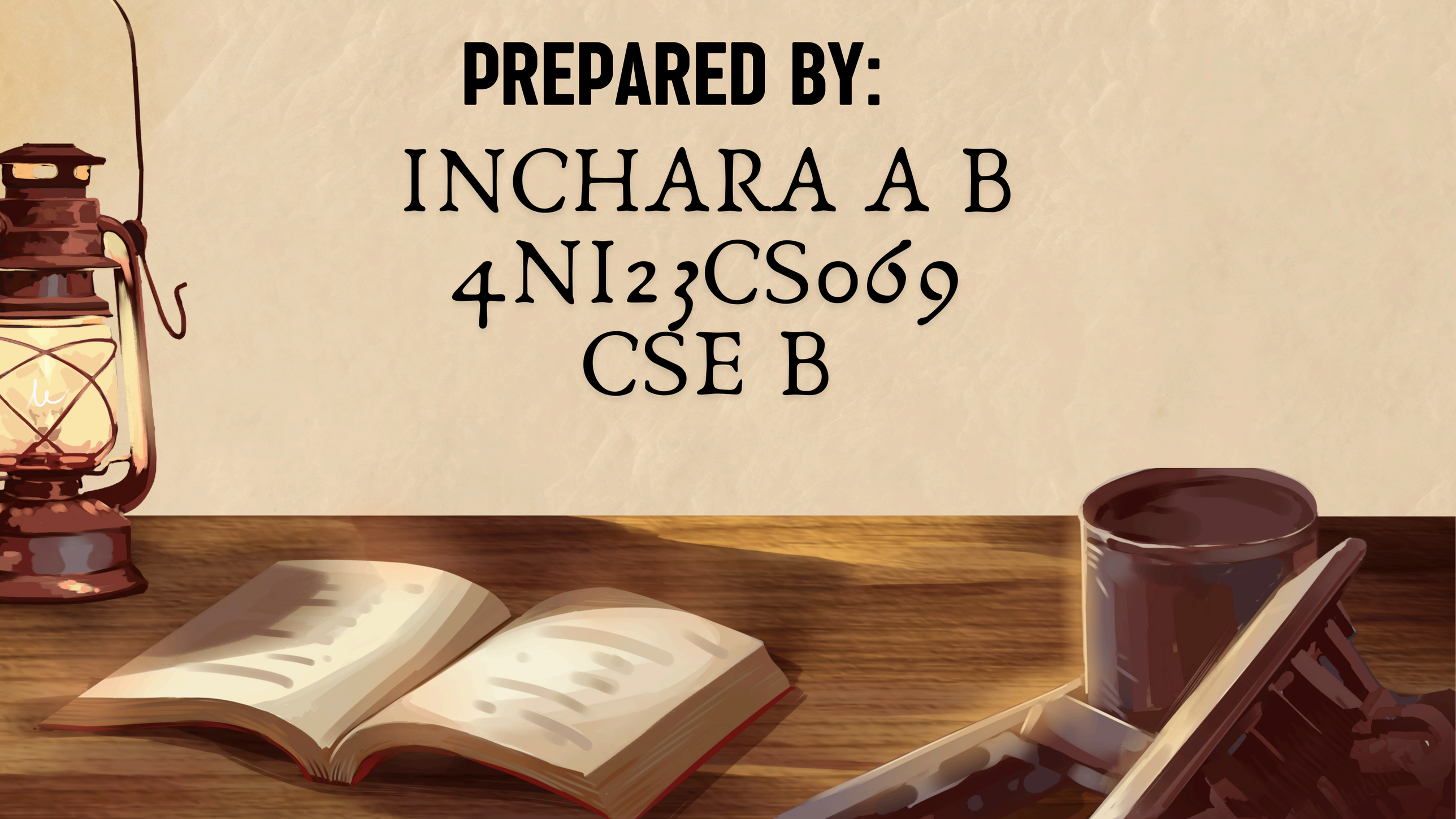


PREPARED BY:

INCHARA A B

4NI23CS069

CSE B

Problem 1:

As more devices become interconnected through the Internet of Things (IoT), securing these devices from cyber threats becomes increasingly challenging. Traditional security methods often fail to detect real-time attacks, leading to breaches

SOLUTION:

Absolutely, the interconnected nature of IoT devices presents a significant challenge in terms of cybersecurity. Traditional security methods often fall short in detecting real-time attacks, which can lead to breaches. This is where advanced technologies like AI and machine learning come into play. By leveraging these technologies, we can enhance threat detection and prevention in IoT environments, making them more secure and resilient against cyber threats.

Problem 2:

Your idea should focus on using AI and Machine Learning to improve real time threat detection and prevent cyberattacks in IoT environments.

SOLUTION:

AI/ML-Based Threat Detection and Prevention:

- Anomaly Detection: Use ML algorithms to learn the normal behavior of IoT devices and detect anomalies that may indicate a cyberattack.
- Predictive Analysis: Implement AI models that predict potential threats based on historical data and current trends.
- Automated Response: Develop AI systems that can automatically respond to detected threats in real-time, minimizing the impact of attacks.

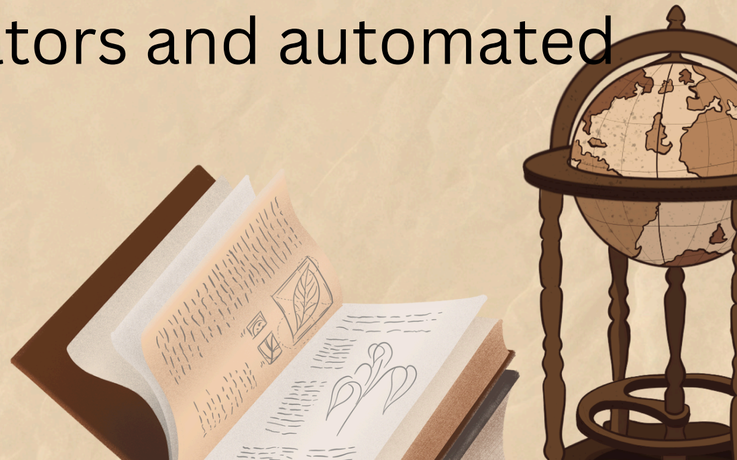
Problem 2:

Your idea should focus on using AI and Machine Learning to improve real time threat detection and prevent cyberattacks in IoT environments.

SOLUTION:

Integration of AI and IoT Devices:

- Data Collection: Gather data from various IoT devices and sensors.
- Data Processing: Use edge computing to process data locally and reduce latency.
- AI/ML Models: Deploy AI/ML models on the edge or in the cloud to analyze data and detect threats.
- Real-Time Alerts: Send real-time alerts to administrators and automated systems for immediate action.



Expected Impact and Future Vision

Short-Term Improvements:

- Enhanced detection of real-time threats.
- Reduced response time to cyberattacks.
- Improved overall security of IoT networks.

Long-Term Vision:

- Development of more sophisticated AI models that can adapt to new types of threats.
- Creation of a robust and resilient IoT ecosystem that can withstand cyberattacks.
- Continuous improvement of security measures through AI-driven insights and analytics.

By focusing on these areas, we can significantly improve the security of IoT environments and protect them from cyber threats. This approach not only addresses current challenges but also prepares for future advancements in IoT security.

THANK YOU