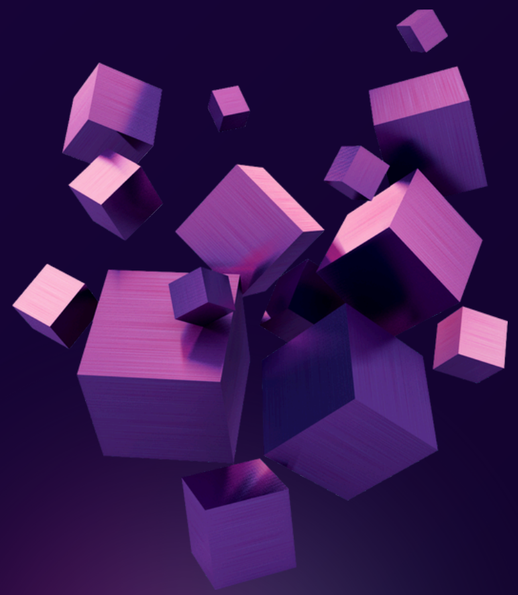
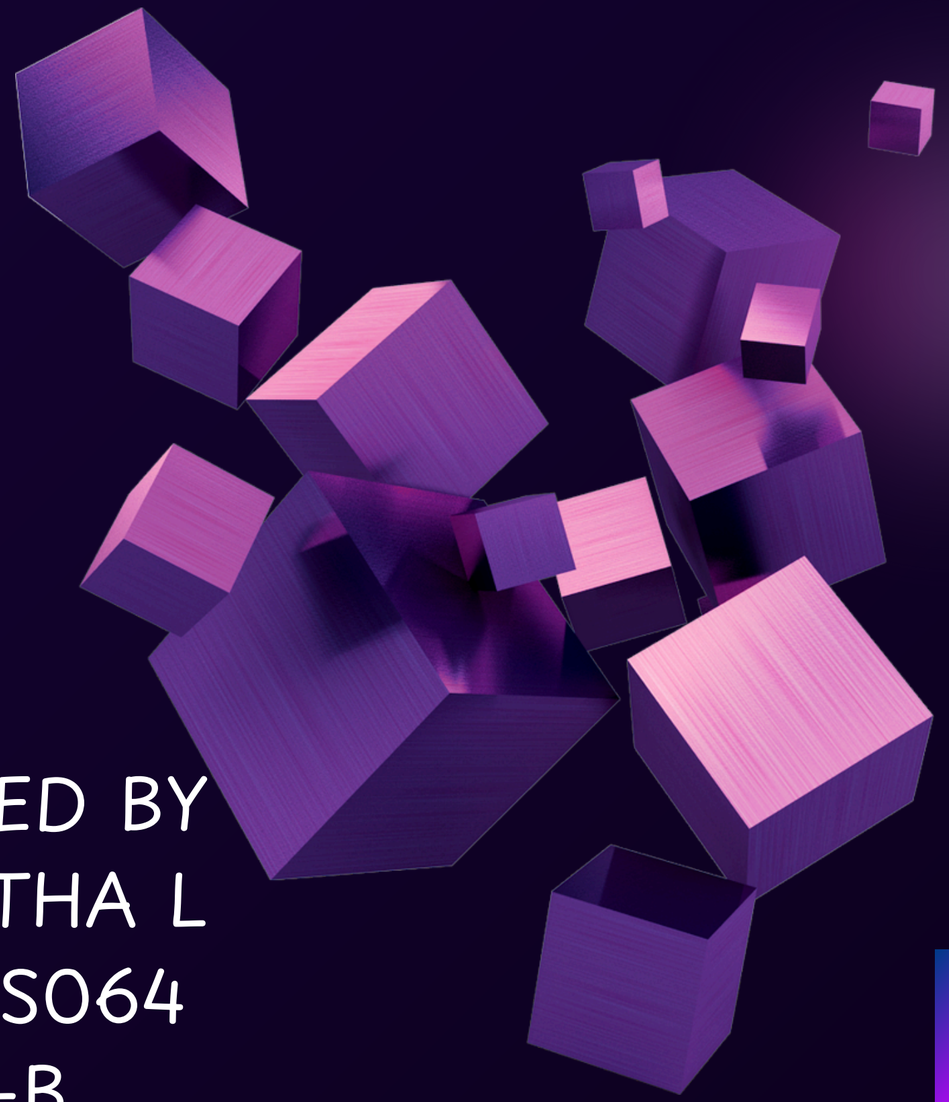
SECURE NET IDEA PITCHING





PREPARED BY
HARSHITHA L
4NI23CS064
CSE-B

Slide 1: The Problem - Challenges of Securing IoT Networks

The rapid growth of IoT devices has led to billions of interconnected devices operating across various networks, creating an expansive attack surface for cyber threats. Traditional security methods, like rule-based systems, struggle to keep up with the dynamic nature of these environments. They often fail to process the vast amount of real-time data generated by IoT devices, resulting in high false-positive rates and missed detections of zero-day attacks. Additionally, IoT networks are highly heterogeneous, comprising devices with varying security capabilities and resource limitations. This complexity, coupled with the increasing frequency of cyberattacks, has led to significant risks, including data theft, privacy violations, operational disruptions, and financial losses.

Slide 2: The Solution - AI/ML for Enhanced Threat Detection

Artificial Intelligence (AI) and Machine Learning (ML) offer transformative solutions for addressing IoT security challenges. These technologies enable real-time analysis of network traffic and device behavior to detect potential threats. ML techniques, such as supervised learning, can identify known attack patterns, while unsupervised learning excels at detecting anomalies, including previously unknown threats. Reinforcement learning can further optimize real-time responses to attacks. AI-driven solutions also facilitate predictive analytics to proactively prevent breaches. By leveraging adaptive learning, AI continuously improves its threat detection capabilities, making it an indispensable tool in combating sophisticated and evolving cyber threats.

Slide 3: System Architecture – AI & IoT Integration

A robust AI-driven IoT security system integrates multiple layers to enable real-time threat detection and response. At the device layer, IoT sensors and actuators transmit data, which is then preprocessed at the edge using lightweight AI models. This edge AI processing reduces latency and minimizes reliance on centralized systems. Data from edge devices is aggregated and analyzed on a cloud-based AI platform, where advanced ML models identify complex and coordinated threats. A centralized threat intelligence database stores known attack signatures and behavioral patterns, enhancing the system's accuracy. The architecture also includes a centralized command system to issue real-time alerts and automate threat mitigation strategies, ensuring swift responses to potential breaches.

Slide 4: The Impact - Enhancing IoT Security

AI/ML integration significantly enhances IoT security by improving threat detection accuracy and reducing false-positive rates. Automated, real-time responses ensure faster mitigation of cyberattacks, while scalable solutions accommodate the diversity of IoT devices. In the short term, these advancements lead to improved operational resilience and minimized downtime. Over the long term, AI-driven systems pave the way for a unified IoT security ecosystem capable of self-healing through autonomous learning and vulnerability patching. By reducing the impact of cyberattacks, these technologies safeguard the interconnected future and protect organizations from financial losses and reputational harm. Investing in AI-powered IoT security is vital for creating a resilient and secure digital environment.