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

Presented By
Name Raman Kumar
Registration No - 2301326327

Under the Guidance of
Prof. Himanshu Shekhar Maharana

Department of Electrical & Computer Engineering
Gandhi Institute for Education & Technology
Baniatangi,Bhubaneswar,khordha-752060

Introduction to IoT

- Network of interconnected smart devices
- Used in homes, industries, healthcare, and more
- Communicates over the internet autonomously

Growth of IoT Ecosystem

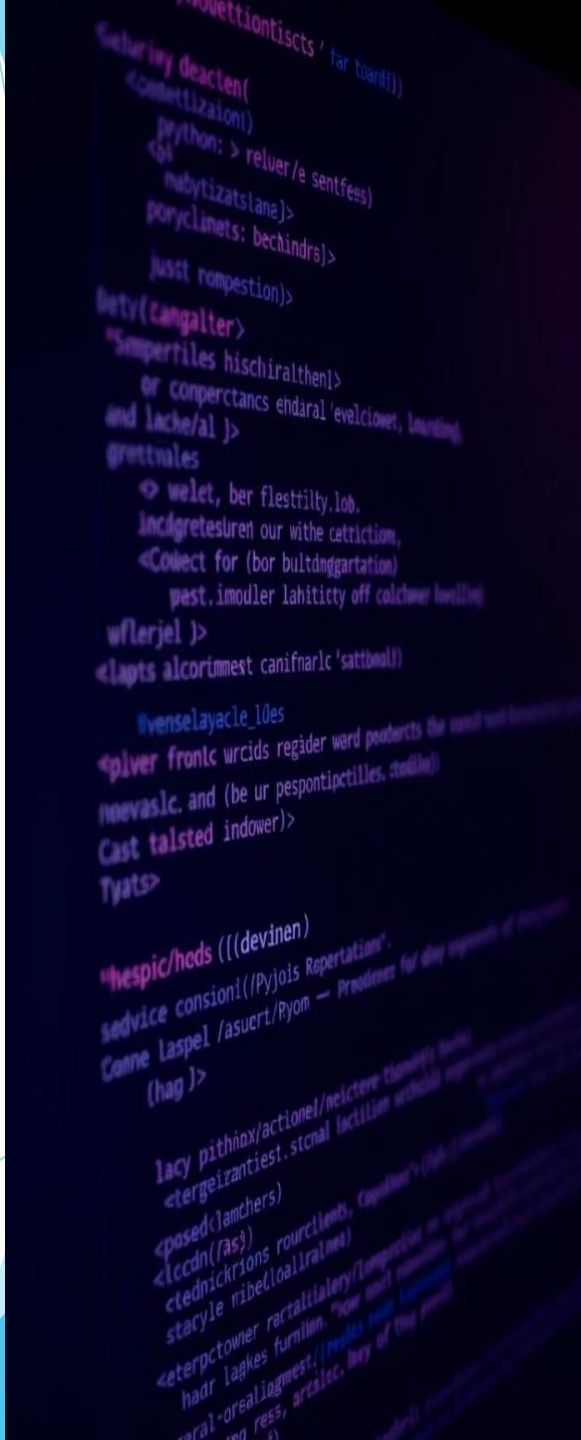
- Billions of devices deployed globally
- Increasing automation in daily life
- Expanding attack surface for hackers

Key Features

- Real-time traffic inspection and analysis
- ML-driven anomaly detection
- Signature-based threat identification
- Alert notifications (email, SMS, webhook
- Automated response actions

Technologies Used

- **Language** - Python, Node.js, HTML , CSS, JavaScript.
- **Network Tools** - Zeek , Suricata, tcpdump ,WireShark.
- **Machine Learning** - scikit-learn, TensorFlow, Isolation Forest.
- **Supported Protocols** - MQTT, CoAP, HTTP, Zigbee, UPnP

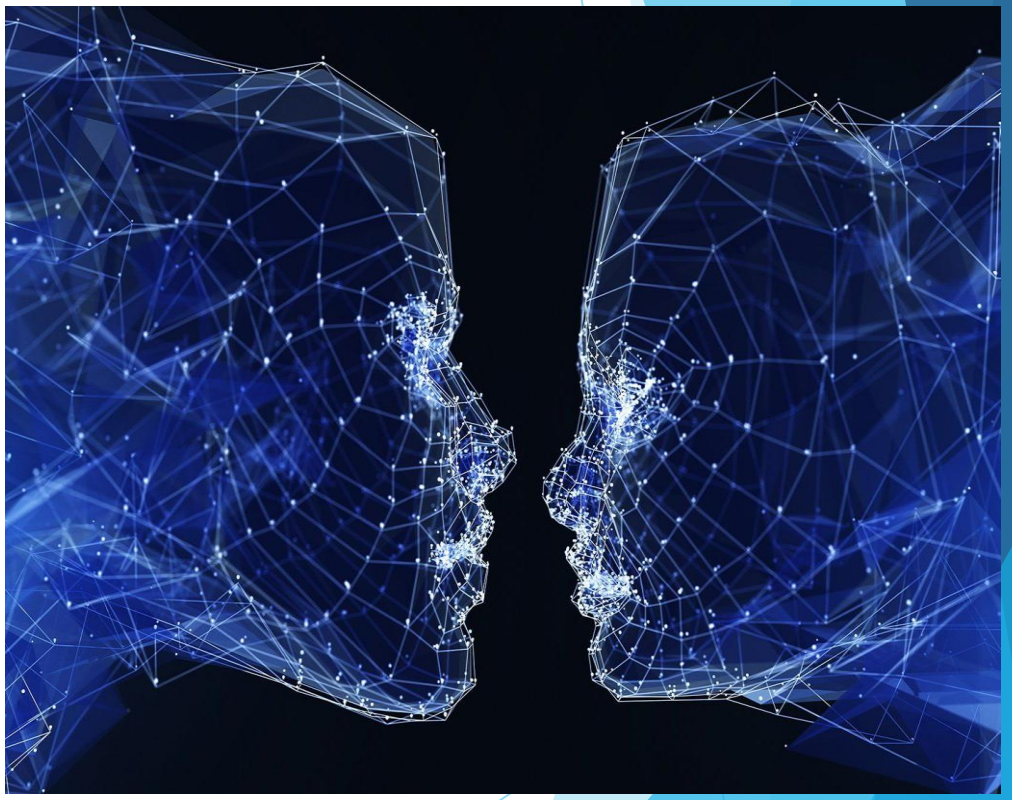


Why IoT Security Matters

- Devices handle sensitive data
- Compromise can impact safety and privacy
- Weak security can enable large-scale attacks

Challenges in IoT Security

- Limited processing capabilities
- Lack of standard security guidelines
- Weak Authentication & Authorization
- Poor manufacturer support
- Data Privacy Issues



Benefits in IoT Security

1. Early Threat Detection
   - Identifies suspicious behavior or attacks

2. Enhanced Data Privacy
   - Protects sensitive user and system data from tampering or leaks

3. Continuous Protection

Protection Ensures that even unattended

Real-World Applications

Smart Homes

Detect compromised smart TVs or locks.

Smart Cities

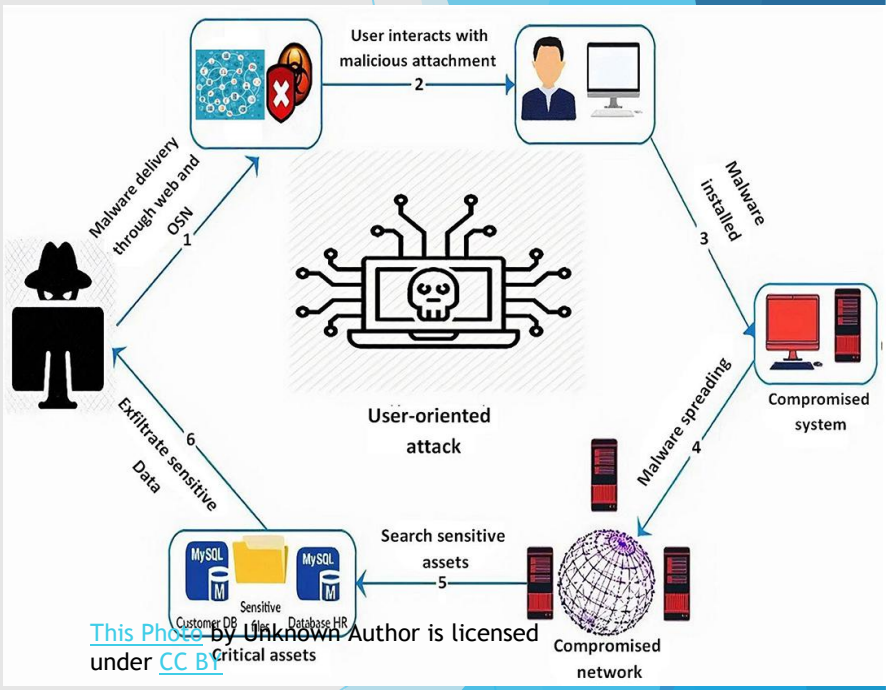
- Monitor traffic systems, public Wi-Fi routers, and surveillance cameras cameras

Industrial IoT

- Secure SCADA systems and PLCs

Common IoT Vulnerabilities

- Weak/default passwords
- Unpatched firmware
- Unencrypted network communication
- Third-Party Component Risks
- Physical Access Vulnerabilities



Future of **Enhancements**

1

Blockchain Authentication

Ensure tamper-proof device identity

2

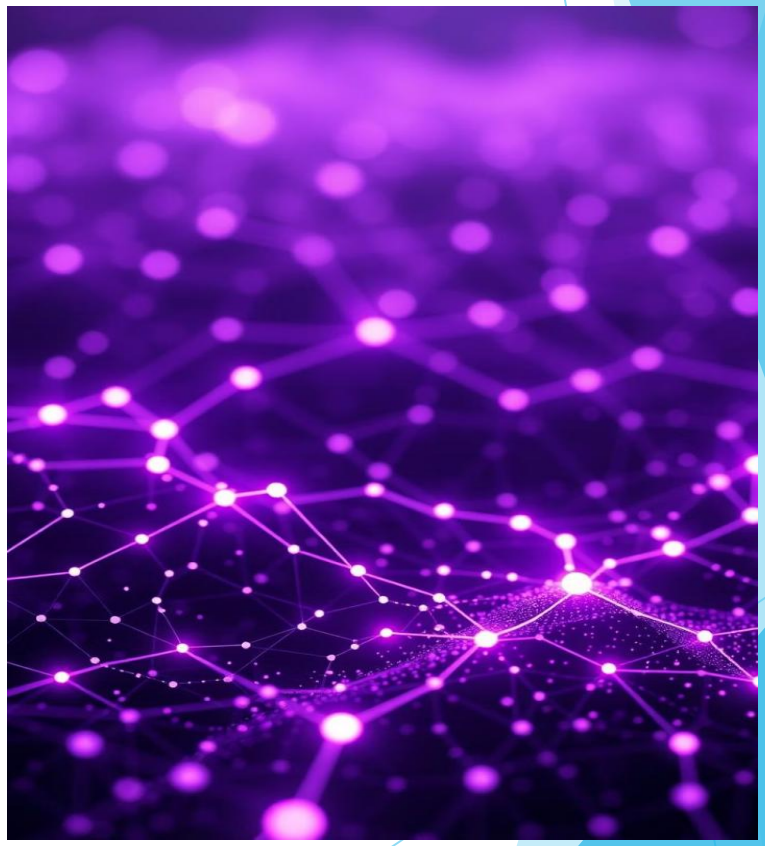
Federated Learning

Train ML models without sharing raw data

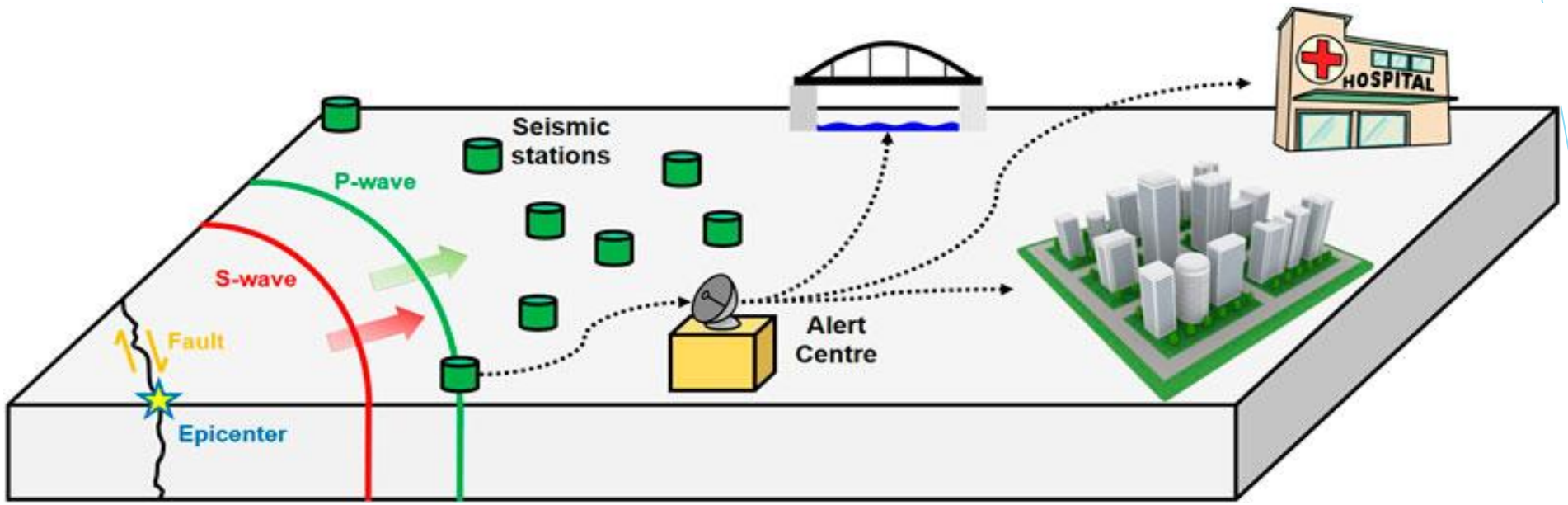
3

Threat Intelligence Feeds

Integrate with sources like AlienVault OTX



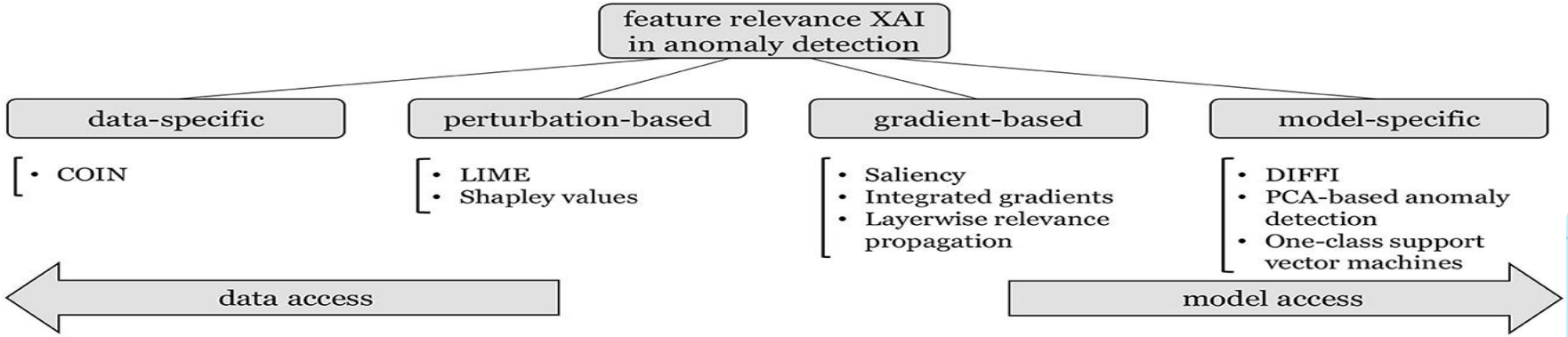
Alerting and Automated Response



- Immediate administrator notification
- Immediate administrator notification
- Automated blocking of malicious traffic

Anomaly Detection Techniques

- ✓ Rule-based detection
- ✓ Signature-based patterns
- ✓ Machine learning algorithms



Security Dashboards

- Visual representation of alerts
- Track device health and status
- Provides risk insights to administrators

Conclusion

1. Real-time monitoring reduces hidden threats

2. Essential for continuous device safety

3. Future innovations will enhance resilience

Thank You!