

Research Proposal

Title: Anomaly Detection Using Deep Learning for Securing 802.1X Authentication and Network Access Control

By Mohammed Baatiyyah - 261002493

Master of AI - 2026

Table of Contents

Abstract	2
Introduction	3
Background	3
Problem Statement	5
Research Objectives	6
Research scope	7
Literature review	8
Research Methodology	9
Ethical Considerations.....	10
Limitations	10
Expected Outcomes	11
Gantt chart	12
References	13

1. Abstract

Modern enterprise network security relies on IEEE 802.1X and Network Access Control (NAC) to manage authorized access. However, these frameworks are increasingly vulnerable to sophisticated threats that bypass initial authentication. Traditional NAC solutions remain largely reactive and rule-based, failing to detect post authentication malicious activities. Furthermore, the prevalence of end-to-end encryption has rendered Deep Packet Inspection (DPI) obsolete. This research proposes a proactive anomaly detection framework by integrating Deep Learning (DL) architectures specifically Autoencoders and Self-Supervised Learning (SSL) into the 802.1X ecosystem.

The proposed system learns the behavioral of the network by analyzing flow-level (e.g., packet lengths and inter-arrival times), shifting the focus from payload inspection to behavioral analysis. This approach enables the detection of Zero-day attacks, identity spoofing, and lateral movement within encrypted environments. The methodology follows a four-phase approach: a systematic literature review, Qualitative Research, Quantitative Research and Framework Development and Validation. Finally, the framework is validated for real-time detection with minimal latency. Expected outcomes include detection accuracy exceeding 95% and a significant reduction in false positives, providing a scalable, AI-driven defense mechanism adapting to modern network complexities.

2. Introduction

In today's digital world, network security is the foundation of every organization. As more devices like laptops, smartphones, and IoT sensors connect to the network, managing them safely becomes a big challenge. For many years, the 802.1X protocol has been the main standard for authenticating these devices. When combined with Network Access Control (NAC), it works like a security guard to ensure that only authorized users and healthy devices can access the network.

However, cyber threats are changing very fast. Traditional 802.1X and NAC systems mostly depend on static rules and known signatures. While this worked in the past, it is not enough to stop modern attacks like Zero-day exploits or lateral movement inside the network. Also, a major problem has appeared: Encryption. Today, most network traffic is encrypted. This protects privacy, but it also creates "blind spots" where attackers can hide because traditional security tools cannot see inside the encrypted data.

To fix these gaps, we need to move from reactive security to proactive and intelligent defense. This is where AI becomes very important. Unlike old methods, Deep Learning models such as Autoencoders and Self-Supervised Learning can learn the "normal behavior" of a network by analyzing statistical data like packet lengths and arrival times, these models can find small changes that indicate an attack, even if the traffic is encrypted.

The main goal of this research is to connect traditional network authentication with Artificial Intelligence by adding Deep Learning to the 802.1X and NAC framework, we want to create a system that is smart and adaptive. This study will show how unsupervised and self-supervised learning can detect complex threats in real-time data. Ultimately, we aim to provide a strong, AI-driven solution that protects the network against the next generation of cyber threats.

3. Background

To understand how Deep Learning can secure a network, we must first look at the current state of network access technologies and the rise of advanced artificial intelligence in cybersecurity.

- The Evolution of 802.1X and NAC

The 802.1X standard was originally created to provide "Port-based Network Access Control." Its job was simple: when a device connects to a switch or a wireless access point, it must provide credentials (like a username/password or a certificate) before the port opens.

Over the years, this evolved into Network Access Control (NAC) solutions, which not only check "who" is connecting but also "what" is connecting (the health of the device, its OS version, and its antivirus status).

While these systems are excellent for basic security, they are mostly "static." They work based on pre-defined policies created by network administrators. If an attacker manages to steal a valid certificate or uses a trusted device to perform a "low and slow" attack, traditional NAC systems often fail to see the threat because the device is technically "authorized."

- Deep Learning in Cybersecurity

Deep Learning (DL) is a more advanced branch of Machine Learning inspired by the human brain's neural networks. In recent years, DL has changed how we fight cyber threats. Unlike older methods that require humans to manually tell the computer what to look for, Deep Learning models can automatically discover complex patterns in massive datasets.

In the context of network security, DL is particularly powerful for Anomaly Detection. An "anomaly" is any behavior that is different from the normal pattern. For example, if a VOIP phone—which normally only sends small voice packets—suddenly starts transferring gigabytes of data to an external server, a DL model will immediately flag this as an anomaly.

- The Challenge of Encrypted Traffic

One of the biggest changes in modern networking is that almost all communication is now encrypted (using TLS/SSL). While this protects privacy, it makes it impossible for traditional security tools to perform "Deep Packet Inspection" (DPI) to see what is inside the traffic.

Deep Learning solves this by focusing on Traffic Metadata—which includes things like the size of packets, the time between them (Inter-arrival time), and the total duration of the flow. By learning the "shape" of normal encrypted traffic, DL models can detect hidden attacks inside encrypted tunnels without ever needing to decrypt the data. This makes it a perfect partner for enhancing 802.1X environments.

4. Problem Statement:

Traditional network security systems, such as rule-based intrusion detection systems and basic network access control methods, are facing many challenges in detecting modern cyber threats and anomaly detection. As the number of connected devices, and encrypted network traffic continues to grow, these traditional methods often have difficulty identifying unusual network activity and unauthorized access effectively.

Because of these limitations, traditional systems also have difficulty detecting unusual network activity and unauthorized access. To address this issue, many researchers have studied the use of machine learning techniques for network anomaly detection. For example, Tyagi and Kumar (2020) investigated supervised machine learning algorithms to detect malicious network traffic. Their study showed that models such as Decision Trees and Random Forest can successfully identify attack patterns when trained with labeled datasets. However, their method depends heavily on the availability of high-quality labeled data, which is often limited in real-world network environments.

Similarly, Abdallah et al. (2021) studied different machine learning models used in intrusion detection systems. Their results showed that ensemble methods can improve detection accuracy. However, the study also pointed out some challenges, such as scalability and the difficulty of detecting new or unknown attacks in dynamic network environments.

Wang et al. (2022) studied different machine learning methods used for network anomaly detection. Their analysis showed that machine learning can improve the accuracy of detecting network attacks. However, they also explained that these models may require high computational resources and may have difficulty adapting to rapidly changing network traffic patterns.

For unsupervised machine learning, Carrera et al. (2021) proposed an unsupervised anomaly detection method that can detect abnormal network traffic without using labeled data. This approach can adapt better to dynamic network environments. However, it may produce more false positive results compared to supervised learning methods.

More recently, Ness et al. (2025) studied advanced machine learning techniques for detecting anomalies in network traffic. Their research showed that modern ML models can detect suspicious patterns even in encrypted network traffic. However, their study mainly focused on traffic analysis and did not address how anomaly detection can be integrated with network authentication systems.

In addition, Sattar et al. (2024) proposed a self-supervised learning method to detect anomalies in encrypted network traffic. Their approach improves detection accuracy and

reduces the need for labeled data. However, the study does not focus on integrating this method with network access control systems.

Most existing studies mainly focus on network traffic analysis and intrusion detection. Only a limited number of studies have explored combining machine learning based anomaly detection with network access control systems such as 802.1X. For this reason, there is a need for smarter security solutions that integrate ML and DL anomaly detection with authentication and access control mechanisms to improve the real-time detection of suspicious devices and unauthorized network activity in enterprise networks.

5. Research Objectives

The main goal of this research is to build a smart and automated system that can detect security threats in 802.1X environments. To achieve this, the following objectives have been defined:

- **To evaluate** the performance of different Deep Learning architectures, such as Autoencoders and Recurrent Neural Networks, in detecting complex anomalies within 802.1X authenticated traffic.
- **To develop** a robust framework that uses Deep Learning to identify malicious patterns and unauthorized access attempts that traditional NAC systems often miss.
- **To Analyze** flow-level statistical metadata (such as packet length and inter-arrival times) to identify malicious patterns within encrypted network traffic.
- **To optimize** these Deep Learning models for near real-time detection, ensuring they can handle high-speed network traffic without causing delays (latency) in the 802.1X process.
- **To Validate** the framework's capability for near real-time detection to ensure minimal latency and maintain network performance in enterprise environments.

Overall, the literature demonstrates a clear evolution from traditional and supervised approaches toward unsupervised and self-supervised learning techniques. Among these, self-supervised learning particularly contrastive learning provides a balanced solution by addressing data scarcity, privacy preservation, and detection of unknown threats. However, there is still a need for a unified, scalable, and efficient framework capable of achieving high accuracy with low false positive rates in encrypted traffic environments.

6. Research Scope

The scope of this research is specifically designed to address the integration of Deep Learning within enterprise network security. This study includes:

- **Network Environment:** This research focuses on Local Area Networks (LANs) implementing the 802.1X protocol for both wired and wireless access. It targets the interaction between the Supplicant, the Authenticator (Switch/Access Point), and the Authentication Server (RADIUS/TACACS) during and after the access process.
- **Technology Focus:** The study prioritizes Deep Learning (DL) architectures, specifically Autoencoders (AE), Self-Supervised Learning (SSL), and Long Short-Term Memory (LSTM) networks. Traditional machine learning methods will be used only as a baseline for performance comparison.
- **Data Patterns:** The research focuses on Flow-level statistical features (e.g., packet size, inter-arrival time, and flow duration). This approach ensures the framework remains effective in encrypted environments without requiring payload decryption.
- **Anomaly Types:** The study targets anomalies occurring after successful authentication, such as identity spoofing, lateral movement, IOS changes and unauthorized access attempts that bypass traditional NAC rules.
- **Datasets:** To validate the models, the research will utilize recognized cybersecurity datasets, including CIC-UNSW-NB15 and CSE-CIC-IDS2018, along with specialized encrypted traffic data like CIC-IDS2017 and ISCX VPN.
- **Exclusions:** This research excludes physical hardware security and administrative user account management. It is strictly limited to the automated detection of behavioral anomalies at the network access layer.

7. Literature Review

The application of Artificial Intelligence to enhance network security has been a major research focus in recent years. As traditional rule-based systems struggle to keep up with modern threats, researchers are exploring more adaptive solutions. This section reviews the key findings from recent studies regarding supervised, unsupervised, and deep learning in network security.

The initial wave of AI integration focused largely on supervised machine learning paradigms. Researchers like Tyagi and Kumar (2021) demonstrated the early potential of this approach, proving that models such as Support Vector Machines (SVM) and Decision Trees could achieve remarkable accuracy when identifying known attack patterns, particularly within the constrained environments of IoT networks. This success was further refined by Abdallah et al. (2022), who developed a comprehensive taxonomy of supervised algorithms. Their work illustrated that ensemble methods, such as Random Forest and XGBoost, significantly outperformed single model architectures when tested against modern benchmark datasets like UNSW-NB15 and CICIDS2017. Yet, despite these impressive performance metrics, a critical flaw remained inherent in supervised learning: the dependency on labeled "ground truth" data. This dependency creates a significant bottleneck in real-world deployments where "Zero-day" attacks threats never seen before by the model can bypass security layers unnoticed.

Recognizing the "Zero-day" vulnerability, the academic discourse transitioned toward unsupervised learning to achieve proactive rather than reactive defense. Carrera et al. (2022) spearheaded explorations into near real-time anomaly detection, suggesting that by baselining "normal" network behavior, models could identify suspicious deviations without any prior knowledge of specific attack signatures. This approach offered a new layer of adaptability for dynamic environments. However, unsupervised models introduced their own set of challenges, most notably the "Class Imbalance" problem. In a typical enterprise network, malicious traffic is a needle in a haystack of legitimate data. To address this, Ness et al. (2025) introduced advanced techniques using Isolation Forests and LightGBM, which successfully minimized false positive rates even when the dataset was overwhelmingly skewed toward normal traffic. This advancement was crucial for maintaining business continuity, ensuring that security measures did not inadvertently block legitimate users.

As the industry moved toward universal encryption with protocols like TLS 1.3, a new technical crisis emerged: the "blind spot" created by encrypted traffic. Traditional Deep Packet Inspection (DPI) became largely obsolete, as security tools could no longer peer into the payload of network packets. This forced a radical shift toward analyzing metadata and behavioral flows. A landmark study by Sattar et al. (2025) introduced the ET-SSL framework,

which leveraged Self-Supervised Learning (SSL) to analyze flow-level features such as packet length and inter-arrival times. Their findings were transformative, showing that Deep Learning models—specifically 1D-CNNs and LSTMs—could achieve over 96.8% detection accuracy with a processing latency as low as 15ms. This proved that intelligence could be maintained in high-speed networks without the privacy and performance costs of decrypting data.

Despite these significant strides in traffic analysis and threat detection, a profound structural gap persists in current literature. While AI has become highly proficient at identifying anomalies in isolated traffic flows, there is a distinct lack of research focusing on the native integration of these intelligent layers with network authentication systems like IEEE 802.1X. Most existing frameworks treat anomaly detection as a secondary monitoring tool rather than an active component of the Access Control layer. Currently, 802.1X provides a binary entry point a device is authenticated or it is not but it lacks the continuous, intelligence-driven oversight required to detect a "trusted" device that becomes compromised post authentication. It is at this critical intersection of real-time behavioral AI and 802.1X Network Access Control that the present research finds its purpose, aiming to bridge the gap between static authentication and dynamic, AI driven security orchestration.

8. Research Methodology

This research follows a structured, many phase methodology to develop an intelligent anomaly detection system. The approach combines theoretical study, data analysis, and framework development.

Phase 1: Literature Review

In this initial phase, a comprehensive review of existing academic papers, industry standards (802.1X), and current NAC technologies will be conducted. The focus is to identify the limitations of traditional security methods and explore the latest advancements in Deep Learning. This phase helps in selecting the most suitable neural network architectures such as Autoencoders and LSTMs that can effectively handle high-speed and encrypted network traffic.

Phase 2: Qualitative Research

This phase involves gathering expert insights and technical requirements to understand the real-world challenges of network access control.

- **Expert Consultation:** As a Network Expert, internal technical requirements and common attack patterns seen in enterprise environments will be analyzed.

- **System Requirements:** Identifying the critical performance needs, such as the maximum allowable latency (delay) for 802.1X authentication, to ensure the AI model does not interrupt the user experience.
- **Feature Selection:** Determining which "behavioral" features (like packet size and timing) are most important for detecting threats without looking at the encrypted content.

Phase 3: Quantitative Research

This is the technical core of the research, where data-driven experiments are conducted.

- **Data Collection:** Utilizing recognized datasets like UNSW-NB15 and CIC-IDS2017 which contain thousands of network traffic records.
- **Model Training:** Implementing Deep Learning models using Python. We will train the models to recognize "Normal" traffic patterns and "Malicious" anomalies.
- **Statistical Analysis:** Measuring the performance of the models using numerical metrics such as Accuracy, Detection Rate, and False Positive Rate. This phase provides the evidence needed to prove the model's effectiveness.

Phase 4: Framework Development and Validation

In the final phase, the findings from the previous steps are combined to build the final security framework: Framework Design, Validation and Result Verification

9. Ethical Considerations

Throughout the research, ethical considerations are paramount. This includes obtaining informed consent from participants, ensuring confidentiality and anonymity, and minimizing any potential harm.

10. Limitations

This research methodology acknowledges potential limitations, including the representativeness of the sample in qualitative research and the response bias in survey data. Efforts will be made to mitigate these limitations through careful sampling and data triangulation.

11. Expected Outcomes

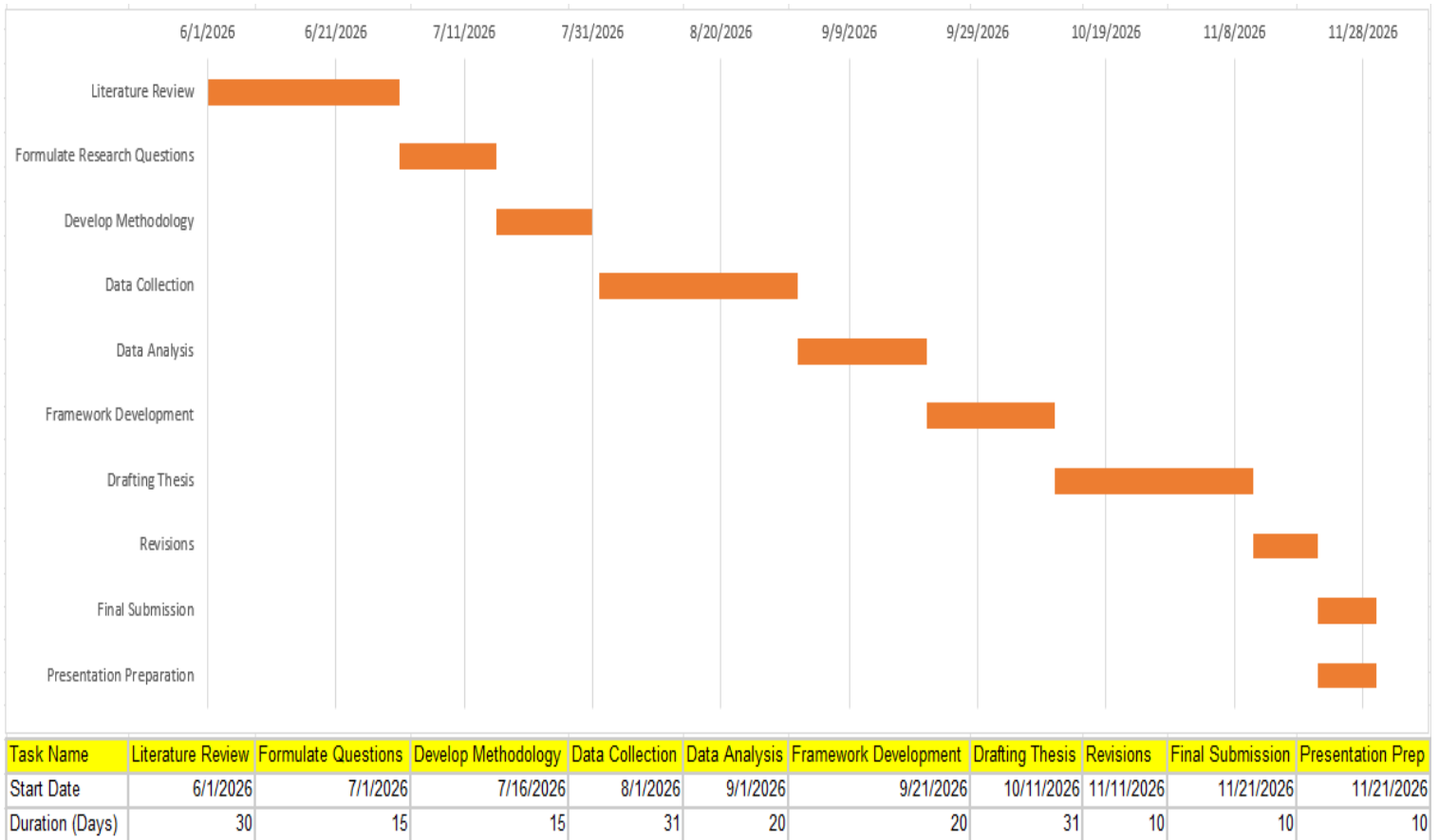
Comprehensive Analysis of Anomalous Traffic in Encrypted Environments: A detailed examination of the current challenges in identifying malicious patterns within 802.1X authenticated networks. This analysis is expected to highlight the limitations of traditional inspection methods when dealing with modern encryption standards and the behavioral complexity of diverse network devices.

Evaluation of ML and DL Efficacy for NAC: An assessment of various machine learning and deep learning methodologies ranging from supervised to self-supervised models—aimed at enhancing network security. This evaluation is anticipated to uncover gaps in how existing algorithms handle class imbalance and real-time processing requirements at the network access layer.

Development of an Integrated AI Framework: The formulation of an innovative framework that seamlessly integrates AI-driven anomaly detection with 802.1X authentication workflows. This framework is expected to provide a dynamic security model that moves beyond "permit/deny" access, offering continuous post authentication monitoring based on real-time behavioral insights.

Optimization of Detection Accuracy for Encrypted Flows: The derivation of a specialized feature-extraction methodology that focuses on flow-level metadata (such as packet length and inter-arrival times). This outcome aims to achieve high detection accuracy and minimal latency, proving that robust security can be maintained in high-speed enterprise networks without the need for data decryption.

Gantt chart



12. References:

- Tyagi, H., & Kumar, R. (2020). Attack and anomaly detection in IoT networks using supervised machine learning approaches. *Revue d'Intelligence Artificielle*. [Link](#)
- Abdallah, E. E., Eleisah, W., & Ootom, A. F. (2022). Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. *Procedia Computer Science*. [Link](#)
- Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Gomez Chavez, K., & Rubinstein, B. (2021). Machine learning in network anomaly detection: A survey. *IEEE Access*. [Link](#)
- Carrera, F., Dentamaro, V., Galantucci, S., Iannacone, A., Impedovo, D., & Pirlo, G. (2022). Combining unsupervised approaches for near real-time network traffic anomaly detection. *Applied Sciences*. [Link](#)
- Ness, S., Eswarakrishnan, V., Sridharan, H., Shinde, V., Janapareddy, N. V. P., & Dhanawat, V. (2025). Anomaly detection in network traffic using advanced machine learning techniques. *IEEE Access*. [Link](#)
- Sattar, S., Khan, S., Khan, M. I., Akhmediyarova, A., Mamyrbayev, O., Kassymova, D., Oralbekova, D., & Alimkulova, J. (2025). Anomaly detection in encrypted network traffic using self-supervised learning. *Scientific Reports*. [Link](#)