OPTIMISED HYBRID SECURITY MODEL FOR EDUCATIONAL NETWORKS

Saydullo Uzoqov
first-year Master's student,
Department of Computer Science, Sharda University Uzbekistan
https://doi.org/10.5281/zenodo.19363834

Abstract: Educational institutions increasingly rely on network technologies to support learning, communication, and research activities. However, the growing use of internet services also increases the risk of cyber threats such as malware, phishing attacks, unauthorized access, and distributed denial-of-service (DDoS) attacks. Traditional security mechanisms often fail to detect complex and evolving cyber threats.

This study proposes an Optimised Hybrid Security Model for Educational Networks that integrates multiple security technologies including firewall systems, intrusion detection systems (IDS), intrusion prevention systems (IPS), and machine learning-based detection models. The hybrid model aims to improve the detection and prevention of cyber threats in educational network environments. The proposed model provides a layered security architecture that enhances the overall network protection while maintaining efficient network performance.

Keywords: Network Security, Hybrid Model, Educational Networks, Machine Learning, Intrusion Detection.

In modern educational environments, computer networks play a crucial role in supporting academic activities such as online learning, research collaboration, digital libraries, and communication between students and teachers. Universities and educational institutions rely heavily on internet connectivity to deliver educational services.

However, the increasing dependence on network infrastructure exposes educational institutions to numerous cybersecurity threats. Educational networks are particularly vulnerable because they often allow a large number of users to access the network using various devices such as laptops, smartphones, and tablets.

These open and dynamic environments make educational networks attractive targets for cyber attackers. As a result, there is a strong need for advanced security mechanisms capable of detecting and preventing different types of cyber threats.

This research focuses on designing an Optimised Hybrid Security Model for Educational Networks. The proposed model integrates traditional security mechanisms with modern machine learning techniques to improve network security.

Educational institutions face several security challenges due to their open network environments.

1. Large Number of Users:Educational networks serve thousands of students, teachers, and staff members. Managing network access for such a large number of users increases the complexity of network security.
2. Open Network Access: Many universities provide open or semi-open Wi-Fi access for students. While this improves accessibility, it also increases the risk of unauthorized access.
3. Use of Personal Devices:Students often connect their personal devices to the institutional network. These devices may contain malware or vulnerabilities that can compromise network security.

4. Cyber Attacks:Educational institutions frequently experience cyber attacks such as: Malware infections

Phishing attacks

Distributed Denial of Service (DDoS)

Unauthorized network access

These threats require advanced detection and prevention mechanisms.

A Hybrid Security Model combines multiple security techniques to provide stronger protection against cyber threats.

Traditional security systems such as firewalls and intrusion detection systems are effective in detecting known attacks but may fail against new or sophisticated threats. Machine learning techniques can help detect unusual patterns in network traffic and identify potential attacks.

The hybrid approach combines these technologies to create a more robust security system.

The main components of a hybrid security model include:

Firewall

Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)

Machine Learning based threat detection

Access Control mechanism

The proposed model consists of several layers designed to protect educational networks.

1. Firewall Layer

The firewall serves as the first line of defense by filtering incoming and outgoing network traffic. It blocks unauthorized access and prevents malicious traffic from entering the network.

2. Intrusion Detection and Prevention Layer

Intrusion Detection Systems monitor network traffic and detect suspicious activities. Intrusion Prevention Systems can automatically block detected threats.

3. Machine Learning Detection Layer

Machine learning algorithms analyze network traffic patterns to detect anomalies and potential cyber attacks. Hybrid machine learning models such as CNN-GRU or LSTM-SVM can improve the accuracy of threat detection.

4. Access Control Layer

Access control mechanisms ensure that only authorized users can access the network. Authentication and authorization techniques help maintain network integrity.

The architecture of the proposed hybrid security model includes multiple layers of protection.

The network traffic flows through the following components:

User Device → Network Switch → Firewall → IDS/IPS → Machine Learning Detection → Server

Each layer performs a specific function to analyze and filter network traffic. Suspicious activities detected at any stage can trigger security alerts or automatic blocking mechanisms.

The proposed hybrid security model provides several advantages for educational networks.

First, it enhances network protection by combining traditional and modern security techniques.

Second, the integration of machine learning algorithms improves the detection of unknown and evolving cyber threats.

Third, the layered architecture ensures that multiple security mechanisms work together to protect the network.

Finally, the model is scalable and can be adapted to different sizes of educational institutions.

The proposed model can be implemented using various security tools and technologies.

Network Security Tools:

Kerio Control

pfSense

Cisco Firewall

Intrusion Detection Tools:

Snort IDS

Suricata

Machine Learning Tools:

Python

TensorFlow

Scikit-learn

These tools can be integrated to build a comprehensive network security system

Educational institutions face increasing cybersecurity challenges due to the widespread use of internet technologies. Traditional security mechanisms alone are not sufficient to protect modern educational networks.

This research proposed an Optimised Hybrid Security Model that integrates firewall systems, intrusion detection systems, intrusion prevention systems, and machine learning techniques.

The hybrid model improves the detection and prevention of cyber threats while maintaining efficient network performance. Future research may focus on implementing and testing the proposed model in real educational environments.