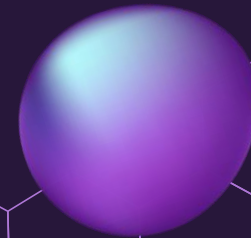




Security in IoT Devices using AI based Intrusion Detection System

Tsinghua University
IEDE-Spring 2024





Team Lead

Major: Computer
Science

Degree: Bachelor

IEDE ID: 2024040


Soumi
sen



Team Members



Komlanvi
Jacob
MANEH

Major: Agricultural
Environmental
Sciences

Degree: Master

IEDE ID: 2024172



Asim
Saleem

Major: Information
and Communication
Engg.

Degree: PhD

IEDE ID: 2024124



Izhar ul
Haq

Major: Control
Science and Engg.

Degree: PhD

IEDE ID: 2024069



Collins
Kandale
Kalonde

Major: Civil Engg.

Degree: Masters

IEDE ID: 2024113



Karamoko
Israel Axel

Major: Robotics
Engg.

Degree: Bachelor

IEDE ID: 2024043



Gambo
Koudjam
Giovann

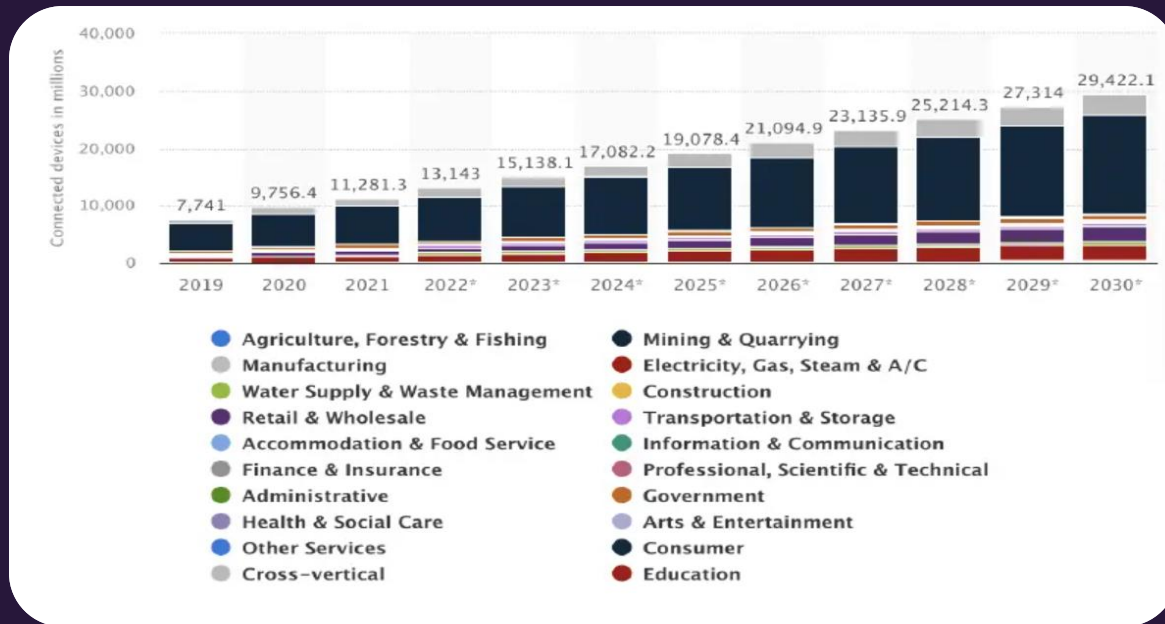
Major: Robotics
Engg.

Degree: Bachelor

IEDE ID: 2024074

Rise of IoT Devices

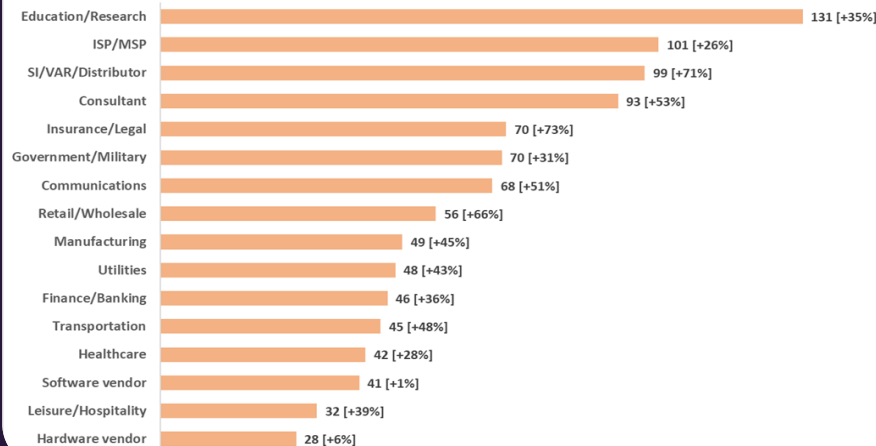
The proliferation of IoT devices has revolutionized our daily lives. From smart homes to industrial automation, these devices have become indispensable. However, their widespread adoption has also made them vulnerable to cyber attacks.



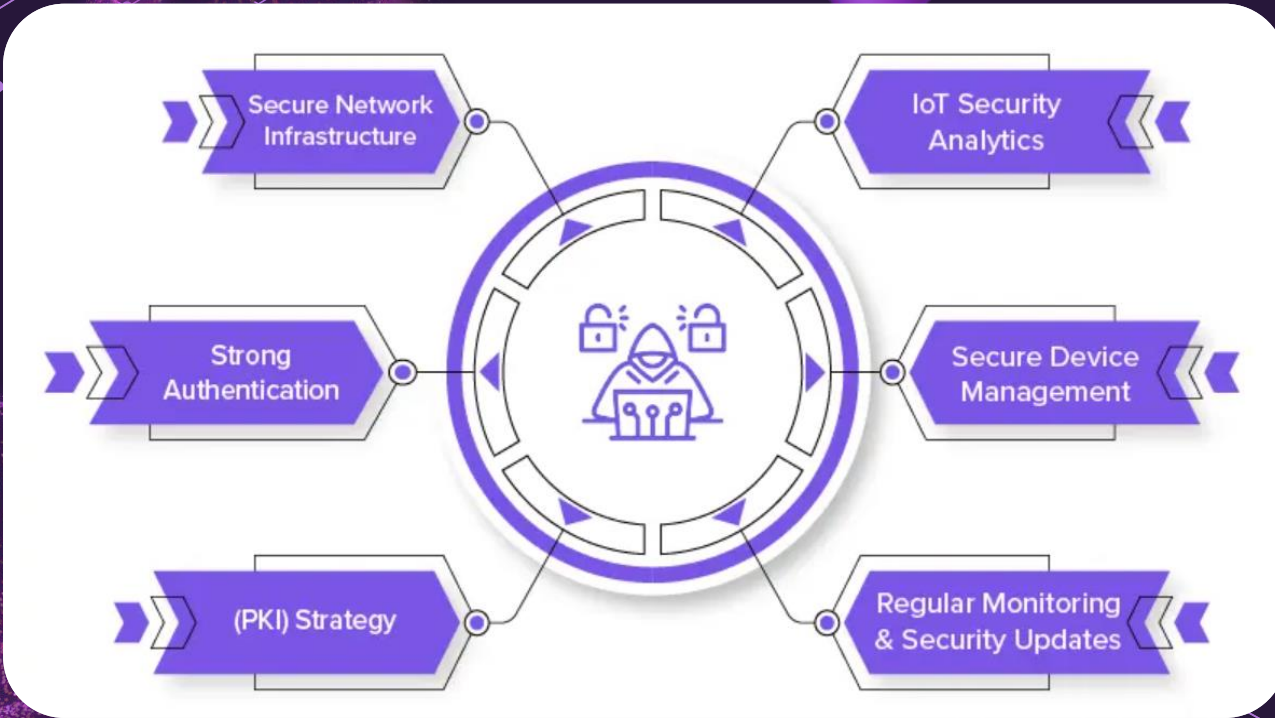
Why do we need to Secure IOT Devices

Imagine your smart thermostat, fitness tracker, or home security camera falling into the wrong hands. Without proper security measures, these devices could be exploited by hackers to spy on your home, steal personal information, or even cause physical harm. Securing IoT devices ensures that your data remains private, your home stays safe, and your devices work as intended without the risk of being tampered with by malicious actors.

Average weekly IoT cyber attacks per organization by sector - Jan-Feb 2023 vs. 2022



Traditional Methods for Protecting IOT Devices



Challenges in IoT Devices Security

Securing IoT devices presents unique challenges due to their diverse nature and limited resources. Traditional security measures are often inadequate, leading to increased susceptibility to cyber threats and intrusions.



Role of AI in Intrusion Detection

Harnessing the power of AI, we can develop sophisticated intrusion detection that continuously monitor and analyze IoT device behavior. This proactive approach enables real-time threat detection and response.

01

Revolutionizing Threat Intelligence

02

Advanced Machine Learning Algorithms

03

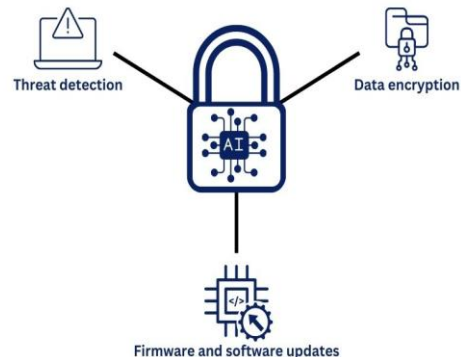
Collaborative Threat Intelligence Sharing

04

Automated Incident Response

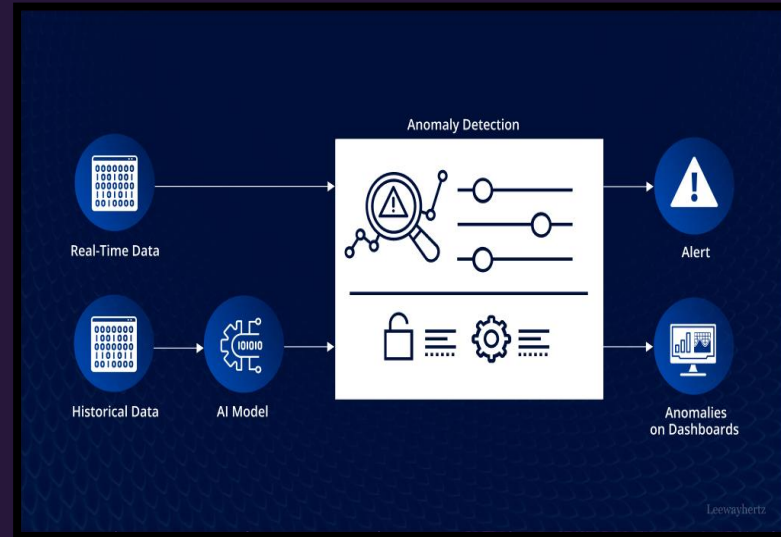
05

Continuous Monitoring and Threat Hunting



Threat and Anomaly Detection

- Threat vs. Anomaly Detection in AI-powered IoT Security
 - Threat detection focuses on identifying known malicious activities
 - Anomaly detection looks for unusual deviations from normal device behavior
- AI's Role in Real-time Threat and Anomaly Detection
 - AI analyzes vast amounts of data from IoT devices in real-time
 - AI automates the process, replacing manual monitoring and improving accuracy
- Benefits of AI-based Detection in Smart Homes
 - AI can detect threats like unauthorized login attempts
 - AI can identify anomalies like unusual sensor readings
 - Prompt alerts enable quick action to prevent security issues or malfunctions



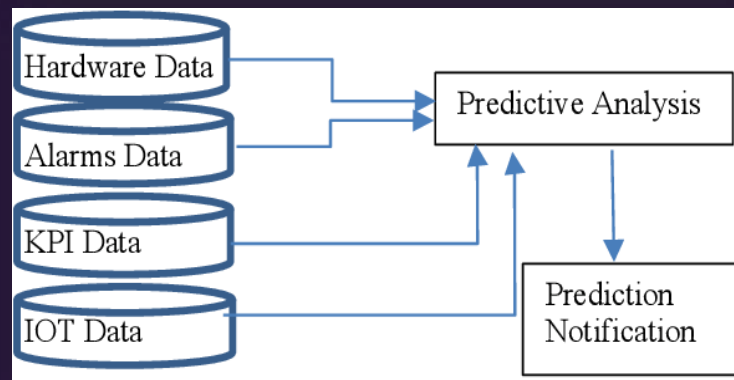
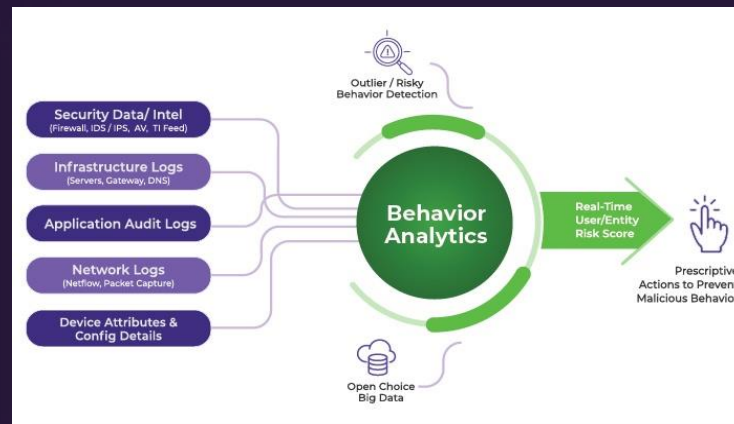
Behavioural and Predictive Analysis

- Different Approaches

- Behavioral analysis: Examines current patterns to identify anomalies or suspicious activities
- Predictive analysis: Forecasts future threats based on historical data and trends

- AI's Role in Security with Both Methods: Analyzes data and uses machine learning algorithms to:

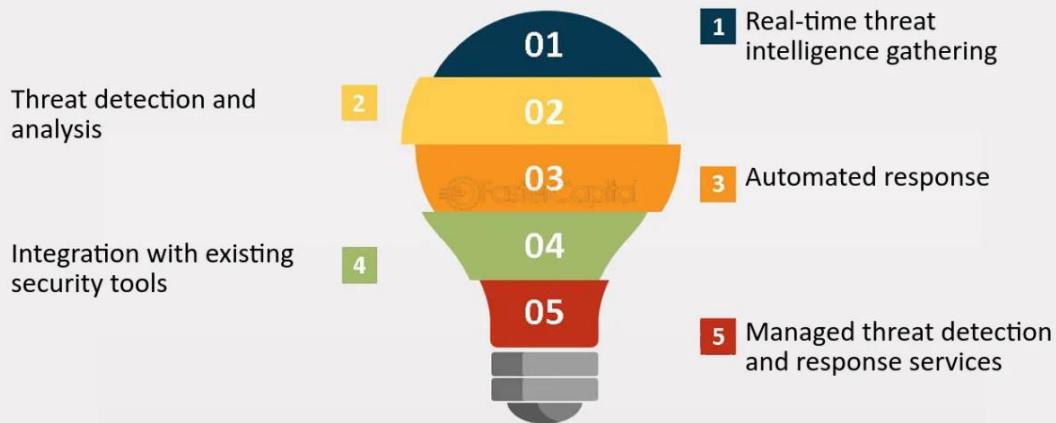
- Detect patterns for behavioral analysis
- Predict potential security incidents for predictive analysis



Real-Time Threat Response

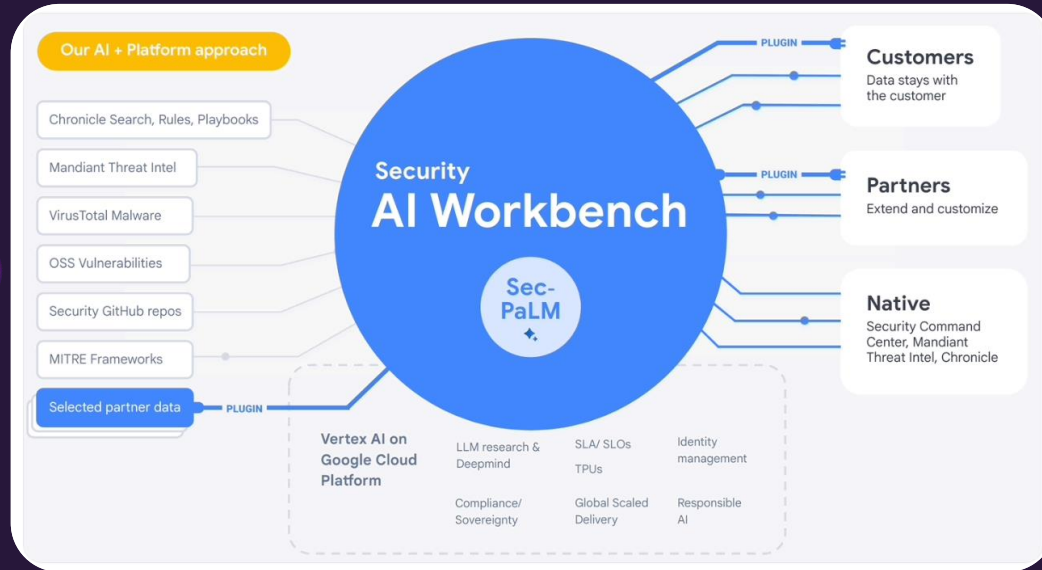
With AI-driven intrusion detection, we can swiftly respond to potential threats, minimizing the impact of security breaches. This proactive approach enables us to maintain the continuous operation of IoT devices.

Real-Time Threat Intelligence and Response



Collaborative Security Ecosystem

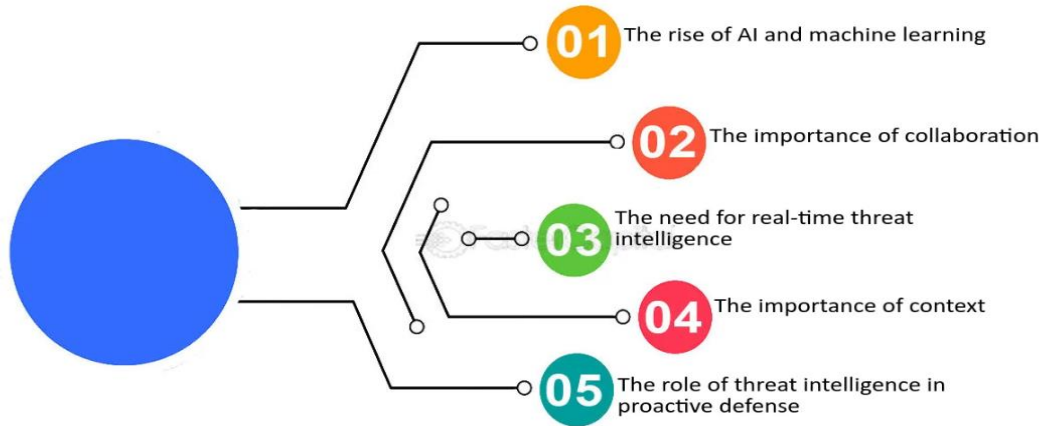
Establishing a collaborative ecosystem where AI-powered intrusion detection systems share threat intelligence enables a collective defence approach. This interconnected network strengthens the overall security of IoT devices.





Future of IoT Security

- Threat intelligence is crucial for proactive cyber defense by identifying and prioritizing threats. This enables organizations to implement preventive measures like patching vulnerabilities before attackers can exploit them.
- The rise of AI, collaboration, real-time capabilities, and focus on context empowers organizations to defend against cyber threats. By embracing these trends, organizations can stay ahead of the curve and better protect themselves from cyberattacks.

Future of Threat Intelligence and Proactive Cyber Defense





AI-powered intrusion detection is a game-changer in fortifying the security of IoT devices. By leveraging advanced technology and proactive defence mechanisms, we can safeguard the interconnected world of IoT.



THANKS!

DO YOU HAVE ANY QUESTIONS?

sensoumi4946@dingtalk.com

+86-18258412953

