

Fortifying IoT Ecosystems: A Hybrid Security Framework with Blockchain & AI

Junior Gonzalez, Cedric Green, Winaldo Walker

Aparicio Carranza, Ph.D

Vaughn College of Aeronautics and Technology

Marist Computing Conference: Poughkeepsie, NY – November 7, 2025



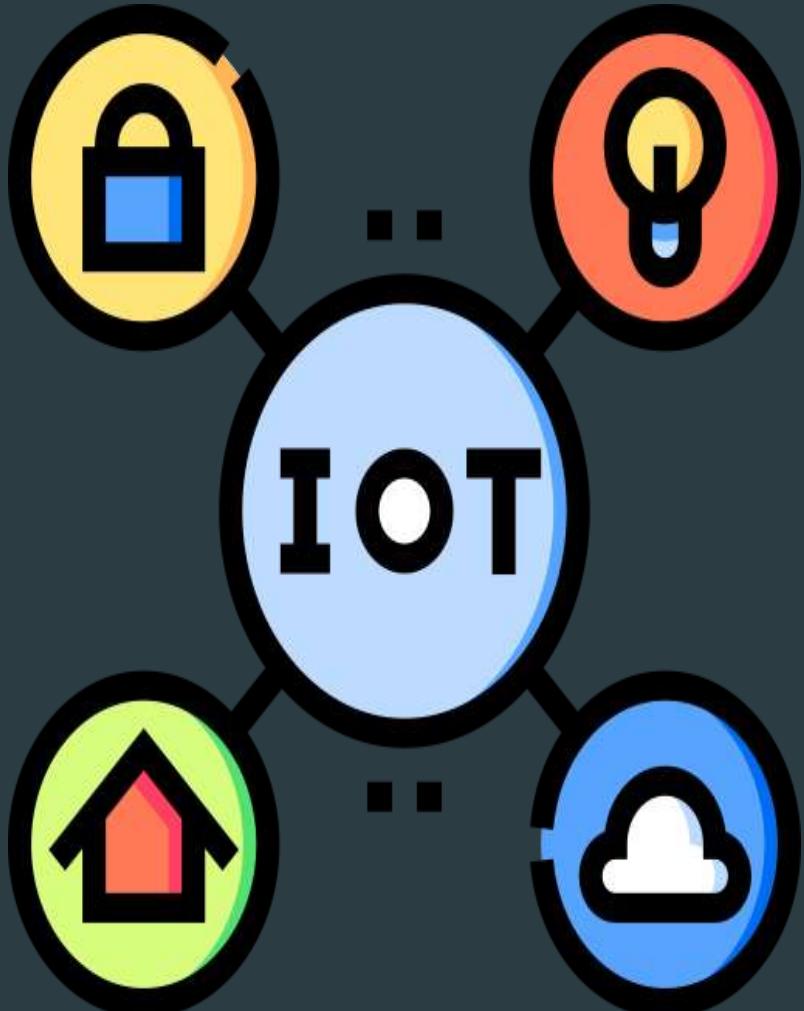
AGENDA

- ▶ Introduction
- ▶ What is IoT?
- ▶ Security Problems Within IoT
- ▶ Blockchain
- ▶ AI IDS
- ▶ Proposed Solution
- ▶ Methodology
- ▶ Results
- ▶ Conclusion
- ▶ Reference

Introduction

- ▶ *The Internet of Things (IoT) connects billions of devices that communicate and share data across the globe*
- ▶ *These devices often handle sensitive/critical information, making them prime target for cyberattacks*
- ▶ *A major challenge in present time is ensuring that IoT devices data transfer is secure, trustworthy and verifiable*
- ▶ *Our project aims to tackle this challenge*
- ▶ *We propose a multi-layered security framework by integrating Blockchain for data-integrity and an AI-based Network Intrusion Detection System for IoT communication*
- ▶ *Our primary goal is to build a resilient IoT environment that can detect, prevent, and ultimately recover from cyber-threats in real time*

What is IoT (Internet of Things)



- ▶ Network of interconnected physical devices exchanging data through the internet
- ▶ Highly advantageous for automation, real-time monitoring and more across various industries
- ▶ IoT devices include wearables, smart home appliances, healthcare devices, and connected vehicles

Security Problems Within IoT



High exposure to spoofing, data tampering and man-in-the-middle attacks



Centralized authentication models prone to compromise



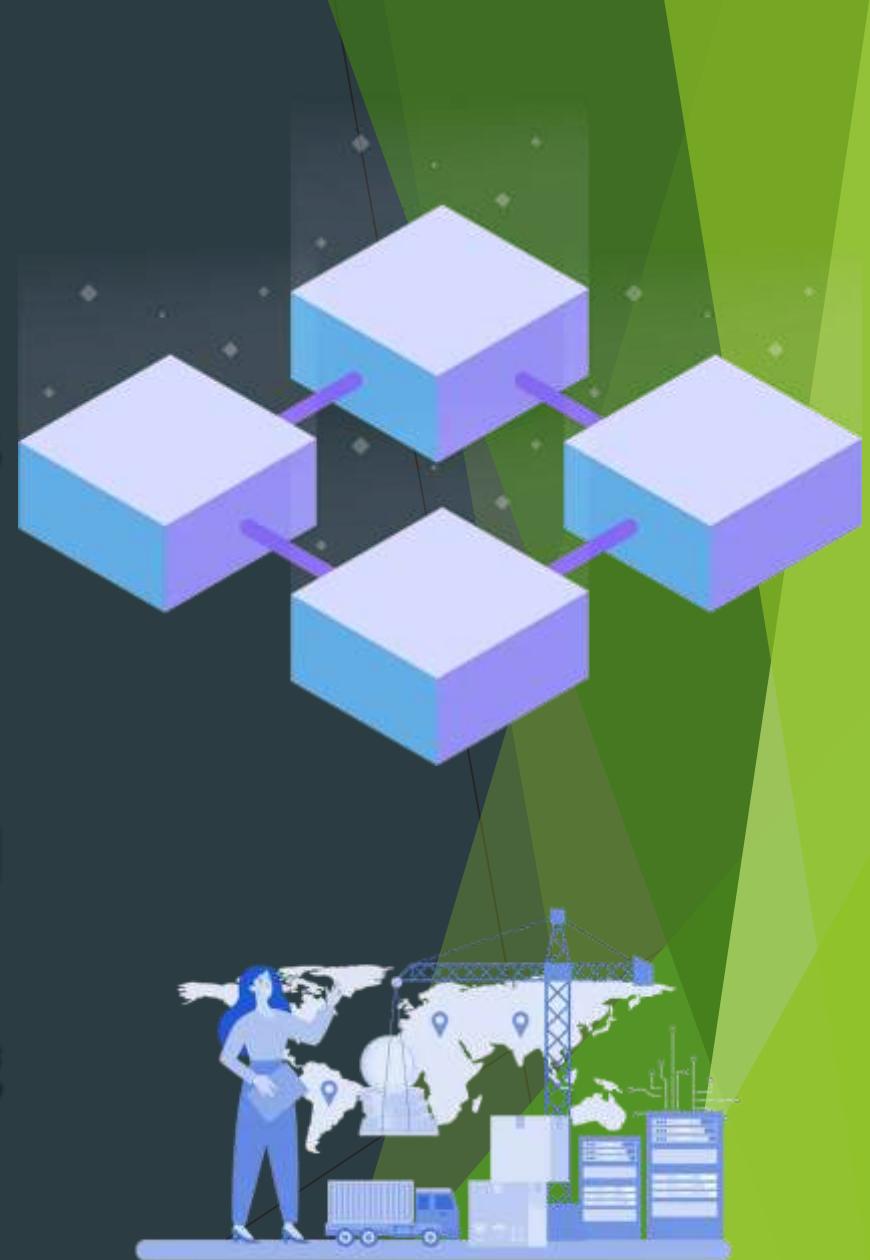
Lack of real-time threat detection and data integrity



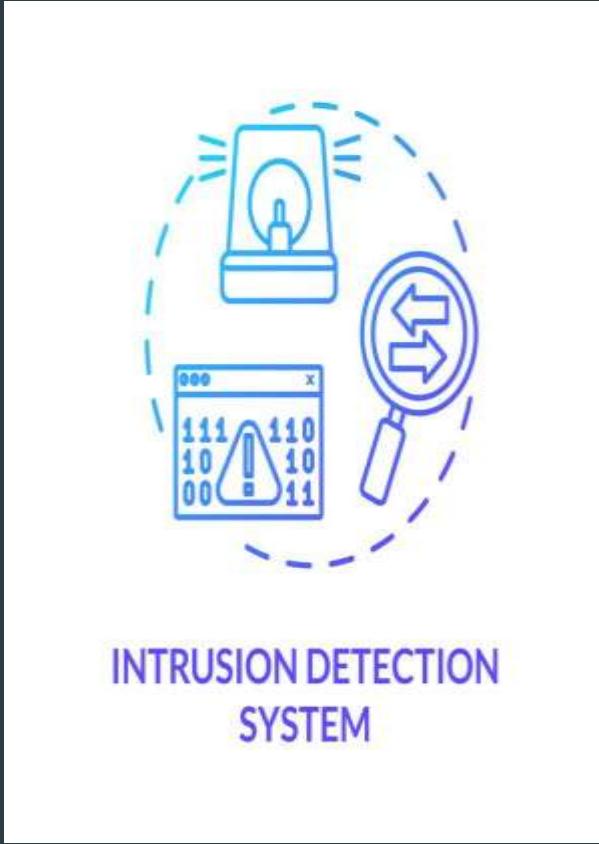
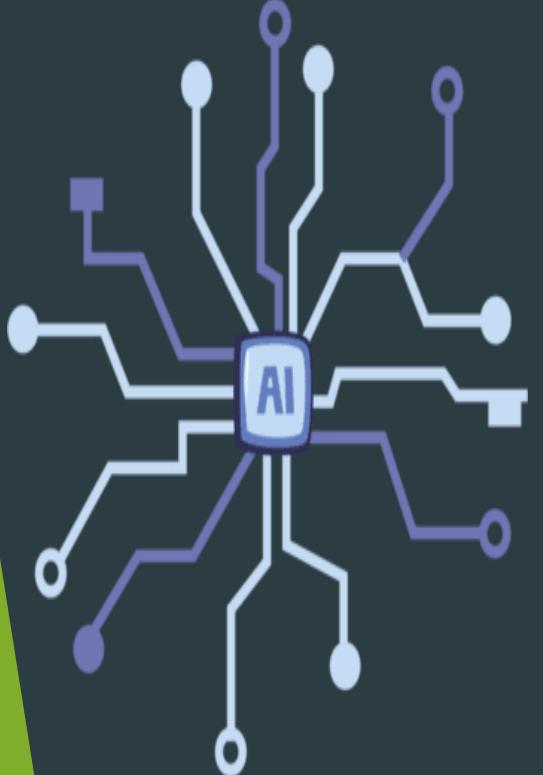
Absence of trust mechanisms between IoT nodes

What is Blockchain?

- ▶ A distributed digital ledger that records transactions across multiple nodes
- ▶ Each block is cryptographically linked, preventing data tampering
- ▶ Provides transparency, traceability, and trust without a central authority
- ▶ Ideal for securing IoT data by ensuring authenticity and integrity



What Is An AI Intrusion Detection System (IDS)?



- ▶ Uses AI to detect anomalies in network traffic
- ▶ Learns normal IoT behavior and flags deviations that may indicate attacks
- ▶ Enables real-time, adaptive threat detection
- ▶ Complements blockchain by adding intelligent, proactive defense

Proposed Solution

- ▶ Goal: Secure IoT data transfer using Blockchain & AI IDS
- ▶ Blockchain Integration:
 - ▶ *Device registration and transaction validation/*
 - ▶ *Immutable record of IoT communication and logging*
- ▶ AI IDS Integration:
 - ▶ *Monitors live traffic for anomalies*
 - ▶ *Detects malicious or unauthorized data flows*
- ▶ Outcome: Verified, and trustworthy IoT communication

Methodology (*IoT Node Development*)



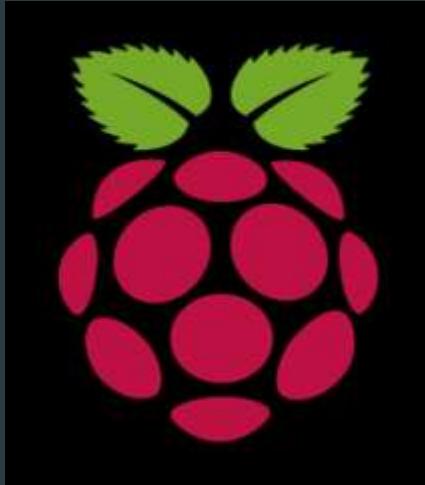
- ▶ Used an STM32L475 Discovery board with onboard modules such as Wi-Fi interface, and RFID sensor
- ▶ Create RFID driver using C
- ▶ Used basic Wi-Fi driver provided from STM32 package
- ▶ Implemented an access control IoT node using STM32CubeIDE for data acquisition, and secure transmission via Wi-Fi
- ▶ Established it as our IoT testbench

Methodology (*Blockchain Development & Integration*)



- ▶ Created a private Ethereum-based blockchain network
- ▶ Blockchain network consists of IoT node, our laptops, a secondary IoT node which is a Raspberry Pi
- ▶ Developed smart contracts to ensure traceability, transparency and immutability
- ▶ Implemented blockchain ledger to create a tamper-proof transaction layer for recording IoT device activity logs
- ▶ Allows for others on the ledger to securely access data and ensures data integrity

Methodology (*AI IDS Development & Integration*)



- ▶ Used Snort as basis for IDS
- ▶ Developed and researched existing AI models for network anomaly detection
- ▶ Created python program for AI-driven anomaly detection
- ▶ Snort and AI model work in tangent to ensure blockchain ledger is secure
- ▶ In the event of anomalies or possible threats being detected
 - ▶ *The logs are sent to the ledger for record and traceability*
- ▶ The AI IDS is deployed on a Raspberry Pi since it is a more resource intensive system

Results

- ▶ IoT data integrity is ultimately increased immensely through the implementation of the blockchain ledger
- ▶ Anomaly detection achieved successful true-positive rate for malicious traffic
- ▶ Slight increase in latency due to some overhead in implementation of ledger
- ▶ A highly scalable framework in which multiple IoT nodes can connect to the blockchain ledger for secure data transfer

Conclusion

- ▶ IoT requires a secure, trustworthy and adaptive data transfer systems
- ▶ Blockchain can ensure IoT data integrity and trust
- ▶ AI IDS serves as a highly beneficial and impactful network monitor
- ▶ This framework creates a secure and defensive IoT communication layer
- ▶ Future Works:
 - ▶ *Scale IoT system*
 - ▶ *Perform deeper system evaluations*
 - ▶ *Optimize edge deployment*

References

- ▶ [1] A. Vinitha, B. Vanitha, and Dr. E. J. T. Fedrik, “Review on vulnerabilities of IOT Security,” International Journal of Trend in Scientific Research and Development, <https://www.ijtsrd.com/computer-science/computer-network/24020/review-on-vulnerabilities-of-iot-security/dr-e-j-thomson-fedrik> (accessed Oct. 7, 2025).
- ▶ [2] L. F. Jumma, L. Sharifi, and P. Rashidi, “A review paper: Blockchain security with IOT devices and deep-learning methods,” Periodicals of Engineering and Natural Sciences, <https://pen.ius.edu.ba/index.php/pen/article/view/1287> (accessed Oct. 7, 2025).
- ▶ [3] Gomez, J., & Santin, M. (2009). Extending Snort with an Anomaly Preprocessor. *Communications in Computer and Information Science*, 48, 662-671. https://doi.org/10.1007/978-3-642-02481-8_75 (accessed Oct. 7, 2025)

Thank You!