ROBUST HARDWARE SECURITY IN IOT NETWORKS USING DEEP LEARNING AND MACHINE LEARNING FOR THREAT DETECTION

Aicha Ouattara & Kerin Quintero

TABLE OF CONTENTS

RESEARCH QUESTION

- How can machine learning enhance hardware security for IoT devices against cyber threats?
- What role does deep learning play in detecting hardware-level anomalies in IoT networks?

- How effective is real-time anomaly detection in preventing hardware-based attacks on IoT devices?
- How does combining hardware security with ML/DL detection improve IoT network resilience?

- What are the most effective ML algorithms for identifying hardware tampering in IoT networks?
- How can anomaly detection models be trained to differentiate between normal and malicious IoT device behavior?

Introduction

IoT Growth:

- The Internet of Things (IoT) is rapidly expanding across fields like healthcare, transportation, and manufacturing, improving efficiency and enabling automation.

Rising Security Risks:

- With this growth, hardware vulnerabilities in IoT devices present serious security risks, making devices susceptible to unauthorized access and data breaches.

Need for Robust Hardware Security:

- Traditional security mainly focuses on software, often leaving hardware exposed to attacks. Stronger hardware protections are essential.

Role of ML and DL:

- Machine Learning (ML) and Deep Learning (DL) enhance IoT security by providing real-time analysis and detecting unusual patterns that indicate potential threats.

Comprehensive Protection:

- Combining ML and DL for hardware and software security ensures a more resilient and secure IoT network against evolving cyber threats.

4o

Problem Statement

Growing Threat to IoT Devices:

- As IoT devices become more integrated into daily life, they increasingly attract cyber attacks targeting their hardware.

Hardware Vulnerabilities:

- Unlike software, hardware is difficult to secure and can be exploited through tampering, side-channel attacks, or by planting malicious components (hardware Trojans).

Limitations of Traditional Security:

- Most security measures focus on software, leaving IoT hardware exposed to threats that can bypass standard protections.

Research Objective:

- This project aims to address these hardware security gaps by using Machine Learning (ML) and Deep Learning (DL) to detect threats in real time.

Goal:

- Develop a system that can quickly identify abnormal hardware behavior and prevent attacks, ensuring the integrity and security of IoT networks.

Purpose of Research

GOAL

Develop methods to detect and prevent hardware-based security threats in IoT networks using machine learning (ML) and deep learning (DL).

Focus on Hardware Security

Addressing the often-overlooked vulnerabilities in IoT hardware that traditional software-focused security misses.

Strengthening IoT Network Reliability

By improving hardware security, this research aims to make IoT networks more resilient to cyberattacks, ensuring safer data handling and device functionality.

THE IMPACT AND ROLE OF DEEP LEARNING & MACHINE LEARNING

Real-Time Threat Detection

ML and DL analyze large data streams to detect unusual patterns that indicate security threats in real time.

Predictive Capabilities

These technologies can identify potential risks before they escalate, allowing proactive responses to hardware vulnerabilities.

Enhanced IoT Security

ML and DL strengthen IoT hardware security by continuously adapting to new attack methods, improving overall network resilience.

Case Study- SILEX Malware Attack (2019)

Overview:

- The SILEX malware targeted IoT devices with weak or default passwords, such as security cameras and smart home systems.
- It spread quickly, disabling over 4,000 devices in a single day by deleting files and network settings, making them unusable.

Attack Method:

- Exploited open or unsecured ports in device hardware

Lessons Learned:

- Importance of strong, unique passwords and regular firmware updates.
- Critical to close unused access points (e.g., debugging ports) to prevent unauthorized access.

Significance:

- Highlights the need for robust hardware security in IoT networks.
- Demonstrates the potential impact of poor security on device functionality and data protection.

Federated Learning for Decentralized Security

Local Threat Detection:

- Federated learning lets each IoT device learn and detect threats on its own, making security specific to each device's hardware and needs.

Improved Privacy and Security:

- By keeping data on the device, federated learning reduces risks from data sharing, boosting hardware security.

Stronger IoT Networks:

- Useful for settings like smart homes and factories, where local, ML-driven monitoring helps keep hardware safe from new types of attacks.

Apple T2 Security Chip for Robust IoT Hardware Security

Dedicated Hardware Security:

- Manages secure boot, encryption, and isolates critical functions for enhanced hardware protection.

ML and Deep Learning for Threat Detection:

- Uses machine learning and deep learning to monitor device activity, detecting unusual patterns like unauthorized firmware changes in real time.

Stronger IoT Defense:

- Combines hardware security with ML and DL-based detection to safeguard IoT devices from tampering, unauthorized access, and other threats.

Microsoft Azure Sphere For Robust Hardware Security In IoT

Hardware Security:

- Azure Sphere uses a secure microcontroller to manage key security functions, like secure boot and device authentication, protecting the hardware directly.

ML-Based Threat Detection:

- With cloud-based machine learning, Azure Sphere monitors devices for unusual activity, spotting threats in real time.

Stronger IoT Defense:

- By combining hardware protection with ML monitoring, Azure Sphere builds a strong, reliable defense for IoT devices against advanced cyber threats.

Google Titan M Security Chip

Dedicated Hardware Security:

- Titan M chip provides secure boot, encryption management, and firmware protection, isolating critical functions to prevent tampering and unauthorized access.

ML and Deep Learning Detection:

- Integrated ML and DL algorithms monitor device activity, identifying unusual patterns like unauthorized acces

Stronger IoT Defense:

- Titan M’s combination of hardware security with ML/DL detection secures sensitive tasks like payments and app integrity, making it ideal for both consumer and enterprise IoT, enhancing Google’s overall IoT security framework.

ARM TrustZone Technology For IoT

Hardware-Level Isolation:

- ARM TrustZone divides the processor into secure and non-secure regions, isolating critical tasks like cryptographic operations from general processes.

ML and Deep Learning Monitoring:

- Integrates ML/DL to monitor secure and non-secure regions, identifying unauthorized access attempts or unusual activity in real time.

Strengthened IoT Security:

- Widely used in IoT applications like smart homes and industrial systems, TrustZone's lightweight design enhances data integrity and protects sensitive operations.

Robust Defense for IoT Networks:

- By combining hardware isolation with ML/DL detection, ARM TrustZone strengthens device-level security, making IoT networks more resilient against advanced threats.

CONCLUSION

Essential Hardware Security: Protects IoT devices from unauthorized access and data breaches.

Power of ML and DL: Enables real-time threat detection by identifying unusual patterns.

Stronger IoT Defense: Combining hardware security with ML/DL boosts network resilience.

Future Outlook: Advancements in ML/DL will lead to safer, more reliable IoT networks.

Key Takeaway: Prioritizing hardware security is crucial for a secure IoT environment.

Tensorflow-Based Long Short Term Memory for Anomaly Detection in IoT Device Security

Purpose:

- Uses Long Short-Term Memory (LSTM) networks with TensorFlow to monitor IoT device data for unusual patterns that signal security threats.

Deep Learning for Real-Time Detection:

- LSTM networks are effective for analyzing time-series data, learning normal patterns in device behavior and detecting anomalies in real time.

Enhanced IoT Security:

- TensorFlow-based LSTM models provide continuous monitoring, making them ideal for high-stakes IoT settings like industrial and healthcare environments, where early detection of hardware issues is critical.

Robust Defense:

- Combines the power of deep learning with TensorFlow to add a proactive layer of security, improving device reliability and resilience against evolving threats in IoT networks.

References

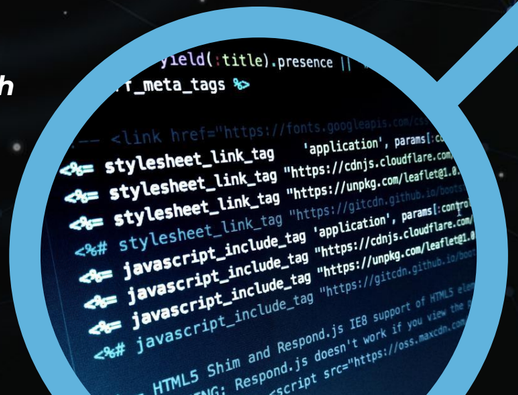
Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies, and open challenges. *Computers & Electrical Engineering, 81*, 106522. doi:10.1016/j.compeleceng.2019.106522

Google, LLC. (2020). Titan M security chip: Enhancing device-level security for IoT. *Google Developers*. Retrieved from https://developers.google.com/

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. doi:10.1109/COMST.20

Cimpanu, C. (2019). SILEX malware is bricking IoT devices, has scary plans. *ZDNet*. Retrieved from https://www.zdnet.com/15.2444095

Mahmud, M. S., Islam, M. A., Rahman, M. M., Chakraborty, D., Kabir, S., Shufian, A., & Sheikh, P. P. (2024). Enhancing industrial control system security: An isolation forest-based anomaly detection model for mitigating cyber threats. *Journal of Engineering Research and Reports*, *26*(3), 161-173.



THANK YOU!