jiot.2019.2900769

[14] Tellez, M., El-Tawab, S., & Heydari, M. H. (2016). IoT security attacks using reverse engineering methods on WSN applications. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. https://doi.org/10.1109/wf-iot.2016.7845429

[15] Vishal, & Taruna, S. (2020). An Efficient Quantum Key Management Scheme. *Advances in Intelligent Systems and Computing*, 269–277. https://doi.org/10.1007/978-3-030-39875-0_29

[16] Xia, S., Chen, D., Wang, R., Li, J., & Zhang, X. (2020). Geometric Primitives in LiDAR Point Clouds: A Review. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *13*, 685–707. https://doi.org/10.1109/jstars.2020.2969119

[17] Yu, J. Y., Lee, E., Oh, S. R., Seo, Y. D., & Kim, Y. G. (2020). A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security. *IEEE Access*, *8*, 45304–45324. https://doi.org/10.1109/access.2020.2977778

[18] Zahra, S. R., & Ahsan Chishti, M. (2019). RansomWare and Internet of Things: A New Security Nightmare. *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. https://doi.org/10.1109/confluence.2019.8776926