# TERM PAPER

VIKRAMADITYA REDDY VARKALA
Z1973679

# INTERNET OF  THINGS (IoT) SECURITY

## Abstract:

The paper presents introduction and analysis on the topic of Internet of things (IoT). IoT typically has a three layers architecture consisting of Perception, Network, and Application layers.A number of security principles should be enforced at each layer to make this framework secure.This paper aims to provide an overview of IoT, the key security challenges and solutions related to IoT  and Emerging trends in IoT.The paper will discuss the importance of IoT security and highlight the various practices  that can be used to secure IoT devices and systems.

## Introduction:

The Internet of things (IoT) describes physical objects (or groups of such objects) with  sensors, processing ability, software  and other technologies that connect and exchange data with other devices and systems over the internet or other communications networks. IoT Security is the act of securing Internet devices and the networks they're connected to from threats and breaches by protecting, identifying, and monitoring risks all while helping fix vulnerabilities from a range of devices that can pose security risks to your business.

## IoT Architecture:

The IoT architecture can be divided into three main layers: the perception layer, the network layer, and the application layer.

- **Perception Layer:** The perception layer is the bottom layer of the IoT architecture and is responsible for collecting data from various sensors and devices. This layer includes sensors, actuators, gateways, and other devices that collect data from the physical world. The data collected by these devices is then sent to the network layer for processing.The physical equipment like RFID reader, GPS, all kinds of sensors, and other equipment comes under this layer
- **Network Layer:** The network layer is responsible for transmitting and processing data collected from the perception layer. This layer includes network gateways, routers, switches,

and other devices that transmit data between devices and the cloud. The network layer is responsible for ensuring that data is transmitted securely and efficiently.\

- **Application Layer:** The application layer is the top layer of the IoT architecture and is responsible for providing various services to users. This layer includes cloud platforms, web services, and other applications that analyze and process the data collected by the perception layer. The application layer is responsible for providing insights, recommendations, and other value-added services to users.

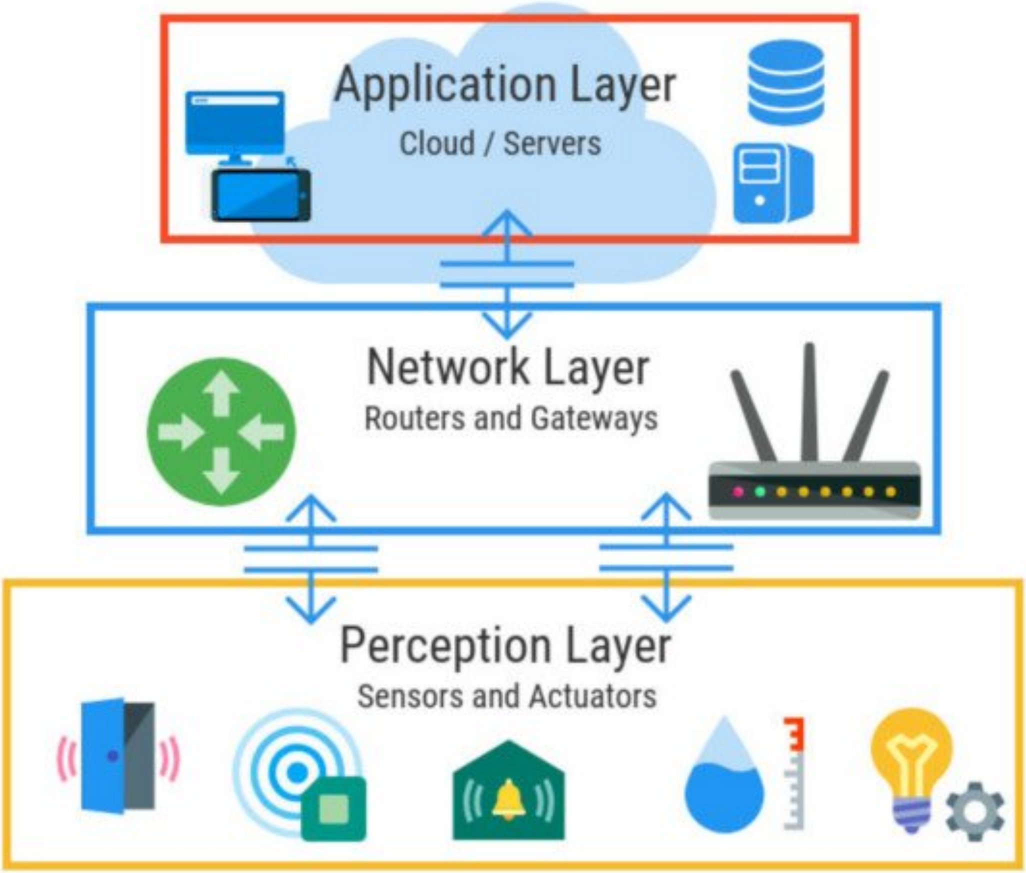


*Figure: IoT architecture*

## IoT Security Threats:

IoT security threats are security risks that can affect Internet of Things (IoT) devices and systems. Here are some common types of IoT security threats:

**Perception Layer Threats:**

The perception layer is also the most vulnerable to security threats. Here are some common security threats in the perception layer of IoT:

- **Data Spoofing:** Data spoofing occurs when attackers manipulate the data collected by sensors, leading to inaccurate or misleading information. This can be used to trigger false alarms or to cause disruptions in the system.
- **Radio Jamming:** Radio jamming is a type of attack in which an attacker floods the communication channel with interference signals, disrupting the communication between nodes
- **Node Capturing:** Node capturing is a type of attack in which an attacker gains unauthorized access to a node in the communication layer.
- **Node Outage:** A node outage occurs when a node in the communication layer fails to operate correctly. This can be due to hardware or software malfunctions, power outages, or other technical issues.

**Network Layer Threats:**

This layer is often vulnerable to several security threats which includes:

- **Selective Forwarding:** This attack involves an attacker selectively dropping or forwarding packets on the network. This can cause disruption in communication between devices and can even lead to the entire network being compromised.
- **Sybil Attack:** In a Sybil attack, an attacker creates multiple fake identities or nodes in the network to gain control or disrupt the communication. This can cause network congestion and affect the reliability of the network.
- **Sinkhole Attack:** A sinkhole attack involves an attacker intercepting and redirecting the network traffic towards a specific node or sinkhole. This can lead to unauthorized access and data leakage.
- **Hello Flood Attack:** A Hello flood attack involves an attacker flooding the network with a large number of hello messages. This can cause congestion and denial of service (DoS) on the network, disrupting communication and causing downtime.

**Application Layer Threats:**

The application layer of IoT (Internet of Things) architecture is ofter can be vulnerable to several security threats, including:

- **Logger Attack:** a logger attack involves the exploitation of software programs used to track and record user activity and system events. Attackers can gain access to loggers and collect sensitive data such as login credentials, personal information, and other confidential data.

- **Injection Attack:** An injection attack involves an attacker injecting malicious code or data into an application or database. This can cause the application to execute unauthorized actions, leading to data loss or unauthorized access to sensitive information.
- **Session Hijacking:** Session hijacking involves an attacker taking control of a user's session or connection to a system or application. This can allow the attacker to access sensitive data or execute unauthorized actions using the user's credentials.

**Support Layer Threats:**

- **Data Tampering:** Data tampering involves the unauthorized modification of data stored in databases or transmitted between devices. This can lead to inaccurate analysis and decision-making, and can compromise the integrity of the entire IoT system.
- **Unauthorized access:**This refers to an attacker gaining access to the IoT network or to sensitive data stored in the network without permission.

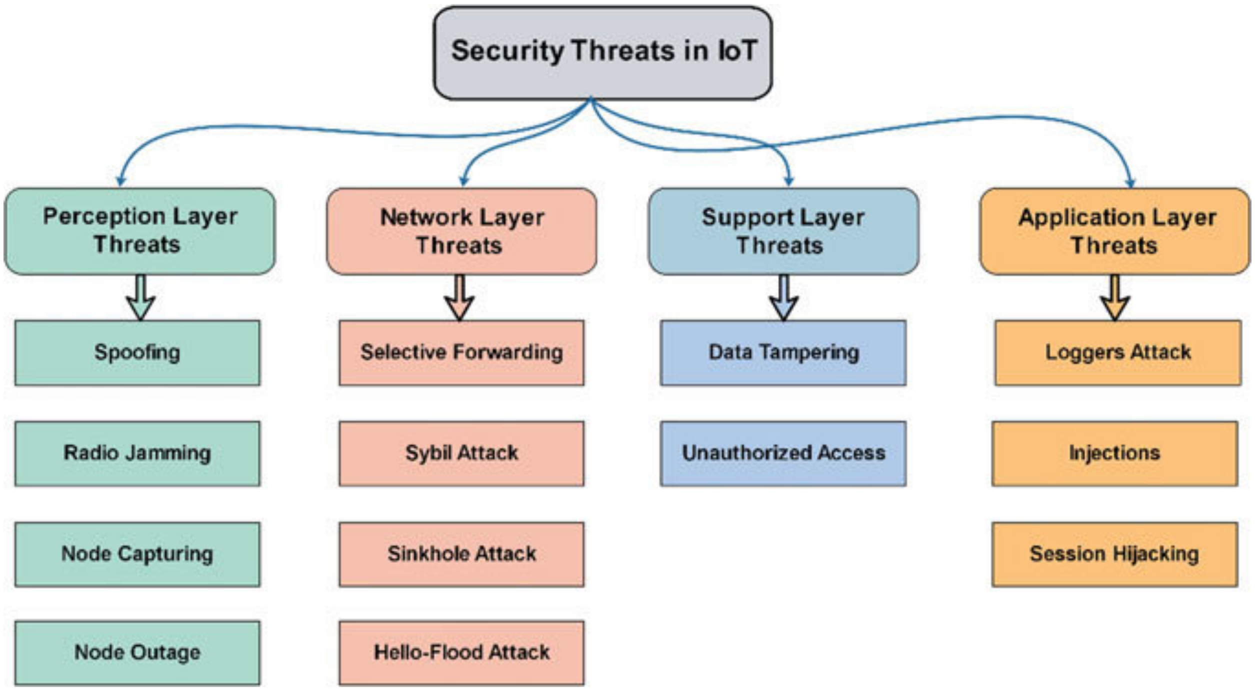


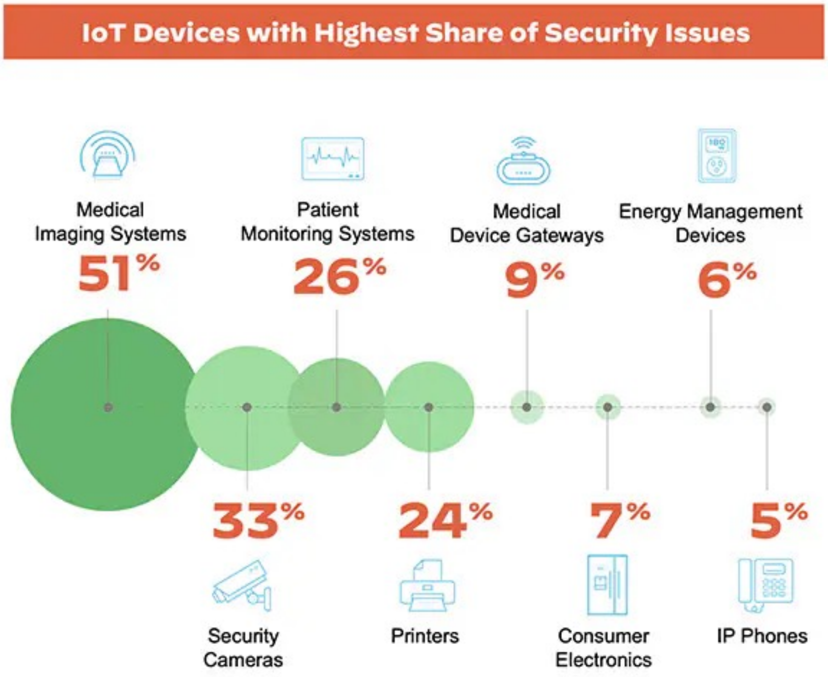
*Figure: Security Threats*

## Challenges to IoT Security:

The overarching challenge for security in IoT is that as large volumes of diverse IoT devices continue to connect to the network, a dramatic expansion of the attack surface is happening in parallel. Ultimately the entire network security posture is diminished to the level of integrity and protection offered to the least secure device.

- **Inventory** :Not having clear visibility and context for what IoT devices are in the network and how to securely manage new devices.
- **Threats** :Lack of well-embedded security into IoT device operating systems that are hard or impossible to patch.
- **Data volume :** Overseeing vast amounts of data generated from both managed and unmanaged IoT devices.
- **Ownership :** New risks associated with the management of IoT devices by disparate teams within the organization.
- **Diversity :**The sheer diversity of IoT devices in terms of their limitless forms and functions.
- **Operations :**The unification crisis wherein IoT devices are critical to core operations yet difficult for IT to integrate into the core security posture.

The figure below shows the IoT devices that have the highest share of security Issues



## Best practices for IoT Security :

Network security and operations teams should be incorporating IoT security into standard practice, process and procedure to ensure both managed and unmanaged devices fall within the same level of visibility and control across the IoT security lifecycle.The IoT (Internet of Things) security lifecycle approach encompasses five critical stages of IoT security :

- **Understand IoT Assets:**Identify all managed and unmanaged devices with context.
- **Assess IoT Risks:**Accurately assess and identify vulnerabilities and risks associated with all devices.
- **Apply Risk Reduction Policies:**Automate Zero Trust policies and enforcement of those policies.
- **Prevent Known Threats:**Take swift action on preventing known threats.
- Rapidly detect and respond to unknown threats.

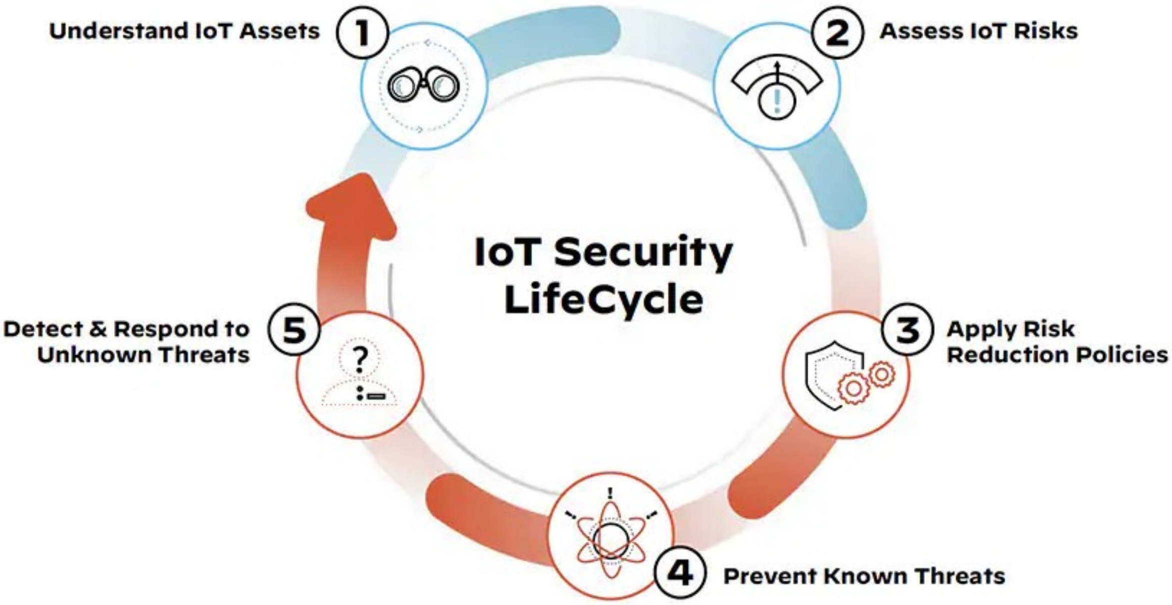


*Figure: IoT Security Lifecycle*

## Regulations and Compliance:

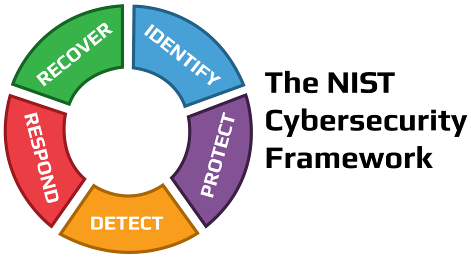
Compliance is a recurring challenge for organizations using IoT solutions.Compliance in IoT comprises both cyber security and operational challenges. IoT teams need to know whether their devices are secure and working properly at all times. Here are some key regulations and compliance frameworks related to IoT security:

**GDPR (General Data Protection Regulation):** The GDPR is a regulation in the European Union that focuses on data protection and privacy. It applies to any organization that processes the personal data of EU citizens, regardless of where the organization is located. IoT devices that collect personal data are subject to GDPR regulations.

**NIST (National Institute of Standards and Technology) Cybersecurity Framework:** The NIST Cybersecurity Framework is a voluntary set of guidelines for organizations to manage and reduce cybersecurity risk. IoT device manufacturers can use the framework to develop secure devices.

**ISO/IEC 27001:** This is an international standard for information security management. IoT device manufacturers can use this standard to ensure their devices are secure and comply with industry best practices.

**ISA/IEC 62443:** This is a series of international standards for industrial control systems cybersecurity. The standards cover a range of topics, including risk assessment, secure development, and network security.



## Security Measures for IoT Security:

- **Change Default Passwords:** Many IoT devices come with default usernames and passwords that are easily guessed by attackers. Change these default login credentials to something more secure immediately after purchasing the device.
- **Update Software Regularly:** Manufacturers may release security updates to fix vulnerabilities in their devices. Always update the firmware of your IoT devices to the latest version available.
- **Incorporate Vulnerability Scanner:** The use of vulnerability scanners is an effective method in detecting the different types of devices linked to a network.Vulnerability scanner in collaboration with a regular scanning schedule is capable of spotting known vulnerabilities related to connected devices.
- **Encryption:** Ensure that all data transmitted between IoT devices and servers is encrypted using the latest cryptographic standards.
- **Network Access Control (NAC):**An organization can successfully improve IoT security by implementing a NAC solution consisting of a proper switch and wireless assimilations. This setup can help detect most devices and recognize problematic connections within the network.
- **Network Segmentation:** Isolate your IoT devices onto a separate network segment from your main network to minimize the risk of attackers gaining access to your entire network.\

## Emerging Trends in IoT:

Emerging trends refer to new and innovative ideas, technologies, or practices that have the potential to have a significant impact on various aspects of our lives. In today's rapidly evolving world, emerging trends are constantly shaping the way we live, work, and interact with technology.Below are emerging trends in IoT (Internet of Things) devices:

- **Edge Computing:** With the increasing number of IoT devices and the massive amount of data generated by them, edge computing is becoming more important. Edge computing involves processing data at the edge of the network, closer to where it is generated, instead of sending it all to the cloud for processing. This helps reduce latency, bandwidth usage, and the cost of cloud services.
- **AI and Machine Learning:** IoT devices generate vast amounts of data, which can be analyzed using AI and machine learning  for IoT can be used to project future trends, detect anomalies, optimize performance, improve and augment intelligence by ingesting image, video and audio
- **5G Connectivity:** 5G networks provide faster and more reliable connectivity, which is essential for IoT devices that require low latency and high bandwidth. This will enable new use cases for IoT, such as remote surgeries and autonomous vehicles.
- **Blockchain:** The distributed and secure nature of blockchain technology can be useful for IoT applications. It can help secure and manage data generated by IoT devices, facilitate device-to-device communication, and enable new business models.

- **Smart Cities:** IoT is being used to create smart cities by integrating various devices and sensors to monitor and control urban infrastructure such as traffic, lighting, and waste management. This can help reduce costs, improve safety, and enhance the quality of life in cities.
- **Health and Fitness:** IoT devices such as wearables and sensors are being used to monitor health and fitness data, allowing for personalized health monitoring and preventative care.
- A**griculture:** IoT devices are being used in agriculture to monitor soil conditions, track crop growth, and manage irrigation systems, leading to more efficient and sustainable farming practices.

IoT Analytics projected that 2023 will see a growth of IoT devices by 18% to 14.4 billion, and by 2025, this could increase to 27 billion connected IoT devices. This will particularly increase connectivity in urban communities, but many rural areas will still depend on lower-performing networks.

## Conclusion:

The security of Internet of Things (IoT) devices and networks is a complex and ongoing challenge that requires a holistic approach. The integration of IoT devices into critical systems and infrastructures has increased the risk of cyber attacks and data breaches, leading to potential harm to individuals, organizations, and society as a whole.

To ensure the security of IoT, it is important to implement strong security measures such as using secure communication protocols, encryption, access control, firewalls, and intrusion detection systems. Regularly updating software and firmware, conducting security audits, and testing for vulnerabilities are also crucial steps to take to mitigate security risks. Education and training for users and stakeholders on IoT security best practices can also help prevent social engineering attacks and other forms of human error.

As the IoT continues to evolve, it is crucial that security remains a top priority for all manufacturers, service providers and users.By implementing strong security measures and staying vigilant, we can help ensure that the benefits of IoT are realized while mitigating the potential security risks.

## References and Images:

- https://en.wikipedia.org/wiki/Internet_of_things
- https://encyclopedia.pub/entry/24469
- https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security
- https://www.researchgate.net/figure/Security-threats-at-different-layers-of-the-IoT-architecture_fig2_337259162
- https://unit42.paloaltonetworks.com/iot-threat-report-2020/
- https://dzone.com/articles/top-7-security-measures-for-iot-systems
- https://www.antino.com/blog/top-9-iot-trends/