VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELAGAVI

SEMINAR REPORT

On

"SECURE AND RELABLE WSN FOR IOT"

In

Computer Science and Engineering

For the Academic Year: 2021-2022

By

USN: 3VC19CS414

NAME: Vinit K

Under the Guidance of

V SHIVA KUMAR
Asst. Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

RAO BAHADUR Y MAHABALESHWARAPPA ENGINEERING COLLEGE

CANTONMENT, Ballari-583104, KARNATAKA

2021 – 2022

VEERASHAIVA VIDYAVARDAHKA SANGHA'S

RAO BAHADUR Y MAHABALESHWARAPPA ENGINEERING COLLEGE

AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM & APPROVED BY AICTE & ACCREDITED BY NBA, NEWDELHI)

BELLARY – 583104, KARNATAKA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL BOARD of ACCREDITATION

CERTIFICATE

Certified that the seminar entitled **"SECURE AND RELABLE WSN FOR"** is carried out by **VINIT K bearing USN: 3VC19CS414** is a bonifide students of Department of Computer Science and Engineering of **Rao Bahadur Y. Mahabaleswarappa College of Engineering** in partial fulfillment of Industry Oriented Seminar of Management and Entrepreneurship on IT Industry as a part of an assessment report and completed successfully.

V Shiva Kumar
Asst. Professor
Department of CSE

Dr.H Girisha
Professor & Head
Department of CSE

Acknowledgement

I would like to express our regards and acknowledgement to all those who helped in making this seminar possible.

I am grateful to the **Principal Dr. T Hanumantha Reddy** for providing facilities and untiring zeal, which constantly inspired me towards the attainment of everlasting knowledge throughout the course.

I am deeply indebted to **Dr. H Girisha Professor and Head** of **Department of Computer Science and Engineering** for the valuable suggestions and constant encouragement provided for the successful completion of Industry oriented seminar on Management and Entrepreneurship on IT Industry.

I would like to thank our guide**, V Shiva Kumar,** Asst. Professor and coordinator, **Suresh K,** Asst. Professor of **Department of Computer Science andEngineering** for the constant guidance for the successful completion of technical seminar.

Finally, I would like to thank all the staff members **of Computer Science and Engineering Department** for their guidance and support. I am also thankful to my family and friends who continue to give me best support.

Vinit K

3VC19CS414

Abstract

Wireless Sensor Network (WSN) is an innovative technology with a broad range of applications and highly attractive benefits, such as low cost of implementation and data transmission, unmonitored access to the network, autonomous and long-term operation. With extensive demand for the advancement of related technologies (cloud computing, near-field communications and cellular mobile networks), the Internet of Things (IOT) is becoming a very exciting paradigm. By using communication technologies in sensors and sensing features in web devices, WSNs have begun interaction with the IOT devices.

IOT provides access to a large amount of information gathered by WSNs. However, the security of WSN and IOT comes at a cost, mainly due to privacy management issues. Therefore, this Topic offers a comprehensive analysis of security threats against WSN and IOT, along with the strategies for preventing, detecting and mitigating those threats. The related defense mechanisms can help in building a safe IOT expansion and widespread understanding by getting familiar with the details of these attacks. The aim of this Topic is to address and demonstrate the impact of the security problems on WSNs from the viewpoint of the IOT and its applications. In the analysis carried out for this work, a classification of available attacks and threats against these requirements has also been included.

CONTENTS

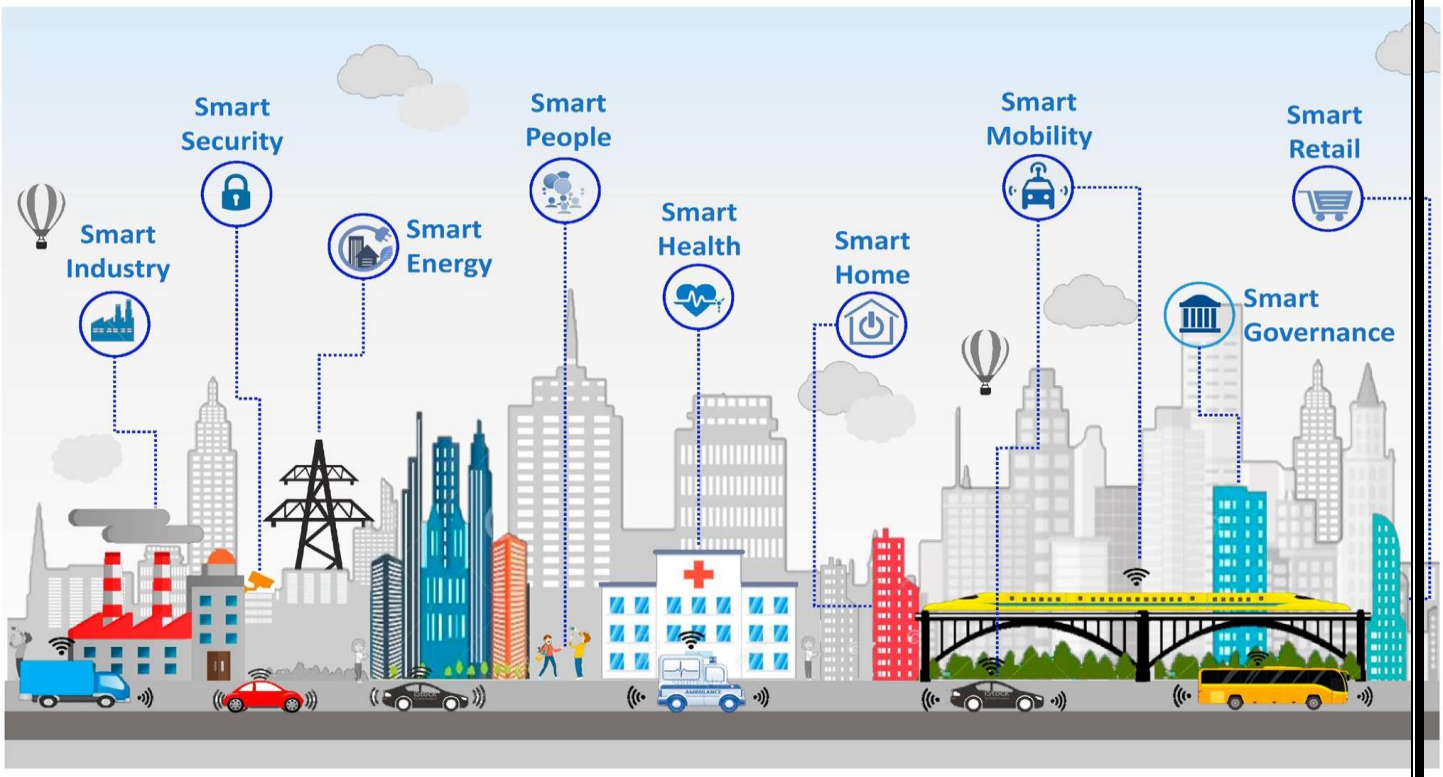
1.Introduction

Wireless Sensor Networks (WSNs) are one of the major technologies required for the implementation of Internet of Things (IOT) architecture. WSNs are the networks used for communication between sensors and radio transceivers. The functional capability and energy of IOT depends on the network interaction, cost efficiency, reliability, stability and productive operation. The developments in Micro Electro Mechanical Systems (MEMS) for wireless communication technologies have made it possible to design WSNs by collecting data from their local environments and transmitting information wirelessly to a realistic sink. The things connected to the internet vary greatly in terms of features. IOT is emerging as a dynamic cyber-physical network that is enabling smart devices to sense and change the world. Further it will assist the humanity in functioning and living.

The protocols used for communication and messaging are one of the key requirements of an IOT system. IOT will integrate a variety of applications into the Internet, e.g., automation, weather sensing, and Smart Grids. WSNs have started to merge with the Internet of Things through the introduction of Internet access capability in sensor nodes and sensing ability in Internet-connected devices. Thereby, the IOT is providing access to huge amount of data, collected by the WSNs, over the Internet. However, owing to the absence of a physical line-of-defence,

More specifically, for the application areas in which CIA (confidentiality, integrity, and availability) has prime importance, WSNs and emerging IOT technology might constitute an open avenue for the attackers. Besides, recent integration and collaboration of WSNs with IOT has opened new challenges and problems in terms of security. A smart object network can access the cloud directly through a gateway via cloud services. One of the essential tasks of the IOT is to incorporate the WSN as the primary communication technology for the IOT. WSN has standards which enable the devices to communicate with each other and with the edge gateway.

The rapid growth in IOT technologies to enable smart living, smart houses, smart workplaces and smart city. For these applications also, detailed investigation of WSN and IOT integration along with security requirements is essential. This study is extremely thorough and systematic as it covers all attacks on WSN, detection and preventive measures for WSN and IOT integration. Moreover, apart from the strategies discovered while learning to secure WSNs, this topic also provides a guide for defending IOT against such attacks.



SMART CITY

2.Literature Survey

Wireless Sensor Networks (WSNs) are emerging as a new area of research in wireless technology. WSN is constructed with more number of inexpensive, tiny sized and battery powered sensor nodes. These senor nodes are utilized for sensing the environmental conditions that are widely deployed in diverse harsh environments like military applications, climate and habitat monitoring, acoustic data gathering, civil applications, surveillance as well. The key limitation of WSN is its processing, security and power consumption. These limitations of sensor nodes call for the immediate development of energy efficient and secure communication protocols. Recently, more research works have been focused on solving the challenges in routing that ensures the energy, security and reliability of the network.

Wireless sensor networks (WSNs) consist of networks composed of devices equipped with sensing, processing, storage, and wireless communication capabilities. Each node of the network can have several sensing units, which are able to perform measurements of physical variables, such as temperature, luminosity, humidity, and vibration. According to E. Chang (2009) the nodes in a WSN have limited computing resources and are usually powered by batteries; thus energy saving is a key issue in these networks in order to prolong their operational lifetime. WSN nodes operate collaboratively, extracting environmental data, performing the same simple processing, and transmitting them to one or more exit points of the network (often called sink nodes), to be analysed and further processed.

According to M. Haenggi (2008) typically, WSNs are used in highly dynamic and sometimes remote and/or hostile environments and should operate without or with minimal human intervention. Therefore, such networks should have an autonomous behaviour and be able to tolerate several types of failures, such as faulty nodes or hardware physical malfunction (e.g., failures in the sensor units or battery) and lack of coverage and connectivity, among others. In other words, WSN should be able to self-manage those failures and to dynamically self-adapt to the environment.

One of the attack in WSN is the node replication attack and number of protocol proposed for tackling these type of attacks but no suitable mechanism is find out for MWSNs. However an appropriate mechanism is described by Deng, Xiong and Chen 2015 . They described the mobility property and propose two protocols for mobility assistance for the detection of node replication attacks in MWSNs. First protocol is the Unary

Time Location Storage and Exchange (UTLSE) that assigns each observer a task of tracking a particular set of other nodes. All the observers only store one time location entitlement for every tracked node and detect the replication when they come across each other. The second protocol is Multi Time Location Storage and Diffusion (MTLSD) that lets every observer stores multi time location claims for each tracked node. It also introduces more cooperation between the observers to improve the detection performance. Both protocols works as encounter-based because they only sent messages for detecting the replication when two nodes meet or come across each other and due to this way of working, the protocols do not have any need of routing signalling messages. Both protocols can also identify the replication with high detection accuracy as well as with very low communication, computation and storage overheads

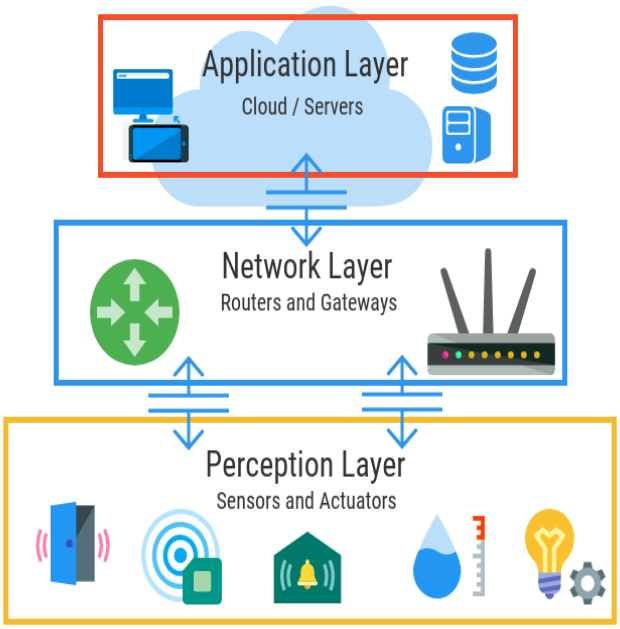
According to Pfleeger (2013) there are four different classes of security threads that are common in computational systems and also in sensor networks. These are Interruption, Interception, Modification and Fabrication. In Wireless sensor networks researcher identified several possible security attacks like passive information gathering, node subversion, false node, node malfunction, node outage, message corruption, traffic analysis, routing loops, selective forwarding, sinkhole, Sybil, wormholes, hello flood and DoS etc. These attacks also disturb WSN layers specifically application, transport, network, data link and physical layers. Different countermeasures and defence techniques are presented by researchers for layered security like malicious node detection and isolation, unique pair wise keys for application layer, limiting connections numbers, client puzzles for transport layer, Key management secure routing, Authentication, Encryption, Redundancy, Probing, monitoring, two way and three authentication and three way handshake for network layer, link layer encryption, rate limitations, error correcting code for data link layer and adaptive antennas, spread spectrum for physical layer. How ever we need to have a security framework in order to provide countermeasures against security attacks in WSN

3.IOT Architecture

The most basic architecture associated with the IOT is known as a "three-layered" architecture. Introduced in the early stages of research into this topic, it consists of the perception, network, and application layers.

- **The Perception Layer** – This perception layer is the IOT architecture's physical layer. In these sensors and embedded systems are used mainly. These collect large amounts of data based on the requirements. This also includes edge devices, sensors, and actuators that communicate with the surroundings. It detects certain spatial parameters or detects other intelligent things /objects in the surroundings.

- **The Network Layer** – The data obtained by these devices must be distributed and stored. This is the responsibility of the network layer. It binds these intelligent objects to other intelligent/ smart objects. It is also in charge of data transfer. The network layer is in-charge of linking smart objects, network devices, and servers. Its is also used to distribute and analyse sensor data.



IOT THREE LAYER ARCHITECTURE

- **The Application Layer** – The user communicates with this application layer. It is in-charge of providing the customer with software resources. Example: in smart home application, where users press a button in the app to switch on a coffee machine, for example. The application layer is in-charge of providing the customer with application-specific resources. It specifies different uses for the IOT, such as smart houses, smart cities, and smart health

4.Challenges and Security Issues

IOT will turn the entire planet into a smarter world. WSN and IOT devices are often installed in an unattended region where they cannot be physically monitored overnight in a day . Intruders could take advantage of the weaknesses of external surveillance and can receive information from the planting site rom certain IOT sensor nodes. By using data retrieved from the seized nodes, the opponent can assign nodes to adversaries and connect them to the existing infrastructure. These malicious nodes can then run a series of network attacks. These attempts can compromise network connectivity, quality and effectiveness. We may notice a decline in connection speeds, a rise in delay and also a decline in the packet forwarding ratio. Intrusion detection protocols are extremely important to avoid these kinds of activities. In this investigation, we have taken up a survey of existing network security protocols for both WSN and IOT applications.

4.1Challenges of WSN Integrated IOT

1. **Security:** Sensor nodes are critical part of WSNs for ensuring the data privacy, transparency, and authentication. By connecting WSNs to the internet, the proximity to the location requirement will not be needed anymore and attackers may threaten WSNs from any where.
2. **Data privacy:** Data protection is a serious concern. The information about a specific user has personal data along with data produced by the objects accompanying the person. It is necessary to decide and be aware of who regulates the relevant information. And how well the person can be self-assured about the data security that it cannot be used without authorization.
3. **IOT Components:** One more critical factor that needs to be considered is the safety of components by utilizing suitable measures for security protocols at the network level. Given that IOT is a global and highly integrated infrastructure, it is critical that a variety of different technologies, standards and authentication models are implemented in order to provide adequate assistance.
4. **Quality of Service:** Sensor nodes contribute to the quality of service operations by optimizing the productive use of the energy of all heterogeneous sensors that would be a part of the future IOT, via gateways operating as repeaters and protocol translators. A huge amount of capital cost, including security mechanisms is needed to improve QoS.
5. **Scalability:** As hundreds of nodes are distributed on the basis of an application and the developer should be aware of the risks associated with the possibilities of expanding the network and large population of sensors must be used to cover as much ground as possible.
6. **Energy Consumption:** Rechargeable batteries cannot be used in some applications. Therefore, the life of the battery greatly influences the life of the node and the functioning of the existing network

will be adversely affected resulting in compromise of the security of the entire network. Detection, encoding, sending and extracting are the key activities for which the sensors consume energy. In addition, noise can increase the power consumption due to retransmission.

7. **Timing of Data Delivery:** Delay in WSNs and IOT based systems depends on the delay in the delivery time of data. For example, if healthcare professionals do not receive alert messages, patient lives would be at risk. While designing protocols, the total disparity between both the transmitter and the receiver should also be analysed. It is necessary to consider the minimal permissible delay based on specific application demands
8. **Configuration:** Sensor nodes can help in controlling the WSN setup, such as addressing the administrator to verify networks adaptability and its ability to repair by finding and preventing node faults. However, on the World Wide Web, self-configurable nodes are not usually available. Instead, the user should install applications and the machine should recover from the crashes. Conversely, the unattended autonomous sensor nodes need new activity configuration for management of the network.
9. **Gathering Data:** Depending on information analysis, WSN applications can be either Event Detection (ED) or Spatial Process Estimation (SPE). ED is used to predict a particular incident by the use of sensors and SPE estimates physical conditions. Both have different applications

4.2 Security Attacks WSN Integrated IOT

Security threats associated with the perception layer

- **Eavesdropping** – This is an unauthorized attack that takes place in real-time. During this attack, private communications such as phone calls, text messages, video conferences, and faxes are seized by the attacker. This data is ultimately intercepted over a network, which may or may not is secured.

- **Node Capture** – This is one of many harmful attacks that can affect the perception layer of IOT devices. Through node capture, an attacker can gain full control over a key node, such as a gateway node. This allows the attacker to leak a variety of communications between the sender and receiver while gaining access to information stored in the device's memory.

- **Fake Node and Malicious** – This is when an attacker adds a node to a system that is designed to input fake data. This attack aims to stop the node from transmitting real information, consuming energy from authentic nodes, and potentially destroying the network.

- **Replay Attack** – Also referred to as a "playback attack," this is where an attacker eavesdrops on a conversation between a sender and receiver and steals information from the sender. They then send

this information to the victim in an attempt to prove their authenticity or as "proof" of their identity. Once they've assumed the real sender's identity, they can then entice the recipient to perform any number of actions.

- **Timing Attack** – This is particularly effective against devices that have weak computing capabilities. It allows an attacker to identify vulnerabilities in the system, bypassing it in order to steal information. To do so, they observe how long it takes the system to respond to a specific input, queries, or algorithms.

Security threats associated with the network layer

- **Denial of Service (DOS) Attack** – DOS attacks attempt to prevent users from accessing their devices or other network resources. It is most often accomplished by flooding targeted devices with so many requests that it becomes impossible for users to actually filter them.

- **Main-in-The-Middle (MITM) Attack** – MITM attacks take place when a third party intercepts and then alters communications between a receiver and a sender, changing the messages to suit their own needs. This signifies a major security breach, as it allows the attacker to manipulate information in real-time.

- **Storage Attack** – A user's information is usually only stored in the cloud or in various storage devices. Both of these can be attacked by outsiders, with users changing information at will. Data can also be replicated in order to facilitate any number of other attacks.

- **Exploit Attack** – This is where an attacker takes advantage of security weaknesses in a system, application, or hardware. The goal is most often to steal information stored on a specific network.

Security threats associated with the application layer

- **Cross-Site Scripting** – This is an injection attack that enables a third party to insert a client-side script in a trusted site. This eventually allows the attacker to change the application's contents according to their needs or to use the original data illegally.

- **Malicious Code Attack** – This is code embedded in software designed to cause damage to the system. It is extremely common and can often be blocked by antivirus or anti-malware programs.

5.Advantages and Disadvantages

Advantages of WSN

- It is scalable and hence can accommodate any new nodes or devices at any time.
- It is flexible and hence open to physical partitions.
- All the WSN nodes can be accessed through centralized monitoring system.
- As it is wireless in nature, it does not require wires or cables.
- WSNs can be applied on large scale and in various domains such as mines, healthcare, surveillance, agriculture etc.
- Enable Long-distance Data Collection and Transmission
- Anticipate Natural Disasters

Disadvantages of WSN

- As it is wireless in nature, it is prone to hacking by hackers.
- It cannot be used for high speed communication as it is designed for low speed applications.
- There are various challenges to be considered in WSN such as energy efficiency, limited bandwidth, node costs, deployment model, Software/hardware design constraints and so on.
- In star topology based WSN, failure of central node leads to whole network shutdown.
- Sensor nodes that are inexpensive to purchase and operate.
- High chances of the entire system getting corrupted

6.IOT Application

1. Smart Homes: One of the best and the most practical applications of IOT, smart homes really take both, convenience and home security, to the next level. Though there are different levels at which IOT is applied for smart homes, the best is the one that blends intelligent utility systems and entertainment together. As IOT evolves, we can be sure that most of the devices will become smarter, enabling enhanced home security.

2. Smart City: Not just internet access to people in a city but to the devices in it as well – that's what smart cities are supposed to be made of. Efforts are being made to incorporate connected technology into infrastructural requirements and some vital concerns like Traffic Management, Waste Management, Water Distribution, Electricity Management, and more.

3. Self-driven Cars: We've seen a lot about self-driven cars. Google tried it out, Tesla tested it, and even Uber came up with a version of self-driven cars that it later shelved. Since it's human lives on the roads that we're dealing with, we need to ensure the technology has all that it takes to ensure better safety for the passenger and those on the roads.

4. IOT Retail Shop: If you haven't already seen the video of Amazon Go – the concept store from the e-commerce giant, you should check it out right away. Perhaps this is the best use of the technology in bridging the gap between an online store and a retail store. The retail store allows you to go cashless by deducting money from your Amazon wallet. It also adds items to your cart in real-time when you pick products from the shelves.

5. Farming: Farming is one sector that will benefit the most from the Internet of Things. With so many developments happening on tools farmers can use for agriculture, the future is sure promising. Tools are being developed for Drip Irrigation, understanding crop patterns, Water Distribution, drones for Farm Surveillance, and more. These will allow farmers to come up with a more productive yield and take care of the concerns better.

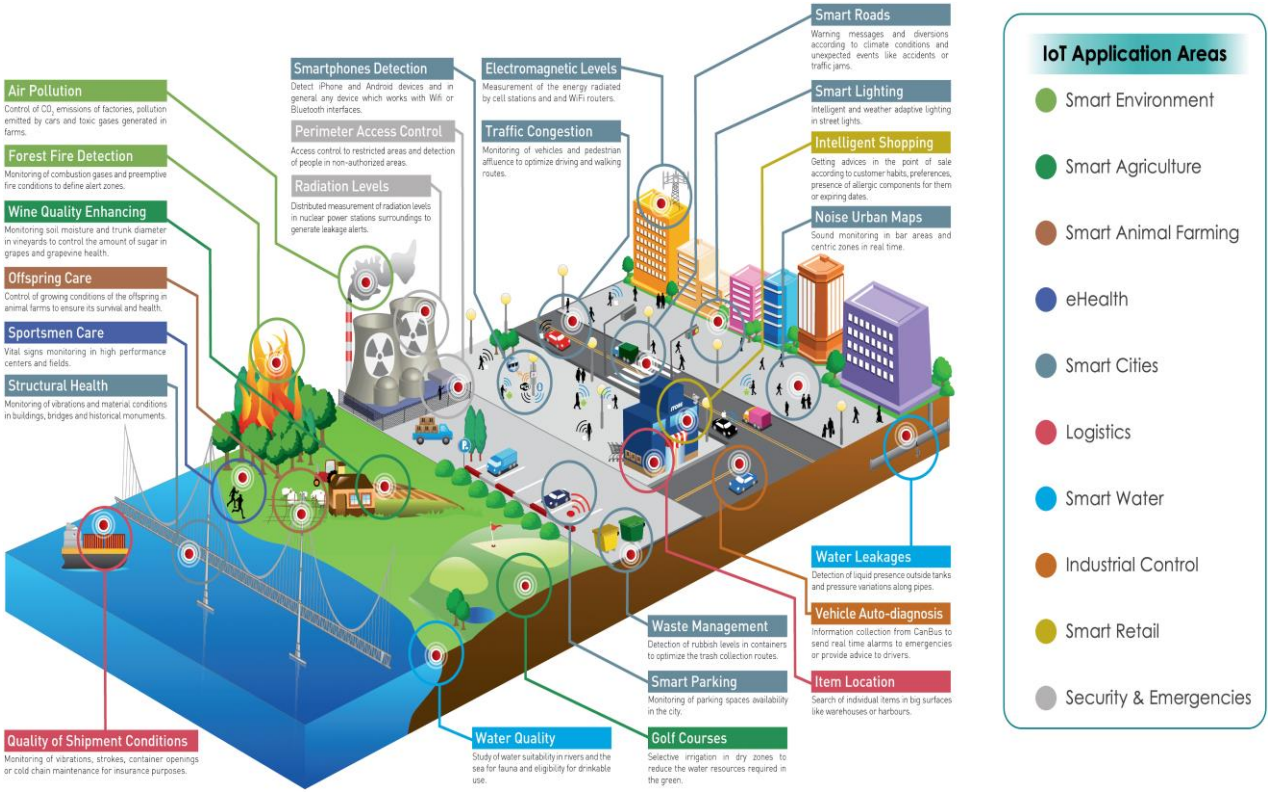
6. Wearables: Wearables remain a hot topic in the market, even today. These devices serve a wide range of purposes ranging from medical, wellness to fitness. Of all the IOT start-ups, Jawbone, a wearables maker, is second to none in terms of funding.

7. Smart Grids: One of the many useful IOT examples, a smart grid, is a holistic solution that applies an extensive range of Information Technology resources that enable existing and new gridlines to reduce electricity waste and cost. A future smart grid improves the efficiency, reliability, and economics of electricity.

8. Industrial Internet: The Industrial Internet of Things consists of interconnected sensors, instruments, and other devices connected with computers' industrial applications like manufacturing, energy management, etc. While still being unpopular in comparison to IOT wearables and other uses, market researches like Gartner, Cisco, etc., believe the industrial internet to have the highest overall potential.

9. Traffic Management: Car traffic management in large cities can be greatly improved with the help of the Internet of Things (IOT). The Internet of Things helps us stay informed and improves traffic monitoring by allowing us to use our mobile phones as sensors to collect and share data from our vehicles through apps like Waze or Google Maps.

10. Water/ Waste Management: Many cities are adopting water recycling using water treatment units. Using an IOT application, you can see how much wastewater is being produced, how much is being consumed in a specific area, and how waste production is changing over time.



7.Conclusion

- Integration of IOT and WSNs enables the broad opportunity in almost every aspect of the life. The integration seems fascination at first look but it comes with unseen challenges. In WSNs, sensor node is equipped with very low resources in terms of hardware as well as software.
- On the other hand IOT has no limitation either in processing capability or hardware compatibility. In the integration, the layered function of WSNs and IOT has to be tailored for the interoperability.
- The Internet of Things (IOT) is quickly weaving itself into modern life all around the world. By connecting smart devices, applications, and other technology, it has the power to enhance quality of life and automate a near-infinite number of interactions.
- Still, we hope this brief overview has properly outlined how layered architectures of IOT can be subject to specific, malicious attacks by third parties.
- the possibilities of the IOT are indeed exciting, proper precautions and security measures must be taken at all times.
- Moreover, it is important to consider new multi-layered architectures in order to design a more secure infrastructure for the IOT.

8.References

1] N. Salman, I. Rasool and A. H. Kemp, "Overview of the IEEE 802.15.4 standards family for Low Rate Wireless Personal Area Networks," 2010 7th International Symposium on Wireless Communication Systems, 2010, pp. 701-705, doi: 10.1109/ISWCS.2010.5624516.

2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

3] S. Fang, L. Da Xu, Y. Zhu, J. Ahati, H. Pei, J. Yan, Z. Liu et al., "An integrated system for regional environmental monitoring and management based on internet of things." IEEE Trans. Industrial Informatics, vol. 10, no. 2, pp. 1596–1605, 2014.

4] P. Gope and T. Hwang, "Bsn-care: A secure IOT-based modern health care system using body sensor network," IEEE Sensors Journal, vol. 16, no. 5, pp. 1368–1376, 2016.

5] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Information Systems Frontiers, vol. 17, no. 2, pp. 243–259, 2015.

6] Ghosal A., Halder S. (2013) Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches. In: Khan S., Khan Pathan AS. (eds) Wireless Networks and Security. Signals and Communication Technology. Springer, Berlin, Heidelberg.

7] A. G. Finogeev and A. A. Finogeev, "Information attacks and security in wireless sensor networks of industrial scada systems," Journal of Industrial Information Integration, vol. 5, pp. 6–16, 2017.