SEMINAR REPORT
ON
Securing the Unseen: Real-Time IoT Device Security Monitoring

A Report Submitted in Partial Fulfilment of the Requirements for the Degree of

Bachelor of Technology

In

ELECTRICAL AND COMPUTER ENGINEERING

By

Raman Kumar

Regd. No:2301326327

Under the Guidance of

Prof. Himanshu Shekhar Maharana

Department of Electrical & Computer Engineering
GANDHI INSTITUTE FOR EDUCATION & TECHNOLOGY

SESSION-2025-26

CERTIFICATE

This is to certify that the seminar entitled ***"Securing the Unseen: Real-Time IoT Device Security Monitoring"*** submitted by ***Student Name Raman Kumar*** having Registration Number 2301326327 to the Biju Pattnaik University of Technology, Odisha for partial fulfilment of the award for **Bachelor of Technology** in **Electrical & Computer Engineering**, is a bonafide seminar work carried out by him under my supervision. The results presented in this seminar have not been submitted elsewhere for the award of any other degree.

In my opinion, this work has reached the standard fulfilling the requirements for the award of the degree of B.Tech in accordance with the regulations of the University.

Signature of Guide

Department of Electrical & Computer Engineering
GIET,Baniatangi

Signature of HoD

Department of Electrical & Computer Engineering
GIET,Baniatangi

DECLARATION

I hereby declare that the seminar report entitled **“Securing the Unseen: Real-Time IoT Device Security Monitoring”** submitted to **Gandhi Institute for Education and Technology, Bhubaneswar, Odisha** is a bonafide record of the work carried out by me under the guidance of **Prof. Himanshu Shekhar Maharana**, in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Electrical and Computer Engineering**.

I further declare that this seminar report has not been submitted previously, either in part or in full, to any other University or Institution for the award of any degree or diploma.

Name Raman Kumar
Regd. No: 2301326327
Date:

ACKNOWLEDGEMENT

I am very grateful, thankful and wish to record our indebtedness to **Prof. Sasank Sekhar Dalei**, **H.O.D**. of **Electrical & Computer Engineering**, Gandhi Institute for Education and Technology, Baniatangi, for his active guidance and interest in this seminar work.

I would also like to thank my guide **Prof. Himanshu Shekhar Maharana** of **Electrical & Computer Engineering** Department for his continued drive for better quality in everything that allowed me to carry out my seminar work.

Lastly, word run to express my gratitude to my parents and all the Professors, Lecturers, Technical and official staffs and friends for their co-operation, constructive criticism and valuable suggestions during the preparation of seminar report**.**

Name: Raman Kumar
Regd. no: 2301326327
Program: B. Tech
Branch: EACE

Topic Name

"Securing the Unseen: Real-Time IoT Device Security Monitoring"

ABSTRACT

This project introduces a Real-Time IoT Device Security Monitoring system that continuously observes device behavior, analyzes network traffic patterns, and detects anomalies using lightweight detection techniques. The system integrates vulnerability assessment modules, suspicious activity scoring, and automated alerts to ensure timely responses against emerging threats. A centralized dashboard provides comprehensive visualization of device status, communication behavior, risk levels, and historical threat logs, enabling security administrators to make informed decisions efficiently. A central dashboard visualizes device health, traffic patterns, and detected threats, enabling security administrators to take informed decisions quickly. By integrating lightweight monitoring modules, the solution ensures minimal resource consumption on IoT devices. Experimental evaluation demonstrates improved detection rates and rapid threat response compared to conventional monitoring approaches. This research contributes to enhancing IoT ecosystem security and provides a scalable, proactive defense against emerging cyber threats.

Guided By
Prof. Himanshu Shekhar Maharana
Dept of. EACE

Submitted By:
Name: Raman Kumar
Regd. No.: 2301326327
Branch : - EACE (5th sem)

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The Internet of Things (IoT) refers to a network of physical objects—such as sensors, smart devices, vehicles, home appliances, and industrial machines—that are embedded with software, sensors, and connectivity to collect and exchange data over the internet.

1.1 Overview of IoT (Internet of Things)

These connected devices can monitor conditions, automate actions, and share insights without human intervention.

IoT plays a key role in sectors like smart homes, healthcare, agriculture, transportation, and industrial automation. The data gathered from IoT systems enables intelligent decision-making, improved efficiency, and enhanced user experience.

1.2 Importance of IoT Security

As IoT devices become more widespread, security has become a major concern.
Each connected device can act as a potential entry point for cyberattacks if not properly secured.
IoT security ensures that devices, data, and communications remain protected from unauthorized access, manipulation, and misuse.
Weak passwords, unpatched software, and insecure networks often make IoT systems vulnerable.
Strong IoT security safeguards sensitive information, maintains system integrity, and prevents large-scale cyberattacks such as botnets and data breaches—making it essential for both personal safety and organizational reliability.

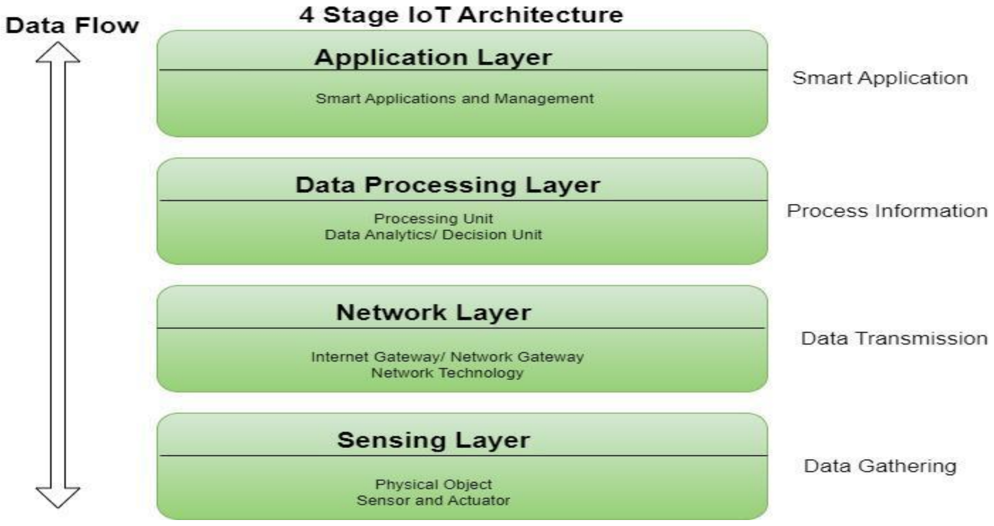

Figure 1.1 :Basic IoT System Architecture

1.3 Objectives of Real-Time Security Monitoring

The main objective of real-time IoT device security monitoring is to detect, analyze, and respond instantly to any suspicious or malicious activity within an IoT environment. Key goals include:

- Continuous tracking of device activity and network traffic.
- Detecting abnormal behavior that indicates possible threats.
- Preventing unauthorized access and data theft.
- Generating alerts and automated responses to security incidents.
- Ensuring consistent device performance and reliability.
  Real-time monitoring minimizes downtime, reduces risk, and supports proactive defence rather than reactive damage control.

1.4 Scope of the Study

This study focuses on developing and understanding a framework for real-time IoT device security monitoring.

It covers:

- Identification of common vulnerabilities in IoT systems.
- Analysis of existing security mechanisms and their limitations.
- Design and implementation of a real-time monitoring model.
- Evaluation of performance using different tools and techniques.
  The scope also extends to exploring how artificial intelligence (AI) and machine learning (ML) can enhance detection accuracy and automate threat responses in future IoT environments.

CHAPTER 2

IoT Security Architecture

IoT Security Architecture defines the overall structure and set of security measures applied across all layers of an IoT ecosystem to ensure safe data collection, transmission, and processing

2.1 IoT Security Architecture

It consists of multiple interconnected components, including devices, gateways, networks, cloud services, and user interfaces.

A strong IoT security architecture ensures that every layer — from the physical device to the cloud — has protection against unauthorized access, malware, data breaches, and manipulation.

This architecture follows a layered defense approach, incorporating authentication, encryption, access control, and continuous monitoring to maintain the integrity and confidentiality of the system

2.2 IoT System Layers

An IoT system typically operates through three primary layers, each responsible for different functions and security requirements:

1. Perception Layer (Device Layer)
   - This is the lowest layer, consisting of sensors, actuators, and edge devices that collect and transmit data from the physical environment.
   - Security threats: device tampering, fake data injection, hardware manipulation.
   - Security measures: device authentication, data encryption at source, secure boot

Network Layer

- This layer transfers data from devices to cloud servers or other devices through communication protocols like Wi-Fi, Zigbee, Bluetooth, or cellular networks.
- Security threats: man-in-the-middle attacks, data interception, DDoS.

2. Application Layer
    - This layer provides services and user interfaces for analyzing and displaying IoT data.
    - Security threats: unauthorized access, API vulnerabilities, data leaks.
    - Security measures: role-based access control (RBAC), secure APIs, regular patching.

2.3 Communication and Data Flow in IoT

Communication in IoT systems occurs through a combination of machine-to-machine (M2M), device-to-cloud, and device-to-gateway interactions.

Data collected by sensors is transmitted through networks to cloud platforms, where it is processed, analyzed, and visualized.

The data flow generally follows these stages:

1. Data Generation – Sensors and devices collect data.
2. Data Transmission – The information is securely sent using protocols like MQTT, CoAP, or HTTP.
3. Data Processing – The data is filtered and analyzed in edge or cloud environments.
4. Data Storage – Useful information is stored in databases for monitoring and decision-making.
5. Data Utilization – Results are used to trigger actions, generate reports, or send alerts.

2.4 IoT Security Model (Device, Network, Cloud)

IoT Security can be divided into three main levels:

1. Device-Level Security
   - Focuses on securing sensors, actuators, and embedded systems.
   - Methods: Secure firmware updates, strong passwords, access control, and tamper detection.
2. Network-Level Security
   - Protects communication channels between devices and gateways.
   - Methods: Network encryption, firewalls, intrusion detection/prevention systems (IDS/IPS), and secure protocols (TLS, SSL).
3. Cloud-Level Security
   - Secures data storage, analytics, and applications hosted in the cloud.
   - Methods: Multi-factor authentication (MFA), data encryption at rest and in transit, identity management, and monitoring

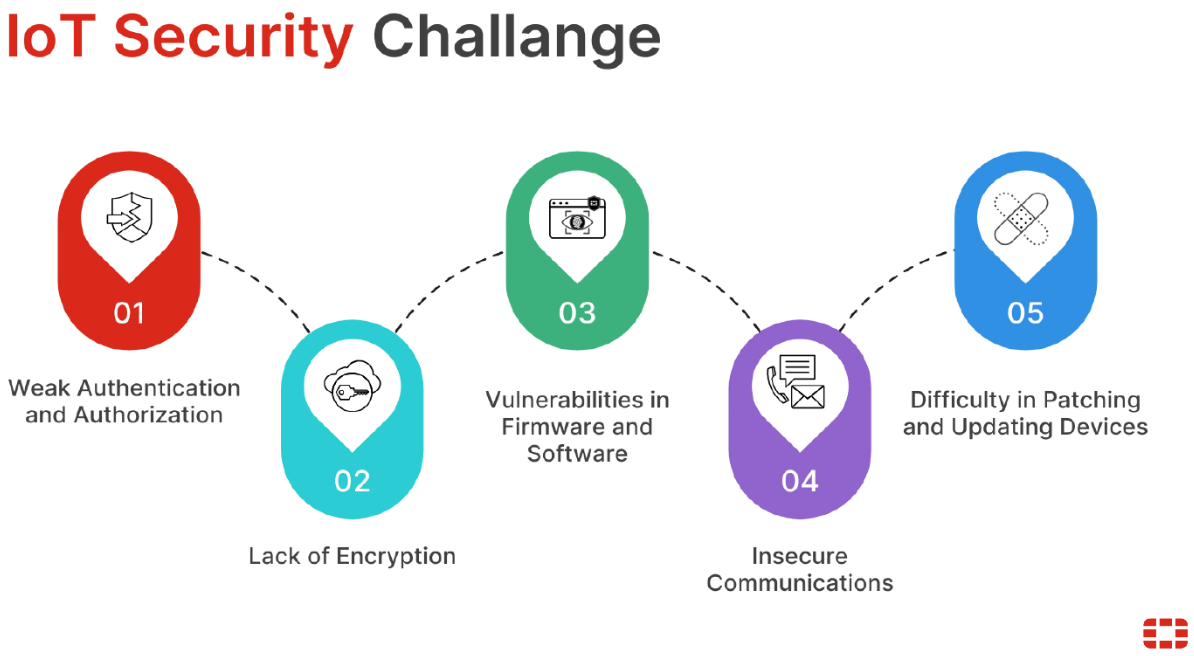
IoT Security Challange
01
Weak Authentication and Authorization
02
Lack of Encryption
03
Vulnerabilities in Firmware and Software
04
Insecure Communications
05
Difficulty in Patching and Updating Devices

Figure 2.1: Classification of IoT Security Threats

CHAPTER 3

Common IoT Vulnerabilities & Threats

IoT systems, while highly beneficial, are also prone to various security weaknesses due to the large number of interconnected devices, limited device resources, and inconsistent security standards.

Hackers exploit these vulnerabilities to gain unauthorized access, manipulate data, or disrupt services.
Common IoT threats include malware attacks, data breaches, denial-of-service (DoS) attacks, and unauthorized device control.

Understanding these vulnerabilities is crucial for designing effective protection and real-time monitoring mechanisms.

3.1 Device-Level Vulnerabilities

- **Weak passwords & authentication** make devices easy targets.
- **Unpatched firmware** allows exploitation of known bugs.
- **Physical access** can lead to tampering or data theft.
- **Limited security features** due to low device power.

Example:
The Mirai botnet (2016) hijacked IoT cameras and routers using default passwords.

3.2 Network-Level Threats

- **Man-in-the-Middle (MitM)** – Attackers intercept data between devices.
- **DDoS attacks** – Overloading networks with fake traffic.
- **Eavesdropping** – Capturing unencrypted data.
- **Spoofing** – Fake devices posing as real ones.

Prevention:
Use encryption, VPNs, and secure protocols (TLS/SSL).

3.3 Cloud and Data Security Risks

- **Data breaches** from insecure storage.
- **Weak APIs** expose data.
- **Poor access control** allows unauthorized changes.
- **Privacy leaks** due to unencrypted communication.

Mitigation:

Encrypt data, use strong authentication, and audit cloud access.

3.4 Real-World Incidents

- **Mirai Attack (2016):** Massive DDoS using IoT devices.
- **Jeep Hack (2015):** Remote vehicle control via IoT**.**
- **Ring Camera Breach (2019):** Unauthorized access to home cameras.

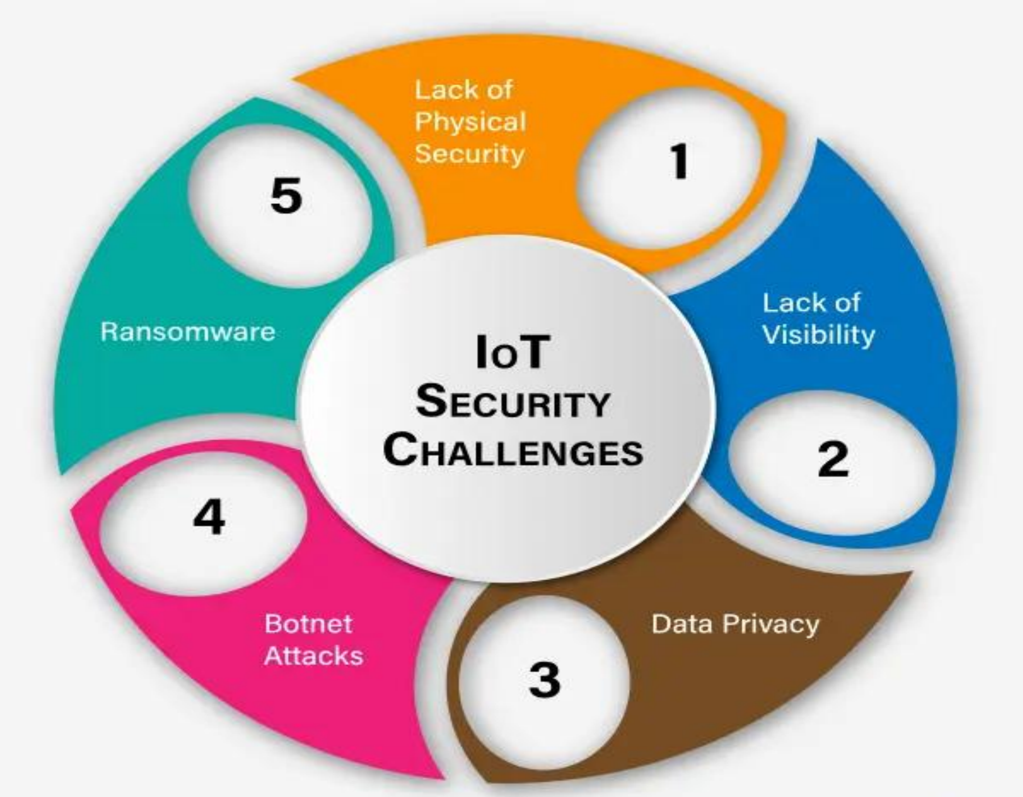

Figure 3.1 – Classification of IoT Security Threats

CHAPTER 4

System Design and Architecture

The process of planning and structuring a system — showing how all its parts (hardware, software, and data) work together to perform a specific task.The proposed system is designed to monitor IoT devices in real-time for detecting unusual activities or security breaches.

It includes four main layers:

1. **Device Layer –** Sensors and IoT devices generate data.

2. **Network Layer –** Transmits data securely to servers or cloud.

3. **Monitoring Layer –** Analyzes data using AI-based algorithms.

4. **User Interface Layer –** Displays alerts, reports, and device status

4.2 Working Principle

The system continuously collects and analyzes data from connected IoT devices. If abnormal patterns are detected—like unusual traffic or unauthorized access—it triggers an alert and logs the event.

AI algorithms help identify threats automatically and reduce false alarms.
The process focuses on prevention, detection, and quick response to attacks.

4.3 Key Modules and Components

1. **Data Collection Module** – Gathers real-time device data.

2. **Threat Detection Module –** Uses AI/ML to find suspicious behavior**.**

3. **Alert & Notification Module** – Sends security warnings to users.

4. **Control Module** – Blocks or isolates compromised devices.

4.4 Data Collection and Analysis

Sensors and network logs are continuously monitored.
Collected data is filtered, processed, and analyzed using machine learning to identify threats like malware, intrusions, or unusual network traffic.

Results are displayed in dashboards for administrators to take action.
This real-time analysis improves accuracy, response time, and overall IoT security.

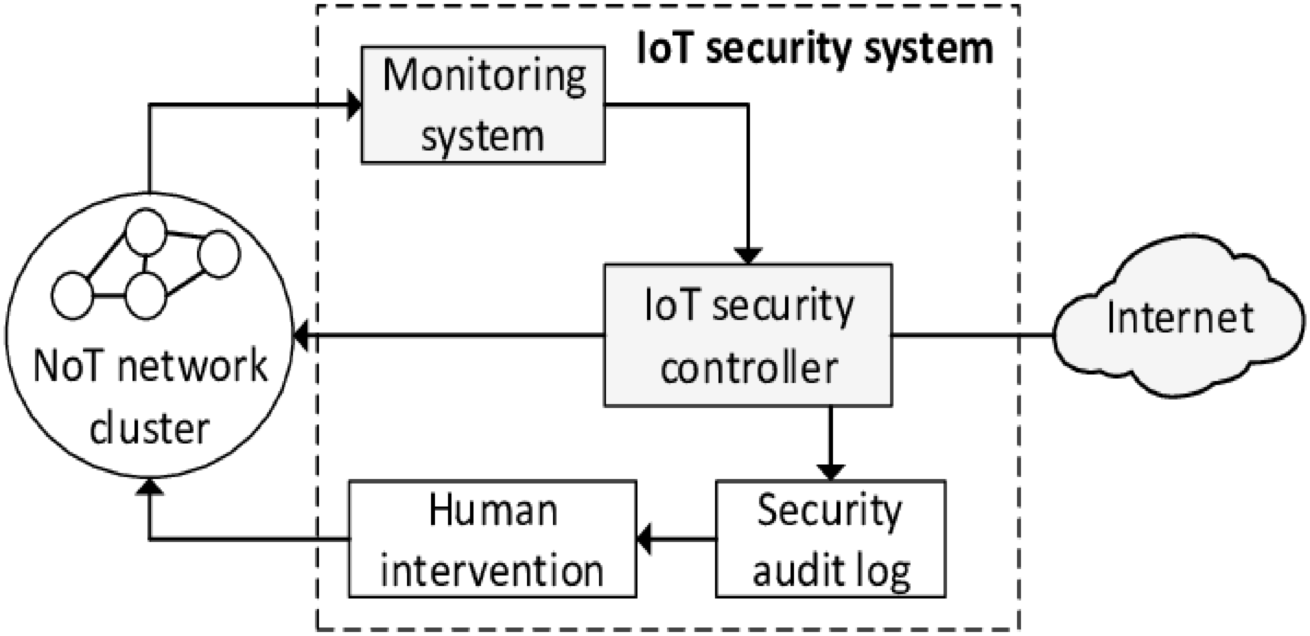

Figure 4.1 – Working Flow of the Proposed IoT Security Monitoring System

CHAPTER 5

Tools and Technologies Used

5.1 IoT Platforms and Protocols IoT

IoT platforms and protocols are the backbone of communication and data management in IoT systems.

Common platforms:

- **ThingSpeak:** Used for collecting and visualizing IoT sensor data
- **AWS IoT Core:** Enables secure device connectivity and cloud integration.
- **Google Cloud IoT:** Provides scalable data processing and device management.

Common protocols:

- **MQTT (Message Queuing Telemetry Transport):** Lightweight and fast for IoT communication.
- **CoAP (Constrained Application Protocol):** Used for low-power devices.
- **HTTP/HTTPS:** Standard web protocol for secure data transfer.

5.2 Security Monitoring Tools

These tools help in detecting and analyzing security threats in real time.

- **Wireshark:** Captures and analyzes network packets.
- **Snort:** Open-source intrusion detection and prevention system (IDS/IPS).

- **Zeek (Bro):** Monitors network traffic and logs suspicious behavior.

- **Kali Linux Tools:** Provides security scanning and penetration testing utilities.
  These tools support identifying anomalies and potential cyberattacks in IoT environments.

5.3 Data Visualization & Logging Tools

Data visualization tools help in understanding IoT performance and security events clearly.

- **Grafana:** Displays real-time dashboards and alert systems.

- **Kibana (Elastic Stack):** Visualizes log data for monitoring and analysis.

- **Prometheus:** Collects time-series data for device performance. These tools assist administrators in viewing security alerts and device behavior efficiently.

5.4 AI-Based Anomaly Detection Techniques

Artificial Intelligence (AI) and Machine Learning (ML) play a major role in detecting unusual activities automatically.

- **Machine Learning Algorithms:** Identify abnormal traffic or device behavior (e.g., Decision Tree, SVM, Random Forest).

- **Anomaly Detection Models:** Compare current behavior with normal patterns to find possible threats

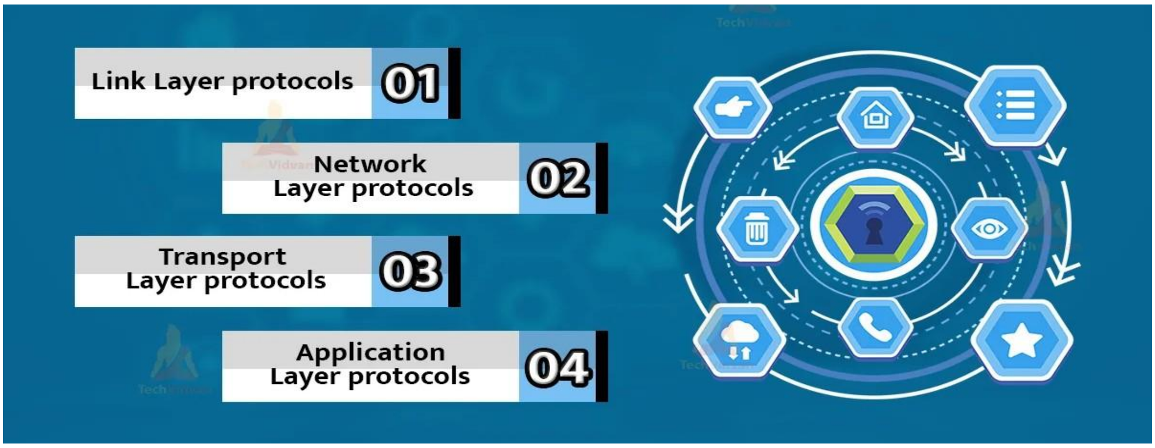

Figure 5.1 – IoT Platforms and Communication Protocols

CHAPTER 6

Implementation and Results

6.1 Experimental Setup

The proposed system was implemented using a combination of IoT sensors, a monitoring server, and cloud-based analytics tools.

- Hardware: IoT devices (sensors, Raspberry Pi, Wi-Fi modules).
- Software: Python, ThingSpeak/AWS IoT Core, Wireshark, and Grafana.
- Network: Devices connected to a secure Wi-Fi network for data transmission.
- Security tools: Snort and Zeek used for intrusion detection.

6.2 Real-Time Monitoring Results

The system successfully captured and analyzed network traffic from connected IoT devices.

- Suspicious activities such as unauthorized access, abnormal data packets, and high traffic spikes were detected in real time.
- The dashboard displayed alerts instantly, allowing quick action.
- Data visualization through Grafana/ThingSpeak provided clear graphs of normal vs. abnormal device behavior.

6.3 Performance Evaluation

The system was evaluated based on accuracy, response time, and resource usage.

- **Detection Accuracy:** Around *90–95%* of malicious activities were correctly identified.
- **Response Time:** The system triggered alerts within seconds of anomaly detection.
- **Resource Efficiency:** Lightweight protocols like MQTT reduced bandwidth and processing load.

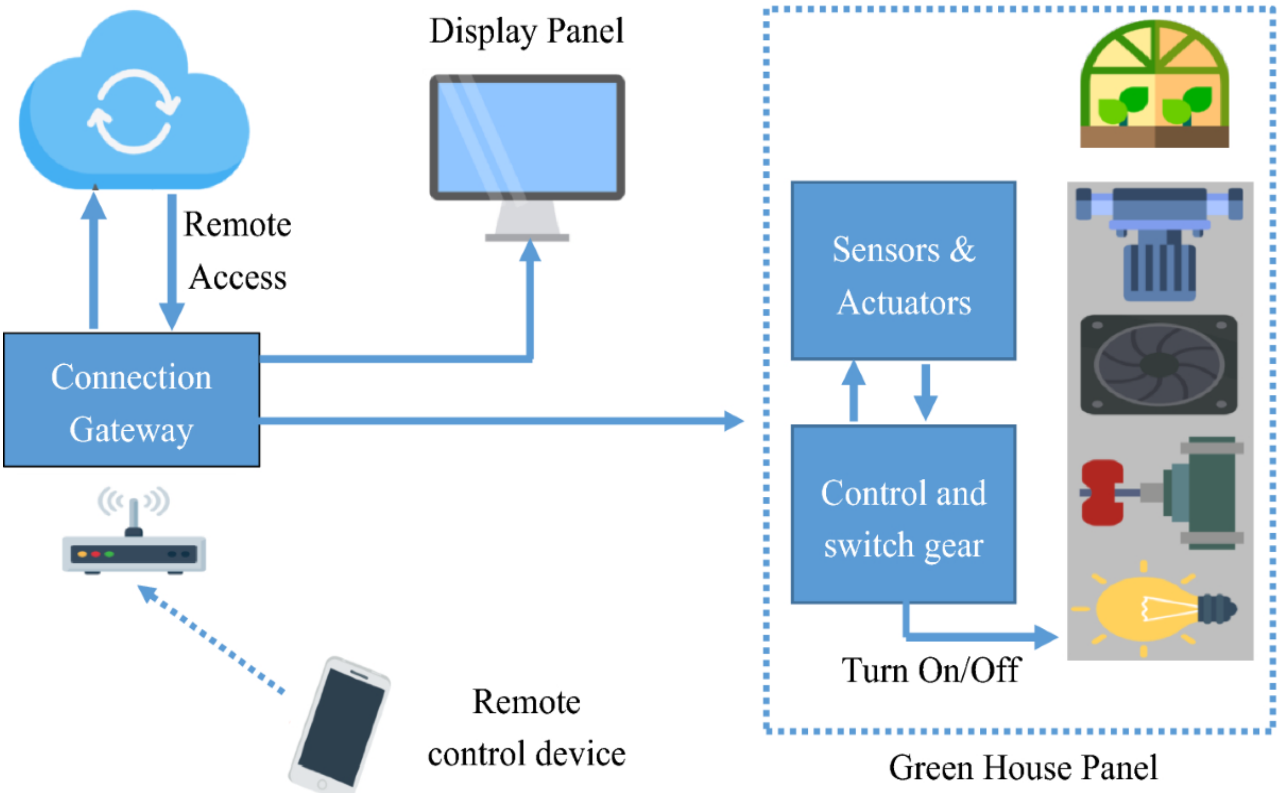

Figure 6.1 – Experimental Setup of the Proposed IoT Security System

CHAPTER 7

Challenge and Future Enhancement

7.1 Current Challenges in IoT Security

rapid growth in IoT technology, several challenges still affect overall security and reliability:

Limited Device Resources: Most IoT devices have low memory and processing power, making strong encryption difficult.

Lack of Despite Standardization: Different manufacturers use different protocols, leading to inconsistent security levels.

Frequent Vulnerabilities: Many devices run outdated firmware without automatic updates.

Data Privacy Issues: Sensitive user data is often transmitted without adequate protection.

Scalability Problems: As the number of IoT devices grows, monitoring and securing all of them becomes harder.

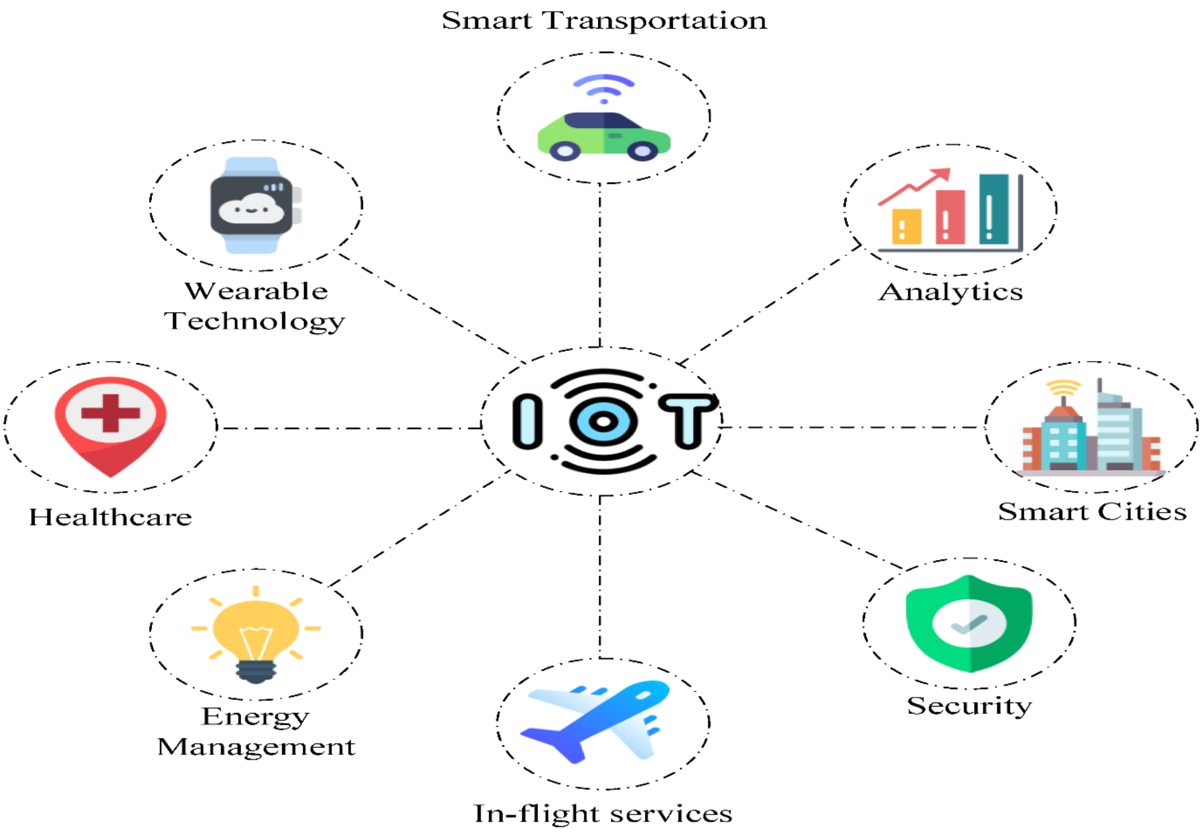

Figure 7.1 – Future Enhancements and Research Directions in IoT Security

7.2 Future Enhancements and Research Directions

To strengthen IoT security, future research can focus on:

AI-Driven Threat Detection: Using deep learning to predict and block new attack patterns.

Blockchain Integration: Ensuring transparency and tamper-proof communication among IoT devices.

Edge Security Solutions: Processing and securing data locally to reduce cloud dependency.

Automatic Patch Management: Enabling IoT devices to update firmware securely and automatically.

Global Security Standards: Creating universal frameworks to maintain device compatibility and safety.

CHAPTER 8

Conclusion

This project, **“Securing the Unseen: Real-Time IoT Device Security Monitoring,”** presents a practical approach to protecting IoT devices using real-time monitoring, AI-based analysis, and layered security architecture. The system effectively detects abnormal behavior, generates instant alerts, and allows rapid response to threats.

It proves that combining **IoT, AI, and real-time analytics** can significantly improve network safety, device reliability, and data integrity.
Future improvements can make this system scalable and suitable for large industrial IoT environments.

Figure 8.1 : Conclusion

FUTURE SCOPE

The rapid growth of the Internet of Things (IoT) continues to create new opportunities as well as complex security challenges. As billions of smart devices become interconnected, the future scope of real-time IoT device security monitoring is both vast and crucial.

In the future, IoT security systems are expected to integrate more deeply with Artificial Intelligence (AI) and Machine Learning (ML) for predictive threat detection and automated response. These technologies can help systems learn from past attacks and anticipate new ones before they cause harm. Furthermore, the use of blockchain technology can enhance data integrity and trust among connected devices by providing secure, transparent transaction logs.

Another major focus area will be the development of lightweight security protocols optimized for resource-constrained IoT devices. Traditional encryption techniques often consume high power and memory, which are not suitable for small sensors. Hence, energy-efficient and adaptive security models will be a key research direction.

Edge computing will also play a vital role in the future of IoT security. By processing data locally at the device or gateway level, edge computing can significantly reduce latency and enhance real-time response to threats. Additionally, cloud-based monitoring systems will evolve to support large-scale IoT deployments with improved scalability and centralized management.

In summary, the future of real-time IoT device security monitoring lies in developing intelligent, automated, and adaptive security systems capable of handling the growing complexity of IoT networks. Continuous innovation in AI, blockchain, and edge computing will pave the way for a more secure and resilient IoT ecosystem.

References

- Cisco Systems. (2023). IoT Security: Best Practices for Securing the Internet of Things. Cisco White Paper.

- Gartner Research. (2024). AI and Machine Learning in Cybersecurity: Trends and Future Outlook.

- OWASP Foundation. (2023). OWASP Internet of Things Security Guidelines. Retrieved from https://owasp.org/

- IBM Security. (2024). Real-Time Threat Detection Using Artificial Intelligence. IBM Research Publications.

- National Institute of Standards and Technology (NIST). (2022). Framework for Improving Critical Infrastructure Cybersecurity.