INTEL HACKATHON

AI DRIVEN CYBER RESILIENCE FOR DRONES SWARMS

USING INTEL ONEAPI

Present by Vigilant Vanguards ,A0234

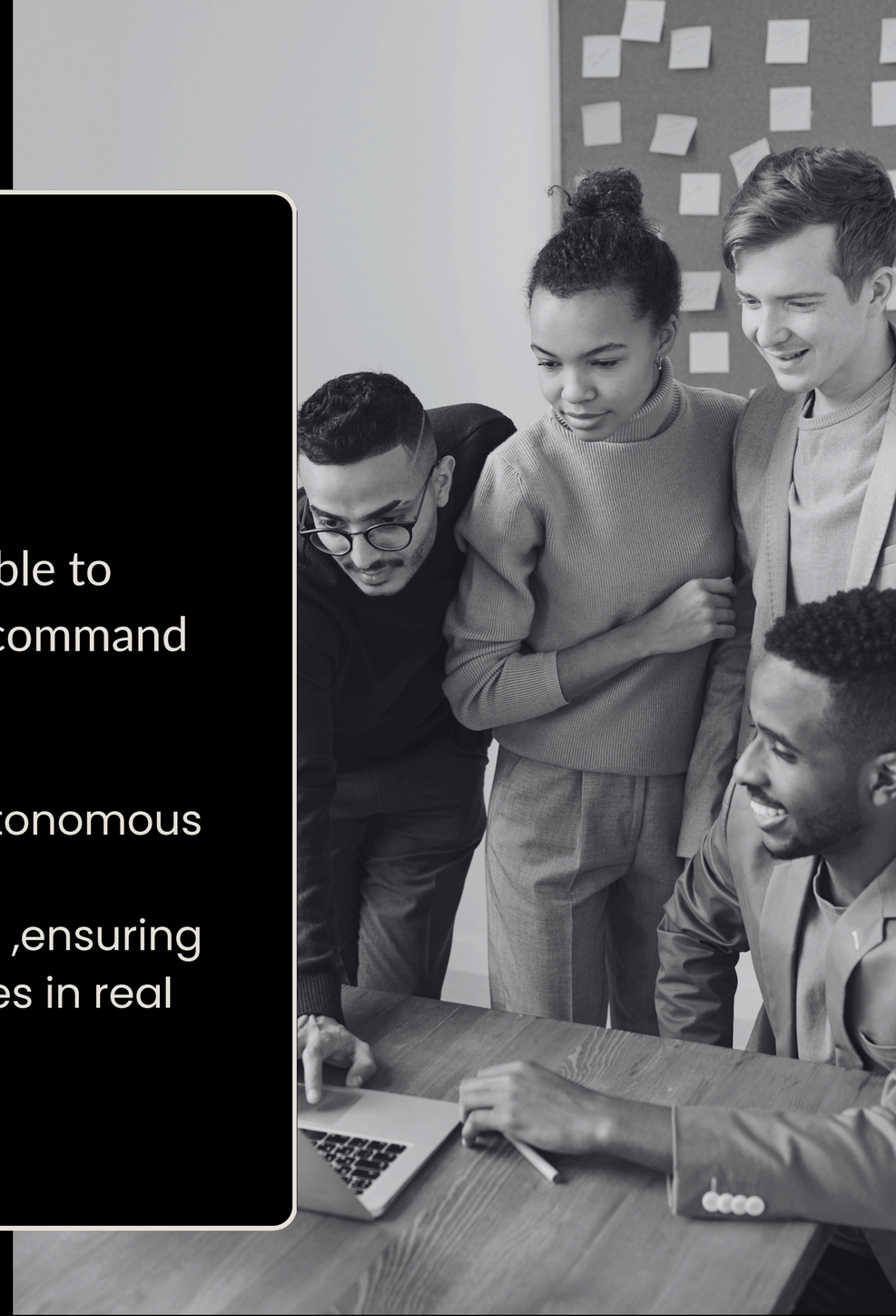
PROBLEM STATEMENT

Drones which are used in military operations are vulnerable to cyber attacks such as GPS spoofing, signal jamming and command injection attacks.

Solution:

a) Designing an AI based intrusion detection system for autonomous drone swarms.

b) Integrate AI Driven Cybersecurity with swarm intelligence ,ensuring decentralized and distributed security across multiple drones in real time.



WORKING

Data Preprocessing

a) collect data from sensor
b) Handle missing data,normalization and feature selection
c) Data cleaning to ensure reliability

Isolation forest for anomaly detection

a) Unsupervised anomaly detection
b) Random partitioning of data
c) Isolation forest tree visualization

Detection

Flagging deviation in flight behavior or sensor malfunctions or unexpected environmental conditions

Fail Safe Mode Activation

a) Transitioning to a safe state when an anomaly is detected.
b) Automatic activation of fail state mode when an anomaly is detected.

Real Time messaging system

a) Notification system for anamalies .
b) Message passed indicating a problem in specific drone.
c) Integration with communication systems for real time alerts to the control center.

TECHNICAL APPROACH AND INTEGRATIONS

a) **Using OpenVino ToolKit**

i) We used Intel Open Vino Toolkit for optimization of machine learning models for edge inference on drones

ii) Model deployment on intel hardware

b) Dashboard

i) Real time anomaly tracking

ii) Display of key metrics

iii) Interactive and userfriendly design

CONCLUSION

a) Our solution provides effective protection for drone swarms in hostile environment through real time ,decentralize AI driven security.
b) By leveraging Intel’s toolkits ,we ensure enhanced performance and adaptability in detecting and neutralizing cyber threats.