ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	:	Koo Wai Kit (TP081761)
INTAKE CODE	:	APUMF2406CYS
MODULE TITLE	:	Research Methodology in Computing and Engineering (102024-SIL)
MODULE LECTURER	:	Assoc. Prof. Dr. Shahrinaz binti Ismail
SUPERVISOR NAME	:	Ts. Dr. Vinesha A/P Selvarajah
PROJECT TITLE		Project Proposal: A Framework for Real-Time Detection of Wi-Fi DoS Attacks in IoT Environments
DATE ASSIGNED	:	7 November 2024
DATE COMPLETED	:	28 January 2025

ABSTRACT

The rapid expansion of the Internet of Things (IoT) networks have made the network vulnerable to Wi-Fi Denial-of-Service (DoS) attacks, causing communication disruption, performance degradation and substantial operational and financial losses. Traditional security mechanisms like conventional intrusion detection systems (IDS) are not suitable for IoT ecosystems for their resource-intensive nature, inability to adapt to heterogeneous traffic, and the need for post-event analysis. In this research, a new framework for real-time detection of Wi-Fi DoS attacks in IoT environments is proposed using lightweight machine learning (ML) models and anomaly detection algorithms. The framework is designed to address IoT-specific challenges like limited device resources, dynamic network traffic, and evolving attack patterns. It integrates optimised ML techniques, such as Random Forest, along with simulated IoT attack scenarios using datasets like BoT-IoT and synthetic traffic data. The framework is evaluated in terms of detection speed, accuracy, and resource efficiency using a simulation-based methodology that uses tools like NS-3 and OMNeT++. The goal of the study is to show that lightweight ML-driven approaches can achieve higher accuracy and faster response times while operating within IoT constraints. This framework aims at contributing towards enabling proactive threat mitigation to increase operational continuity, lower financial risks and provide scalable security solutions to IoT manufacturers, developers and consumers. The research advances IoT security paradigms, and provides a foundation for integration with future technologies, such as edge computing and federated learning, to enhance resilience against emerging cyber threats.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DoS	Denial-of-Service
IDS	Intrusion Detection System
IoT	Internet of Things
IT	Information Technology
ML	Machine Learning
RF	Random Forest
RQ	Research Question
Wi-Fi	Wireless Fidelity

CHAPTER 1: INTRODUCTION

The increasing number of devices that connect to the Internet of Things (IoT) networks have made it possible to control technology automatically and effortlessly in many areas, including home automation, health care, factory systems, and vehicle systems (Atzori et al., 2010). These IoT devices mostly use Wi-Fi for network connections, and this makes them vulnerable to malicious attackers who can perform denial-of-service (DoS) attacks against their systems (Gebresilassie et al., 2023). Wi-Fi DoS attacks can stop communication, slow down network speeds, and turn off IoT systems. These issues can lead to significant operational and financial consequences (Altulaihan et al., 2024). The rapid growth of IoT networks requires robust security mechanisms to detect and prevent harmful attacks. However, traditional security measures like conventional intrusion detection system (IDS) struggle to protect IoT networks because they cannot handle the specific problems IoT faces, including weak device processing power, heterogeneity of the network, and constantly changing network traffic (Elrawy et al., 2018; Kaushal et al., 2023).

To address these issues, this research proposal aims to develop a framework for real-time detection of Wi-Fi DoS attacks in IoT environments by leveraging advanced machine learning (ML) techniques and anomaly detection algorithms. The proposed study fills a critical gap in current IoT security tools, which often rely on post-event analysis, by focusing on proactive, real-time detection methods. The project title is: A Framework for Real-Time Detection of Wi-Fi DoS Attacks in IoT Environments. The general subject area of this research is network security, with an emphasis on addressing the unique challenges of real-time threat detection in IoT ecosystems, particularly focusing on Wi-Fi DoS attacks.

This report is structured as follows: The Introduction (Chapter 1) highlights the need for real-time detection of Wi-Fi DoS attacks in vulnerable IoT environments. Next, the literature review in the Research Background (Chapter 2) thoroughly analyzes existing research to show why this research is necessary. The Problem Statement (Chapter 3) shows exactly what challenges and research gaps researchers have found in previous studies that this project needs to fill. Following this, the Research Questions (Chapter 4) specify the key inquiries guiding the investigation. The Aim and Objectives (Chapter 5) section outlines the project’s goals, and the steps required to achieve them. The Research Scope (Chapter 6) defines what areas the study will cover and what tasks it must avoid, for more effective research. Research Significance

(Chapter 7) emphasizes the value and impact of the research findings. Research Methodology (Chapter 8) explains the study methods and methods of collecting and analyzing data. Finally, the Research Plan (Chapter 9) provides a timeline and milestones to guide the project's successful completion.

CHAPTER 2: RESEARCH BACKGROUND

2.1 Problems

There is a growing recognition of the need for real-time security solutions that can detect and respond to real-time threats. For instance, present-day network intrusion prevention systems prioritize real-time detection to protect against cyber threats better (Uhm & Pak, 2022). Research also shows that using historical data alone to find threats is not enough, which makes security teams move towards more proactive methods (Chawla & Thamilarasu, 2018). Traditional security systems struggle to stop DoS attacks in IoT networks because these attacks exploit the weaknesses in IoT devices. Specialized solutions must be designed for these technologies to operate effectively (Elrawy et al., 2018). The challenges faced in real-time detection of Wi-Fi DoS attacks in IoT environments are illustrated in Figure 1.

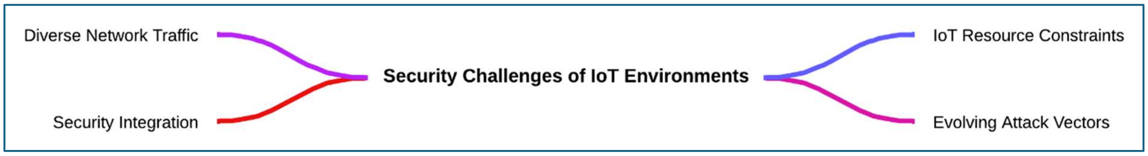


Figure 1: Security challenges in IoT environments

Firstly, diverse network traffic is a significant challenge. The way IoT networks change constantly and support many different devices makes it hard to spot DoS attack patterns. The many different ways devices communicate with each other and the large number of devices make it hard to keep everything secure (Hameed et al., 2019). Adding different security needs for each IoT device makes it hard to build a single security system that can spot threats right away (Khanum & Shivakumar, 2019). According to Kumar and Singh (2024), the wide range of IoT devices calls for ML tools that can adjust to changing traffic patterns and spot threats correctly while keeping false alarms to a minimum.

Secondly, resource constraint of IoT devices results in several security limitations. Common IoT devices function with low computer power, limited memory, and low battery, which makes it hard to run standard real-time security checks. This makes it hard to run advanced security programs designed to find threats instantly. Traditional security measures like regular IDS systems cannot handle the specific challenges of IoT security due to their resource-intensive nature (Altulaihan et al., 2024; Benkhelifa et al., 2018). In addition, the techniques used to keep older IT systems safe can cause delays, which defeats the purpose of real-time reaction needed to stop a DoS attack (Abdulla et al., 2021).

Thirdly, the integration of security solutions for IoT devices is a complicated process. Combining different security tools into one cohesive solution is a major challenge. Most IoT systems use multiple security measures at once: IDS, encryption tools, and methods that separate different parts of the hardware (Hwang & Kim, 2021). Combining different security solutions can lead to problems with how they work together, making it hard to spot DoS attacks in real time. Moreover, various IoT devices struggle to work together because they use different security methods, making it challenging for security systems to protect them (Singh et al., 2023).

Lastly, as cybercriminals keep learning new ways to break into IoT networks, their threats are getting more advanced. The emergence of IoT botnets shows how attackers can use them to cause huge, uncontrollable attacks that strain network capacity and crash services (Dietz et al., 2018). When attackers change how they attack, security systems need to be updated to stay ahead of these new threats. Finding new ways to defend against these attacks requires continuous technological improvement achieved through scientific research and development of advanced tools (Hwang & Kim, 2021).

2.2 Approaches

Recent studies highlight the urgency of developing robust, lightweight, and efficient detection mechanisms made for IoT systems. Modern systems use ML and anomaly detection to find and stop attacks as they happen by looking at network traffic patterns and spotting unusual activity (Pakmehr et al., 2024). Existing studies have already looked at different ways ML can help find DoS attacks in IoT networks. For instance, Alahmadi et al. (2023) did a comprehensive study of ML-based DDoS detection tools, naming multiple ML models that work well and showing where researchers should focus next.

To tackle these challenges, supervised learning has been proven effective. Supervised learning algorithms such as Random Forest (RF), Decision Trees (DT), and Support Vector Machines (SVM) show high success in detecting and labelling suspicious network traffic (Altulaihan et al., 2024). Alsulaiman and Al-Ahmadi (2021) tested several ML methods for detecting DoS attacks in wireless sensor networks, and found that the RF algorithm worked best, with 99.72% accuracy. Moreover, Hulayyil (2023) emphasizes how ML models can find security weaknesses by analysing packet data in IoT ecosystems.

CHAPTER 3: PROBLEM STATEMENT

IoT networks that use Wi-Fi to connect have become easier targets for attackers who can disrupt communications, slow down networks, and cause financial losses through Wi-Fi DoS attacks. Current IoT security tools struggle to stop Wi-Fi DoS attacks in real time because they cannot handle the specific problems IoT networks create, including limited resources, mixed network traffic, and dynamic IoT systems (Elrawy et al., 2018; Kaushal et al., 2023).

Traditional IDS and post-event analysis tools do not work well for IoT networks because they require too many resources, cannot handle different traffic patterns, and cannot detect attacks as they happen (Altulaihan et al., 2024; Benkhelifa et al., 2018). Current ML and anomaly detection methods have shown promise in detecting DoS attacks, but they need to be improved to work better in real-time and across many IoT devices. The lack of lightweight, flexible, and scalable security systems is a major problem that researchers have yet to solve (Bandaru et al. 2024; Wardana et al., 2024).

3.1 Justification

As more IoT devices get used, the IoT network becomes harder to secure, which means more modern techniques are needed to ensure immediate protection. This study is necessary for several reasons, which are described in Table 1.

Table 1: Justifications for this research

Problem	**Explanation**
Resource Constraints	Because IoT devices have limited processing power, memory, and battery life, it is hard to add standard security features. These devices need basic security solutions that quickly find threats, using only a small amount of their available computing power and energy (Agbedanu et al., 2022).
Heterogeneous Traffic	Since different IoT devices use various communication protocols, monitoring and keeping them safe becomes laborious and hard to manage (Altulaihan et al., 2024).
Real-Time Detection	Existing security tools like IDS, mostly rely on post-event analysis, which may cause delayed reactions (Rani et al., 2024).
Integration Challenges	Bringing together different security tools into one working system is a major challenge, primarily because IoT devices and applications are highly diverse. As a result, there is no universal solution for implementing security measures across these devices (Kim, 2024).

CHAPTER 4: RESEARCH QUESTIONS

The research questions in this study cover what needs to be done to develop a system that can find and stop Wi-Fi DoS attacks in real-time for IoT networks. The research questions (RQs) are as follows:

- **RQ1**: What makes Wi-Fi DoS attacks in IoT settings different from regular network attacks?
- **RQ2**: What ML and anomaly detection techniques work best for real-time Wi-Fi DoS attack detection on IoT devices with limited resources?

- **RQ3**: What are the challenges and opportunities in integrating real-time detection frameworks into existing IoT security architectures?

4.1 Hypotheses

The study hypothesizes that a framework leveraging lightweight ML techniques and anomaly detection algorithms will improve the real-time detection of Wi-Fi DoS attacks in IoT environments. Specifically, the hypotheses (Hs) are:

- **H1**: Lightweight ML models, combined with anomaly detection techniques, will achieve higher accuracy and lower false-positive rates in detecting Wi-Fi DoS attacks compared to traditional IDS methods in IoT environments.
- **H2**: The proposed framework will be adaptable to various IoT environments and capable of detecting new Wi-Fi DoS attack patterns.

CHAPTER 5: AIM & OBJECTIVES

5.1 Aim

This main purpose of this research is to design and implement a lightweight, adaptive framework that leverages advanced ML models and anomaly detection techniques to proactively detect and prevent Wi-Fi DoS attacks in IoT environments. Specifically, this framework will address the distinct challenges presented by IoT ecosystems including limited computational resources, heterogeneous network traffic and dynamically changing attack patterns, while maintaining minimal latency and seamless integration with existing IoT systems. The framework seeks to bridge the gap between theoretical ML advancements and practical IoT security needs to increase the resilience of IoT networks to Wi-Fi DoS threats and mitigate the financial risks of cyber disruptions to operational continuity.

5.2 Objectives

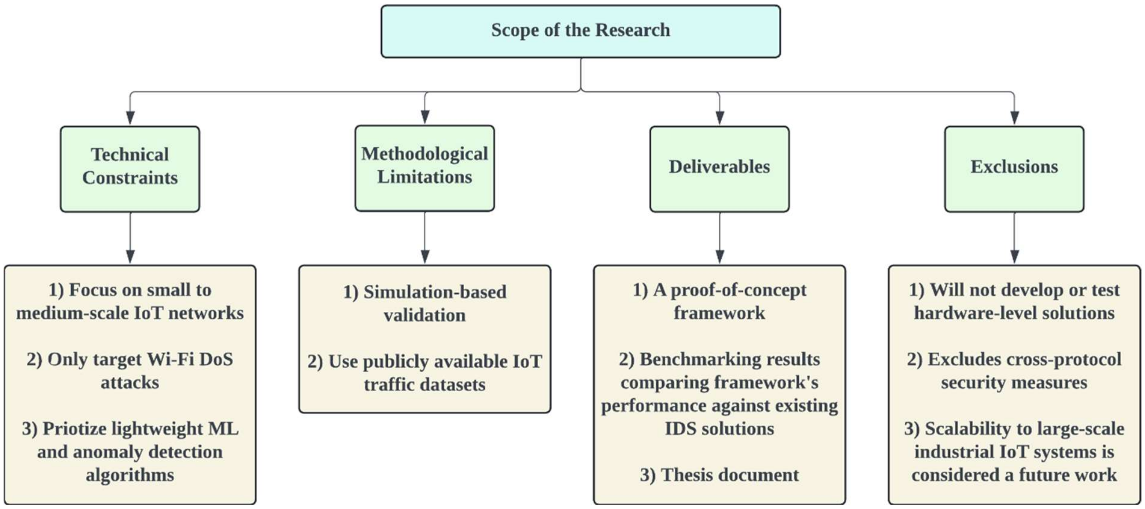
To accomplish the aim, the research objectives (ROs) will be the following:

- **RO1**: To analyse the unique vulnerabilities and attack vectors of Wi-Fi DoS attacks in IoT environments and compare them with traditional network attacks.

- **RO2**: To evaluate ML models and anomaly detection techniques for real-time detection of Wi-Fi DoS attacks that are compatible with resource-constrained IoT devices.
- **RO3**: To design and integrate a single coherent framework that consists of optimized ML models, anomaly detection and IoT specific security protocols to mitigate real-time threat.
- **RO4**: To test the adaptability and scalability of the proposed framework across various IoT ecosystems to demonstrate its effectiveness against changing Wi-Fi DoS attack patterns.
- **RO5**: To benchmark the framework's performance against existing IDS in terms of detection speed, accuracy, and resource efficiency.

CHAPTER 6: SCOPE OF THE RESEARCH

Due to the time constraints (12 weeks) and the focus on feasibility for a master's level project, this research will concentrate on a narrowly defined, simulation based approach to creating a real-time detection framework for Wi Fi DoS attacks in IoT environments. An overview of the scope is illustrated in Figure 2.



Scope of the Research
Technical Constraints
Methodological Limitations
Deliverables
Exclusions
1) Focus on small to medium-scale IoT networks
2) Only target Wi-Fi DoS attacks
3) Priotize lightweight ML and anomaly detection algorithms
1) Simulation-based validation
2) Use publicly available IoT traffic datasets
1) A proof-of-concept framework
2) Benchmarking results comparing framework's performance against existing IDS solutions
3) Thesis document
1) Will not develop or test hardware-level solutions
2) Excludes cross-protocol security measures
3) Scalability to large-scale industrial IoT systems is considered a future work

Figure 2: Overview of research scope

6.1 Technical Constraints

To ensure feasibility, the framework will concentrate on small to medium-scale IoT networks, like smart home systems or industrial sensor networks, rather than large-scale enterprise environments. To maintain depth and specificity, the framework will only target Wi-Fi DoS attacks, excluding other attack vectors such as distributed DoS (DDoS) or malware. Additionally, to suit the limitations of average IoT device resources, lightweight ML models will be prioritized over computationally intensive deep learning architectures.

6.2 Methodological Limitations

This study recognises the inherent limitations of its scope and timeline. Physical deployments of IoT devices would exceed the project's time and resource boundaries, which is why the framework's validation will be based on simulated IoT environments using tools like OMNeT++ and NS-3 (Rashid et al., 2022). Moreover, the research will employ publicly available datasets like CTU-13 and BoT-IoT, combined with synthetic attack data for testing, instead of collecting primary data from real world IoT networks (Wang et al., 2023).

6.3 Deliverables

This research's primary deliverables include a proof of concept framework for real-time Wi-Fi DoS attack detection in IoT environments. To accompany this framework, benchmarking results will be provided, demonstrating the performance of this framework relative to other current IDS in terms of detection speed, accuracy, and resource efficiency. Furthermore, the thesis document itself is also a comprehensive deliverable, synthesising the research methodology, findings, and the framework design into a scholarly contribution to the IoT security literature.

6.4 Exclusions

The research excludes several areas to maintain focus and feasibility. Hardware-level implementations like custom IoT device firmware are out-of-scope, as the study focuses on software-based solutions. The framework also excludes cross-protocol security measures, which involve other communication protocols like Zigbee and non-Wi-Fi attack vectors, concentrating only on Wi-Fi specific DoS threats (Dash & Peng, 2022). In addition, as the project targets small to medium-scale IoT networks, large-scale industrial IoT deployments and enterprise grade security integration are considered future work.

CHAPTER 7: SIGNIFICANCE OF THE RESEARCH

The rise of IoT devices has led to the growth of IoT networks in the sectors like healthcare, smart homes, and industrial automation, which in turn has increased the need to protect these networks from evolving cyber threats. The importance of this research is substantial for the advancement of IoT security by addressing the unique vulnerabilities of Wi-Fi DoS attacks with a novel, real-time detection framework. The project's contributions are supported by recent literature and are targeted to multiple stakeholders including IoT product manufacturers, IoT developers, and IoT consumers (Abdul-Ghani & Konstantas, 2019).

7.1 Address IoT-Specific Security Challenges

Traditional intrusion detection systems (IDSs) are poorly suited to IoT ecosystems as they are resource intensive and cannot adapt to the dynamic, heterogeneous traffic patterns in IoT ecosystems (Elrawy et al., 2018; Kaushal et al., 2023). This framework aims to directly tackle the computational and energy constraints of IoT devices while achieving high detection accuracy by leveraging lightweight ML models and anomaly detection algorithms (Altulaihan et al., 2024). For instance, ML models like Random Forest (RF) achieve more than 99% accuracy in identifying DoS attacks (Alsulaiman & Al-Ahmadi, 2021). This advancement closes a major gap in IoT security with tailored solutions for where standard solutions do not work.

7.2 Improve Real-Time Threat Detection

Most current security tools operate on post event analysis which, inevitably, leads to delayed responses that extend operational disruptions (Rani et al., 2024). This framework, however, focuses more on proactive detection, which is in line with the increasing need for real-time threat mitigation in IoT networks (Uhm & Pak, 2022). The system can identify attack pattern instantly by using supervised learning models like RF and SVM to minimise network downtime and financial losses (Alahmadi et al., 2023). Sectors such as healthcare benefits from this shift of reactive to proactive security, since a delay in response to DoS attacks could put patient safety at risk.

7.3 Economic and Operational Impact

As IoT-dependent operations can be crippled by Wi-Fi DoS attacks, there are serious financial repercussions (Altulaihan et al., 2024). For example, DoS attacks on industrial IoT systems can lead to production halts, repair costs and reputational damage (Dietz et al., 2018). The framework mitigates these risks through real-time detection, which ensures operational continuity while providing industries with a cost-effective means of preventing revenue loss. Furthermore, the reduced false positive rates of ML-driven detection reduce the number of alerts, thus providing a smoother security management (Hulayyil, 2023).

7.4 Foundational Contributions to Future Research

This study serves as a basis for further exploring more advanced techniques like federated learning or edge computing to further improve IoT security (Bandaru et al., 2024). By using publicly available datasets and simulation tools, this research is a reproducible foundation for future studies and this can foster collaboration in the cybersecurity community. In addition, the open design of the framework allows integration with emerging technologies such as 5G, and with AI-driven threat intelligence, making it a foundation for the next generation of security innovation.

7.5 Stakeholder Benefits

Through the proposed framework, several benefits can be brought to the IoT ecosystem, allowing stakeholders to solve security challenges and improve efficiency. The key stakeholders and the benefits this framework offers to each are as follows:

- **IoT Product Manufacturers**: Able to integrate the lightweight framework into devices without costly hardware upgrades, ensuring secure, market-ready products that meet growing consumer demand for robust IoT security.
- **IoT Developers**: Pre-optimised ML models and anomaly detection tools help IoT developers deploy secure applications without custom coding to various protocols, thereby increasing deployment speed.

- **IoT Consumers**: Real-time attack detection prevents attacks in smart homes, healthcare devices, or industrial systems, providing greater privacy and reliability.

CHAPTER 8: RESEARCH METHODOLOGY

To evaluate the effectiveness of the existing ML models and anomaly detection techniques for real-time Wi-Fi DoS attack detection in IoT environments, this research adopts a quantitative, simulation-based experimental approach. Rather than building new models and algorithms, the study analyses pre-trained and publicly available lightweight ML algorithms and anomaly detection algorithms to see if they can be used in IoT-constrained environments. The focus is on comparative analysis, benchmarking these models against classical IDS for IoT networks. This method enables controlled testing of real-time threat detection in IoT environments and is aligned with the evaluation of system performance in different scenarios without the complexities of real-world deployment.

8.1 Data Sources and Collection

In this study, the primary data used include network traffic data and IoT device specifications. The network traffic data used in this work will be drawn from publicly available datasets such as BoT-IoT and CIC-IDS2017, which provide labelled examples of normal and attack traffic (Wang et al., 2023). Synthetic attack traffic will be generated using tools like GNS3 and Aircrack-ng to simulate Wi-Fi specific DoS attack traffic, which provides a diverse range of attack vectors for comprehensive testing (Korolkov et al., 2021; Manickam et al., 2022). In addition, the framework will be designed based on IoT device profiles, such as CPU, memory and power specifications of common devices like Raspberry Pi and ESP32 (Javed et al., 2024). This is to ensure it can work with resource-constrained hardware.

8.2 Resources Required

The project utilizes software tools such as Python with TensorFlow Lite and Scikit-Learn for ML evaluation, NS-3 and OMNeT++ for network simulation, and Wireshark for traffic analysis (Novaes et al., 2021; Rashid et al., 2022). ML models that are pre-trained will be sourced from open repositories such as Kaggle. All the tools and resources used in this project are free.

Moreover, running simulations will not require specialised IoT hardware, so standard computing systems will suffice.

8.3 Methodology Phases

The methodology follows a structured workflow, consisting of six sequential phases. A flowchart in Figure 3 illustrates the methodology process.

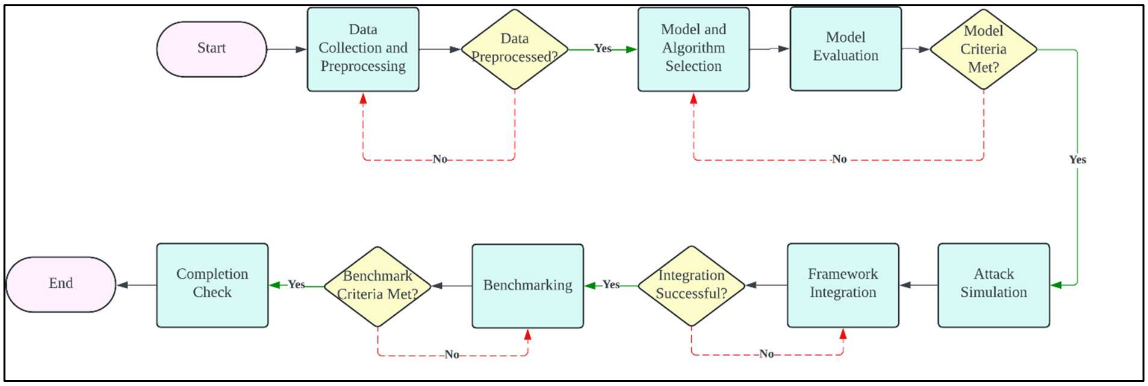


Figure 3: Research methodology phases

The methodology is divided into the following phases:

i. **Phase 1 (Data Collection and Preprocessing)**: A selection of public IoT traffic datasets is filtered and normalized into traffic features like packet rate and signal strength. Custom-generated Wi-Fi DoS attack data, along with simulated network traffic, are created using tools and integrated into the processed datasets to reflect real-world IoT attack scenarios.

ii. **Phase 2 (Model and Algorithm Selection)**: Suitable lightweight ML models and anomaly detection algorithms suitable for IoT environments are identified and selected for evaluation and testing.

iii. **Phase 3 (Model Evaluation)**: The selected models and algorithms are evaluated based on their performance using the datasets, with metrics like accuracy and precision to assess their ability to classify normal and malicious traffic (Singh & Ranga, 2018).

iv. **Phase 4 (Attack Simulation)**: Network simulation tools are used to simulate real-time Wi-Fi DoS attack scenarios in dynamic, simulated IoT environments to evaluate how well the models detect and react to malicious live traffic.

v. **Phase 5 (Framework Integration)**: A unified framework for real-time IoT threat detection will be developed, based on the most effective ML models and anomaly detection algorithms for detecting Wi-Fi DoS attacks.

vi. **Phase 6 (Benchmarking)** : The integrated framework will be benchmarked against existing IDS solutions in terms of detection speed, accuracy and resource efficiency of detecting Wi-Fi DoS attacks in simulated IoT environments.

8.4 Rationale for Methodology

In this work, a simulation-based approach is chosen due to its capability to control the variables and perform reproducible tests, as the base for evaluating Wi-Fi DoS attack detection in IoT environments. The methodology supports each research objective (RO) as follows:

- **RO1**: Through controlled simulations, unique IoT vulnerabilities and attack vectors can be analysed in comparison to traditional network attacks using synthetic and real-world datasets.
- **RO2**: For real-time detection of Wi-Fi DoS attacks, lightweight ML models and anomaly detection techniques are evaluated to ensure they are compatible with resource-constrained IoT devices.
- **RO3**: A real-time threat detection framework is tested in simulated environments, incorporating optimised models and IoT specific security protocols.
- **RO4**: The framework is assessed on its scalability and adaptability to different IoT ecosystems and different attack patterns using network simulation tools.
- **RO5**: The framework is benchmarked in terms of real-time detection performance against existing IDS solutions based on detection speed, accuracy and resource efficiency.

8.5 Ethical and Safety Considerations

Security, privacy, responsible tool usage, and algorithmic bias are the main ethical considerations in this study. Synthetic attack data generation is strictly based on simulated environments to avoid unintended network disruptions, while publicly available datasets only consist of anonymized and insensitive information. The purpose of these measures is to protect privacy, preserve the integrity of the real-world networks, and reduce ethical risks arising from biassed models or misuse of sensitive data.

Additionally, the research does not attempt real-world penetration testing or unauthorised network access, as this is in opposition to ethical hacking guidelines. Reproducibility without malicious replications is ensured through documentation of simulation parameters and attack patterns, so that transparency in methodology is provided. There are no risks associated with consent or privacy breach since there are no human subjects involved. The study, however, acknowledges that there is a dual-use potential to attack simulation tools, and as a mitigation, the framework's design details will not include granular technical specifications of exploit generation.

The study further addresses potential algorithmic bias by considering a wide variety of attack scenarios and cross validating the models with balanced datasets. With this approach, models are less likely to be biassed towards particular traffic patterns or attack types, and the detection performance is more fair and generalizable.

8.6 Potential Limitations and Mitigations

The main limitations of the study are due to its simulation-based approach and reliance on synthetic data. Real world IoT network complexities, including hardware specific vulnerabilities and unpredictable interference, may not be fully simulated in a simulated environment. To increase external validity, the framework is tested across multiple simulation tools and traffic profiles.

Moreover, public datasets may not contain representation of the new Wi-Fi DoS attack vectors emerging. One way to mitigate this is by augmenting datasets with custom-generated attack traffic reflecting recent threat patterns. In addition, the exclusion of other Wi-Fi based attacks and non-Wi-Fi protocols limits the scope of the framework, but this focus enables depth in addressing specific Wi-Fi DoS vulnerabilities with recommendations for future expansion.

Standard IoT devices like Raspberry Pi provide a basis for resource efficiency metrics, which are cross validated with other hardware to reduce bias even if not all edge cases are covered. Finally, physical deployments are absent for insights into long-term operational stability, but this modular framework design enables seamless integration into real systems in future work.

CHAPTER 9: RESEARCH PLAN

Table 2 below presents the research timeline with a 12 week schedule. This timeline lists what activities should be completed in each phase of the project, and what deliverables to track progress and ensure that each stage is completed successfully.

Table 2: Research timeline

Week	Tasks	Deliverables/Milestones
1-2	**Literature Review and Initial Setup** **a)** Refine literature review (focus on IoT security gaps, ML techniques, and DoS detection). **b)** Finalize research design and simulation tools setup.	**a)** Preliminary annotated bibliography. **b)** Refined research objectives and scope. **c)** Simulation environment (NS-3/OMNeT++) configured.
3-4	**Phase 1: Data Collection & Preprocessing** **a)** Collect and preprocess datasets. **b)** Generate synthetic Wi-Fi DoS attack data.	**a)** Cleaned, labeled datasets. **b)** Feature-engineered traffic data (e.g., packet rate, signal strength).
5	**Phase 2: Model & Algorithm Selection** **a)** Identify suitable ML models and anomaly detection algorithms. **b)** Mid-project review.	**a)** Shortlist of models and algorithms. **b)** Progress report.
6-7	**Phase 3: Model Evaluation** **a)** Train/test models on pre-processed datasets. **b)** Analyse performance metrics.	**a)** Model evaluation report.
8-9	**Phase 4: Attack Simulation** **a)** Simulate real-time Wi-Fi DoS attacks in IoT environments. **b)** Test model detection capabilities under dynamic traffic.	**a)** Simulation logs/results. **b)** Documented detection accuracy and response times.
10	**Phase 5: Framework Integration** **a)** Develop unified framework integrating	**a)** List of models and algorithms chosen for integration.

	chosen ML models and anomaly detection algorithms.	**b)** Functional prototype framework. **c)** Code repository with modular components.
11	**Phase 6: Benchmarking** **a)** Compare framework performance against traditional IDS.	**a)** Benchmarking report.
12	**Finalisation** **a)** Proofread, format, and submit thesis. **b)** Final presentation.	**a)** Completed thesis. **b)** Final presentation slides.

9.1 Contingency Plan

The contingency plan is to avoid risks that can delay the project. Additional datasets or simplified preprocessing techniques will be used if delays occur in data collection and preprocessing (Weeks 3-4) to compensate for lost time. When evaluating models (Weeks 6-7), if the models are not performing as expected, other models or adjustments to hyperparameters will be considered to improve results. If there are problems with attack simulation tools (Weeks 8-9), backup tools and pre-test configurations will be used to minimise disruption.

During the integration of framework (Week 10), if the integration process takes too long, key functions will be prioritized first, and the advanced features will be considered later. Preliminary performance metrics will be collected earlier for benchmarking (Week 11) to allow for adjustment if needed.

CHAPTER 10: SUMMARY

This research proposal addresses the critical problem of detecting real-time Wi-Fi DoS attacks in IoT infrastructure. Such attacks are particularly hazardous to IoT networks, where resource-constrained devices and heterogeneous traffic patterns combine to make these networks uniquely susceptible to such attacks, which can disrupt operations, compromise safety, and cause financial losses. The resource-intensive nature and post-event analysis associated with traditional security solutions, such as conventional IDS, cannot meet the demands of IoT.

To bridge this gap, the proposed framework proposes to utilise lightweight ML and anomaly detection algorithms specially designed for the IoT ecosystems. The study attempts to address limitations with existing tools by concentrating on real-time detection, which is adaptable to dynamic network conditions and compatible with low-power devices. Then, by using datasets like BoT-IoT, CIC-IDS2017, and synthetic attack data, the methodology applies a simulation-based approach in order to evaluate ML models like RF. The framework will be tested using network simulation tools such as NS-3 and OMNeT++, to evaluate its effectiveness in detecting live Wi-Fi DoS attacks.

This research has important implications for IoT security as it provides a proactive, scalable solution that strikes an acceptable trade-off between accuracy and resource efficiency. Stakeholders like IoT manufacturers and developers will benefit from improved threat mitigation, operational continuity and lower financial risks. Although the study is confined to simulated environments and Wi-Fi specific DoS attacks, the modular design offers a starting point for future expansion to real world deployments and integration with emerging technologies. This work advances real-time detection capabilities toward the larger goal of securing IoT networks against evolving cyber threats.

REFERENCES

Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: an iot perspective. *Journal of Sensor and Actuator Networks*, *8*(2), 22. https://doi.org/10.3390/jsan8020022

Abdulla, L. S., Mahmood, M. K., Salih, A. F., & Karim, S. M. (2021). Analysis and evaluation of symmetrical key ciphers for internet of things smart home. *Indonesian Journal of Electrical Engineering and Computer Science, 22*(2), 1191. https://doi.org/10.11591/ijeecs.v22.i2.pp1191-1198

Agbedanu, P. R., Musabe, R., Rwigema, J., Gatare, I., Maginga, T. J., & Amenyedzi, D. K. (2022). Towards achieving lightweight intrusion detection systems in internet of things, the role of incremental machine learning: a systematic literature review. *F1000Research, 11*, 1377. https://doi.org/10.12688/f1000research.127732.1

Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., Alotaibi, O. B., & Bajandouh, S. A. (2023). Ddos attack detection in iot-based networks using machine learning models: a survey and research directions. *Electronics*, *12*(14), 3103. https://doi.org/10.3390/electronics12143103

Alsulaiman, L., & Al-Ahmadi, S. (2021). Performance evaluation of machine learning techniques for dos detection in wireless sensor network. arXiv *preprint* arXiv:*2104.01963*.

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection ids for detecting dos attacks in iot networks based on machine learning algorithms. *Sensors*, *24*(2), 713. https://doi.org/10.3390/s24020713

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: a survey. *Computer networks, 54*(15), 2787-2805.

Bandaru, V. N. R., Kaligotla, V. G. S., Varma, U. D. S. P., Prasadaraju, K., & Sugumaran, S.

(2024, July). A enhancing data security solutions for smart energy systems in iot-enabled cloud computing environments through lightweight cryptographic techniques. In *IOP Conference Series: Earth and Environmental Science* (Vol. 1375, No. 1, p. 012003). IOP Publishing.

Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A critical review of practices and challenges in intrusion detection systems for iot: toward universal and resilient systems. *IEEE Communications Surveys & Tutorials, 20*(4), 3496-3509. https://doi.org/10.1109/comst.2018.2844742

Chawla, S., & Thamilarasu, G. (2018, April). Security as a service: real-time intrusion detection in internet of things. In *Proceedings of the Fifth Cybersecurity Symposium* (pp. 1-4).

Dash, B. K. and Peng, J. (2022). Zigbee wireless sensor networks: performance study in an apartment-based indoor environment. *Journal of Computer Networks and Communications, 2022*, 1-14. https://doi.org/10.1155/2022/2144702

Elrawy, M., Awad, A., & Hamed, H. (2018). Intrusion detection systems for iot-based smart environments: a survey. *Journal of Cloud Computing Advances Systems and Applications, 7*(1). https://doi.org/10.1186/s13677-018-0123-6

Gebresilassie, S. K., Rafferty, J., Chen, L., Cui, Z., & Abu-Tair, M. (2023). Transfer and cnn-based de-authentication (disassociation) dos attack detection in iot wi-fi networks. *Electronics*, *12*(17), 3731. https://doi.org/10.3390/electronics12173731

Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in internet of things (iot): a review. *Journal of Computer Networks and Communications, 2019*, 1-14. https://doi.org/10.1155/2019/9629381

Hwang, S. and Kim, J. (2021). A malware distribution simulator for the verification of network threat prevention tools. *Sensors, 21*(21), 6983. https://doi.org/10.3390/s21216983

Javed, A., Ehtsham, A., Jawad, M., Awais, M. N., Qureshi, A., & Larijani, H. (2024). Implementation of lightweight machine learning-based intrusion detection system on iot devices of smart homes. *Future Internet, 16*(6), 200. https://doi.org/10.3390/fi16060200

Kaushal, N., Singh, G., & Singh, J. (2023). An addressing techniques for maintaining security and privacy framework for internet of things. *2023 3rd International Conference on Intelligent Technologies (CONIT)*, 1-7.

Khanum, A. and Shivakumar, R. (2019). An enhanced security alert system for smart home using iot. *Indonesian Journal of Electrical Engineering and Computer Science, 13*(1), 27. https://doi.org/10.11591/ijeecs.v13.i1.pp27-34

Kim, T. (2024). A study on impact of lightweight cryptographic systems on internet of things-based applications. *Asia-Pacific Journal of Convergent Research Interchange, 10*(1), 49-59. https://doi.org/10.47116/apjcri.2024.01.05

Korolkov, R., Kutsak, S., & Voskoboinyk, V. (2021). Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection. *Bulletin of VN Karazin Kharkiv National University, series «Mathematical modeling. Information technology. Automated control systems», 5*0, 59-71.

Kumar, S. and Singh, D. (2024). A review of securing internet of things (iot) with machine learning. *International Journal of Innovative Research in Computer Science and Technology (IJIRCST)*. https://doi.org/10.55524/csistw.2024.12.1.2

Manickam, S., AIghuraibawi, A. H. B., Abdullah, R., Alyasseri, Z. A. A., Abdulkareem, K. H., Mohammed, M. A., … & Al-Ani, A. (2022). Labelled dataset on distributed denial-of-service (ddos) attacks based on internet control message protocol version 6 (icmpv6). *Wireless Communications and Mobile Computing, 2022*, 1-13. https://doi.org/10.1155/2022/8060333

Novaes, M. P., Carvalho, L. F., Lloret, J., & Proença, M. L. (2021). Adversarial deep learning approach detection and defense against ddos attacks in sdn environments. *Future Generation Computer Systems, 125*, 156-167. https://doi.org/10.1016/j.future.2021.06.047

Pakmehr, A., Aßmuth, A., Taheri, N., & Ghaffari, A. (2024). Ddos attack detection techniques in iot networks: a survey. *Cluster Computing, 27*(10), 14637-14668.

Rani, K. S., Parasa, G., Hemanand, D., Devika, S., Balambigai, S., Hussan, M. T., … & Jain, A. (2024). Implementation of a multi-stage intrusion detection systems framework for strengthening security on the internet of things. *MATEC Web of Conferences, 392*, 01106. https://doi.org/10.1051/matecconf/202439201106

Rashid, B., Sharif, K. H., & Shreef, T. (2022). A survey of simulation tools for modelling internet of thing. *Passer Journal of Basic and Applied Sciences, 4*(1), 37-44. https://doi.org/10.24271/psr.2022.313553.1105

Singh, R. P. and Ranga, V. (2018). Performance evaluation of machine learning classifiers on internet of things security dataset. *International Journal of Control and Automation, 11*(5), 11-24. https://doi.org/10.14257/ijca.2018.11.5.02

Singh, S., Singh, D. P., Chandra, K., & Singh, B. (2023). IoT security challenges and emerging solutions: a comprehensive review. *International Journal of Scientific Research in Engineering and Management, 07*(09). https://doi.org/10.55041/ijsrem25662

Uhm, Y., & Pak, W. (2022). Real-time network intrusion prevention system using incremental feature generation. *CMC-Comput. Mater. Contin, 70*, 1631-1648.

Wang, M., Zhang, B., Zang, X., Wang, K., & Ma, X. (2023). Malicious traffic classification via edge intelligence in iiot. *Mathematics*, *11*(18), 3951. https://doi.org/10.3390/math11183951

Wardana, A. A., Kołaczek, G., & Sukarno, P. (2024). Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. *Applied Sciences, 14*(10), 4109. https://doi.org/10.3390/app14104109