

Research Proposal: An Intelligent Intrusion Detection System for IoT Environments Using Deep Learning

Course Title: Research Methodology in Computer Science

Course Code: A1800

Student Name: Abdulmoien Ayman Al-Ali

Lecturer: Dr. Mohammed Anbar

Abstract

This research aims to address security vulnerabilities in the Internet of Things (IoT) by developing an Intrusion Detection System (IDS) based on deep learning techniques. Due to the computational constraints of IoT devices, traditional security solutions often fail to detect sophisticated attacks. This study proposes utilizing Long Short-Term Memory (LSTM) networks to analyze network traffic and identify anomalies with high precision, thereby enhancing privacy and service continuity.

Chapter 1: Introduction

1.1 Introduction

The Internet of Things (IoT) has become an essential part of daily life. As the number of connected devices grows, so does the risk of cyberattacks. IoT security presents unique challenges that require intelligent and adaptive solutions.

1.2 Background

Current security systems rely heavily on known attack "signatures," making them unable to detect zero-day attacks. Deep Learning (DL) offers an effective way to extract features from raw data without human intervention, making it ideal for dynamic IoT environments.

1.3 Problem Statement (Enhanced)

The primary problem is the inability of existing IDS to balance "accuracy" with "resource consumption." Current studies lack solutions that operate efficiently on resource-constrained devices while maintaining a low False Positive rate. This leads to security breaches that could be catastrophic in systems like Smart Healthcare.

1.4 Research Objectives

1. To analyze the unique characteristics of IoT network traffic and identify its vulnerabilities.
2. To develop an IDS model based on the Long Short-Term Memory (LSTM) algorithm.
3. To evaluate the model's performance using Accuracy and F1-score metrics compared to traditional systems.

1.5 Research Scope

This research is limited to analyzing network-layer attacks (e.g., DDoS, Sinkhole) in smart home IoT networks, focusing on algorithmic aspects rather than hardware implementation.

Chapter 2: Literature Review

The following studies were reviewed to identify the research gap:

1. **Al-Fuqaha et al. (2015)**: Reviewed security challenges across IoT layers and emphasized the importance of decentralized systems.
2. **Thamilarasu & Chawla (2019)**: Applied deep learning to IoT and found that deep models outperform traditional ones in detecting injection attacks.
3. **Roopak et al. (2019)**: Compared CNN and LSTM algorithms, proving LSTM's superiority in handling time-series network data.
4. **Hussain et al. (2020)**: Discussed the use of Machine Learning as a Service (MLaaS) in the cloud to secure IoT devices.
5. **Sarhan et al. (2021)**: Critiqued outdated datasets and advocated for modern data like UNSW-NB15 to enhance model accuracy.
6. **Liu et al. (2022)**: Focused on optimizing energy efficiency in AI algorithms embedded in edge devices.

Chapter 3: Research Methodology

3.1 Methodology

The research follows an experimental approach:

- **Data Collection**: Utilizing the reliable CICIDS2017 dataset.
- **Preprocessing**: Cleaning data and transforming categorical features using One-Hot Encoding.
- **Model Design**: Building a neural network with multiple LSTM layers to learn temporal attack patterns.
- **Testing**: Employing random data splitting to ensure no overfitting occurs.

3.2 Expected Outcomes

The proposed model is expected to achieve a detection accuracy exceeding 96% with a significant reduction in memory and processing overhead, making it suitable for IoT gateways.

3.3 Gantt Chart

Task	Month 1	Month 2	Month 3	Month 4
Literature Review	X			
Methodology Design		X		
Model Implementation			X	
Final Reporting				X

References (IEEE Style)

- [1] A. Al-Fuqaha et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Comm. Surveys & Tutorials*, 2015.
- [2] K. Thamilarasu and S. Chawla, "Towards Deep-Learning-Driven Intrusion Detection for IoT," *Sensors*, 2019.
- [3] M. Roopak et al., "Deep Learning Models for Cyber Security in IoT Networks," *IEEE CCWC*, 2019.
- [4] T. Hussain et al., "Machine Learning for IoT Security: Current Status," *IEEE IoT Journal*, 2020.
- [5] M. Sarhan et al., "An Evaluation of Standardized Network Intrusion Detection Datasets," *arXiv*, 2021.
- [6] X. Liu et al., "Energy-Efficient Deep Learning for IoT: A Survey," *IEEE Access*, 2022.