SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

AN INTRUSION DETECTION FRAMEWORK FOR SECURING WIRELESS CAMPUS NETWORKS AGAINST CYBER-PHYSICAL THREATS: CASE STUDY OF NICTM, UROMI

Oriakhi, Henry Eronmosele[1], Buhari, Ahmed[2], Ekanem, Ekpo Ekpo[3]
[1,2,3] Department of Computer Science School of Applied Sciences,
National Institute of Construction Technology and Management, Uromi, Edo State, Nigeria.

ABSTRACT
The rapid adoption of wireless networks in educational institutions has enhanced accessibility to digital resources but simultaneously exposed these networks to sophisticated cyber-physical threats. Traditional intrusion detection systems (IDS) are inadequate in addressing the dynamic nature of modern attacks, necessitating the development of advanced frameworks that integrate anomaly detection and machine learning. This paper proposes and implements a modular intrusion detection framework tailored for wireless campus networks, with a case study on the National Institute of Construction Technology and Management (NICTM), Uromi. The framework encompasses data collection, feature extraction, detection, incident management, and visualization modules. It integrates rule-based methods with placeholders for supervised machine learning models, ensuring scalability and adaptability. The architecture leverages PHP, MySQL, and Bootstrap for proof-of-concept deployment, alongside provisions for future integration with advanced algorithms and real-time streaming via WebSockets. The study anticipates enhanced detection accuracy, reduced false positives, and comprehensive monitoring capabilities. The findings from this research contribute both theoretical insights and practical applications, providing a foundation for future intrusion detection systems in academic and institutional environments.
KEYWORDS: *Intrusion Detection System, Wireless Campus Networks, Cyber-Physical Threats, Machine Learning, Anomaly Detection*

INTRODUCTION

The proliferation of wireless networks in educational institutions has enhanced connectivity and access to information. However, it has also led to an increase in vulnerabilities, particularly against cyber-physical attacks that target both the digital and physical aspects of campus infrastructures. This proposal focuses on the development of a robust intrusion detection framework to secure wireless campus networks. The case study will examine the NICTM, Uromi campus network at the ICT unit.

An intrusion detection framework is a system designed to monitor network traffic for suspicious activity and potential threats. It typically comprises a series of algorithms and processes that analyse data packets traversing the network. Advances in machine learning have introduced complex models capable of identifying patterns indicative of malicious behaviour, significantly enhancing detection accuracy and response capabilities (Natkaniec & Bednarz, 2023).

Wireless local area networks (WLANs) are critical in connecting devices across educational campuses. These networks, characterized by their mobility and ease of access, utilize wireless technology to enable communication between students and educational resources. However, the open nature of wireless communication leaves these networks vulnerable to various security threats such as unauthorized access, eavesdropping, and denial-of-service attacks (Ali et al., 2022).

Cyber-physical threats refer to attacks that compromise both digital systems and their physical environments. In the context of campus networks, this could include scenarios where cyber intrusions lead to unauthorized physical access or disruption of vital infrastructure, such as heating systems or safety alarms. Addressing these threats necessitates a coordinated approach that aligns cyber security strategies with physical security measures (Rubio-Hernán et al., 2018).

Machine learning models have emerged as effective tools for detecting network intrusions due to their ability to adapt and learn from incoming data. These systems can analyse extensive datasets to identify anomalies that may signify an intrusion, thus facilitating timely responses to potential threats (Natkaniec & Bednarz, 2023). The application of machine learning in intrusion detection represents a significant advancement over traditional rule-based systems, which struggle to keep up with the dynamic nature of cyber threats.

The security of wireless networks is a multifaceted challenge exacerbated by factors such as signal interference, range limitations, and the ease of interception inherent to radio transmission. Studies suggest that wireless networks are generally more exposed to security breaches than their wired counterparts due to their intrinsic openness and mobility features (Ali et al., 2022). Successful

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

security mechanisms must account for these unique vulnerabilities to protect against attacks that exploit weaknesses in wireless communication channels.

Historically, the effectiveness of intrusion detection systems has relied heavily on the capacity to accurately detect and respond to potential security breaches. Various approaches, including statistical anomaly detection and signature-based detection, have been utilized, but each has its limitations in rapidly evolving environments. The work by Sodhro et al. emphasizes the need for continuous optimization of security strategies to meet the infrastructural demands of educational settings (Sodhro et al., 2019). The integration of advanced signal processing techniques, as discussed by Fragkiadakis and Askoxylakis, reveals critical insights into identifying malicious attempts to breach wireless networks (Fragkiadakis & Askoxylakis, 2013).

This research aims to develop an intrusion detection framework specifically designed to enhance the security of wireless campus networks against cyber-physical threats. The study will undertake a detailed evaluation of existing methodologies, identify gaps in current security practices, and propose a comprehensive solution tailored to the operational context of the National Institute of Construction Technology and Management, Uromi.

This research intends to fill existing gaps in the intrusion detection landscape, specifically tailored for wireless campus networks, with the goal of contributing both theoretical insights and practical applications in the area of cyber-physical threat mitigation.

Problem Statement/Justification

The rapid deployment of wireless network technology in educational institutions, combined with the growing reliance on cyber-physical systems for operational efficiency, has resulted in greater vulnerability to cyber-attacks. These threats have the ability to corrupt sensitive data, disrupt critical services, and jeopardize physical safety on campuses. Wireless campus networks are especially vulnerable because of their intrinsic qualities, such as openness, accessibility, and the mobility of devices connected to the network (Ali et al., 2022).

In light of these vulnerabilities, traditional intrusion detection mechanisms have proven inadequate in effectively identifying and responding to sophisticated cyber-attacks. Notably, the cybersecurity landscape is evolving, requiring that intrusion detection frameworks move beyond static rules and utilize advanced analytics, including those provided by machine learning algorithms, to detect anomalies indicative of potential threats in real-time.

Furthermore, the situation is exacerbated by a lack of specific solutions to the distinct operational challenges that educational institutions encounter. This includes limited resources for implementing complete cybersecurity measures, diverse user behaviours that influence network traffic, and the need for a collaborative strategy that combines educational purposes and security standards. As a result, there is an urgent need for a specialised intrusion detection framework that not only protects wireless networks but also adapts to the evolving landscape of cyber threats affecting campus security systems.

In summary, the overarching problem to be addressed by this research is the lack of intrusion detection paradigms that will offer effective protection against the complex and evolving cyber threats facing wireless campus networks. This research aims to explore and develop a robust framework that can bridge the gap in existing security measures, thereby enhancing the resilience and security posture of educational networks.

AIM AND OBJECTIVES OF THE STUDY

The primary aim of this research is to develop and implement an intrusion detection framework specifically designed to enhance the security of wireless campus networks against cyber-physical threats. This framework will focus on the NICTM Uromi campus as a case study, addressing the unique security challenges faced by educational institutions' wireless infrastructures.

The Objectives are

1. to conduct a comprehensive literature review to analyse existing intrusion detection methodologies, particularly in the context of wireless networks, and identify gaps that the proposed framework can address,
2. **to design** a proposed intrusion detection framework that incorporates advancements in machine learning and cyber-physical security principles,
3. to integrate various key technologies, such as Wireless Local Area Networks (WLANs), software-defined networks, and real-time data analysis capabilities, to create a cohesive intrusion detection system tailored to campus settings,
4. to implement the proposed framework within the wireless network of the NICTM Uromi campus and test its effectiveness against simulated cyber-physical threats,
5. to analyse wireless network logs to gain insights into user behaviour patterns and their correlation with potential threats. This aspect will assist in refining the framework to improve its adaptability and effectiveness in real-time threat detection.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

to provide recommendations based on the findings of the research, addressing how the framework can be adapted and improved for broader implementation in other educational institutions and similar environments, ensuring a resilient defence against cyber-physical threats. This will be done through publications and presentations of findings.

LITERATURE REVIEW

This section reviews existing research related to intrusion detection frameworks, wireless campus networks, and cyber-physical threats, drawing upon various studies in the field to establish the relevance of the proposed research.

1. Intrusion Detection Frameworks

Numerous methodologies have been developed to identify threats to networks; however, traditional approaches often struggle with the adaptive and dynamic nature of cyber threats. Denney and Tewksbury emphasize that a thorough literature review must encompass prevailing themes and methodologies within the relevant area of study, establishing a foundation for future research Denney & Tewksbury (2013). An essential component in developing an effective intrusion detection system is understanding and implementing various learning algorithms, as detailed in reviews of systematic methodologies which inform current intrusion detection systems (Pati & Lorusso, 2017).

2. Wireless Campus Networks

Wireless networks are vital in campus environments, providing connectivity to educational resources. Nevertheless, due to their open nature, they are vulnerable to numerous security threats. Research indicates that these networks frequently rely on outdated security mechanisms that fail to adapt to new forms of cyber threats (Kucan, 2011). Understanding the complexities related to network environments is critical when designing detection frameworks targeted at educational institutions, highlighting the need for customized solutions that account for user behaviour and network architecture unique to campus settings (Sachs, 2018).

3. Cyber-Physical Threats

The relationship between cyber and physical systems in educational settings is increasingly recognized as a crucial area of vulnerability. It is essential that security measures accommodate interactions between both domains to provide a comprehensive defence strategy (Gordon & Stewart, 2013). Furthermore, while Monteiro et al. discuss various barriers in the context of corruption and supply chain management, they do not specifically address the interplay of cyber-physical threats in networks but rather present a broader framework (Monteiro et al., 2018). Cyber-physical attacks pose risks not only to information systems but also to physical infrastructure. Nundy et al. underscore the integration of research perspectives that encompass both digital and physical disciplines to effectively address cyber-physical threats (Nundy et al., 2021).

4. Machine Learning and Anomaly Detection

Machine learning techniques are increasingly employed in intrusion detection frameworks due to their capacity to analyse large datasets and identify anomalies indicative of potential attacks. Current literature emphasizes the effectiveness of these methodologies in creating robust security solutions. For instance, while Kamarudin and Rashid focus on optimizing assembly line balancing, their insights into systematic approaches could be conceptually translated to understanding and enhancing detection capabilities in network security, although direct correlation is tenuous (Kamarudin & Rashid, 2018). The adoption of real-time data analysis within wireless networks fosters a proactive rather than reactive security posture.

5. Empirical Review of Intrusion Detection Frameworks in Network Security

The following table summarizes various works on intrusion detection frameworks, particularly focusing on network security. The selected studies examine different methodologies, including machine learning approaches, anomaly detection techniques, and system architectures relevant to intrusion detection systems (IDS).

Authors	Title	Summary	Key Techniques	Publication Year
Hussain	Use of Firewall and IDS to Detect and Prevent Network Attacks	This paper illustrates the utility of firewalls and IDS in enhancing network security by preventing unauthorized access.	IDS, Firewalls	2018
Kurniabudi et al.	Network Anomaly Detection Research: A Survey	This survey discusses anomaly and misuse detection as part of IDS, presenting various detection strategies and their applications.	Signature-based and Anomaly-based Detection	2019
Molina-Coronado et al.	Survey of Network Intrusion Detection Methods From the Perspective of the	The study investigates various IDS methodologies and their effectiveness in detecting potential cyber attacks.	Knowledge Discovery, Data Mining	2020

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

	Knowledge Discovery in Databases Process			
Rana	Anomaly Detection in Network Traffic using Machine Learning and Deep Learning Techniques	This research analyzes different techniques used for detecting network anomalies, emphasizing machine learning applications.	Machine Learning, Deep Learning	2019
Shone et al.	A Deep Learning Approach to Network Intrusion Detection	The study explores deep learning techniques for enhancing the accuracy and efficiency of network intrusion detection.	Deep Learning	2018
Li et al.	Routing Attacks Detection Method of Wireless Sensor Network	This paper presents a method for detecting routing attacks in wireless sensor networks, utilizing anomaly detection mechanisms.	Anomaly Detection, Particle Swarm Optimization	2018
Xia	Application of Cloud Computing Technology in Computer Network Secure Storage System	Focuses on improving the security of network storage systems using cloud computing solutions to enhance data integrity.	Cloud Computing	2022
Yadhu et al.	Machine Learning Based Intrusion Detection System	The authors discuss various machine learning techniques that can be applied to build effective IDS for network security.	Machine Learning	2023
Imtiaz et al.	Efficient Approach for Anomaly Detection in Internet of Things Traffic Using Deep Learning	This paper discusses methods for detecting anomalies in IoT traffic, emphasizing the role of deep learning in network security.	Anomaly Detection, Deep Learning	2022
Fotiadou et al.	Network Traffic Anomaly Detection via Deep Learning	Proposes novel deep learning methods for detecting anomalies in network traffic logs, focusing on complex threat patterns.	Deep Learning	2021

In summary, the existing literature highlights the need for an adaptive intrusion detection framework specifically designed to address the unique challenges presented by wireless campus networks in the context of cyber-physical threats. Although substantial research has been conducted in each area of intrusion detection systems, wireless security, and cyber-physical threats, a significant gap remains in the literature specifically linking these elements within educational institutions. By synthesizing insights from various disciplines, this research aims to establish a more integrated approach to network security that combines machine learning techniques with innovative security practices addressing both cyber and physical vulnerabilities in campus environments.

This literature review not only highlights the importance of understanding interconnected domains when designing security systems but also emphasizes the necessity of a dedicated study that focuses on the intersection of these areas, particularly in a campus setting. The proposed research aims to address these gaps and enhance the overall security posture of educational institutions.

METHODOLOGY

The methodology outlined below details the systematic approach the researchers intend to follow to develop a robust intrusion detection framework tailored for wireless campus networks, focusing on the integration of machine learning and anomaly detection techniques. This methodology is divided into several key phases:

1. Requirements Analysis

- A comprehensive analysis of the current wireless network infrastructure at NICTM, Uromi will be conducted to establish security requirements and identify existing vulnerabilities.
- Key stakeholders will be, including IT staff and network users, to gather insights into their experiences with network security and potential threats.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

2. Literature Review and Framework Design

- We will perform a thorough literature review of existing intrusion detection frameworks, focusing on works that emphasize on both anomaly detection and machine learning techniques. Notable studies include (Aziz & Bešťák 2024), which discusses utilizing K-means clustering for anomaly prediction, and (Zhang & Liao, 2018), who propose a dynamic link anomaly analysis (DLAA) framework that utilizes network topology for security assessments.
- Based on the insights gained from the literature review, a proposed intrusion detection framework that combines statistical methods, machine learning algorithms, and deep learning approaches to enhance predictive accuracy and adaptability will be designed. This design will include the following components:
  i. **Data Collection Module**: to gather network traffic data using existing network log systems which can be accessed by network admin.
  ii. **Feature Extraction Module**: to apply feature engineering techniques to identify significant metrics influencing network behavior.
  iii. **Detection Module**: Implement machine learning algorithms such as Random Forest, Support Vector Machines (SVM), and deep learning models (e.g., Convolutional Neural Networks) for anomaly detection based on developed features similar to the ones used by (Li, 2024; Imtiaz et al., 2022).

3. Implementation

- The research will utilise a simulation environment to build and validate the designed framework. This may involve using tools such as CloudSim or other network simulation environments to evaluate model performance.
- Integrate various algorithms for anomaly detection as indicated in the literature, such as those proposed by Ramasamy et al. (2004) and Fotiadou et al. (2021), to compare and analyse their effectiveness in a controlled environment.
- Establish a feedback mechanism that allows the model to adapt based on the continuously changing network landscape and user behaviour.

4. Testing and Evaluation

- The framework's detection capabilities will be tested using synthetic as well as real-world datasets to evaluate its performance under various scenarios. Use metrics such as accuracy, recall, precision, and F1-score to assess model performance (Pelati et al., 2022).
- The framework's ability to detect both known and unknown attacks will be analysed, as well as its resilience against false positives and false negatives. This can be achieved through cross-validation techniques and performance benchmarking against existing state-of-the-art frameworks (Jadidi et al., 2020).

5. Optimization and Fine-Tuning

- Based on the evaluation results, the parameters may need to be fine-tuned. This process may involve hyperparameter tuning and the application of ensemble methods to optimize detection capabilities.
- The finally investigate the use of real-time monitoring techniques to ensure that the network remains secured continuously.

6. Deployment and Continuous Monitoring

- Upon successful completion, we will then deploy the finalized intrusion detection framework in the real operations of the NICTM, Uromi campus, integrating it into the existing network security architecture.
- It is importannt to also implement continuous monitoring and an incident response strategy to address real-time security threats and adapt the system as new vulnerabilities emerge, as suggested by the work of (Zhao et al., 2009).

7. Documentation and Reporting

- Document the entire development process, challenges encountered, and lessons learned during implementation.
- Prepare comprehensive reports showcasing the effectiveness of the framework and recommendations for further research and enhancements.
- Present findings through journl publications and seminar presentationns.

This structured methodology ensures a comprehensive approach to developing an effective intrusion detection framework, tailored specifically for addressing the security needs of wireless campus networks while leveraging advanced machine learning techniques.

Proposed System Architecture

The framework follows a layered, modular design including: log collection, feature extraction, detection, incident management, alerting, and visualization modules. Future enhancements include real-time updates via WebSockets and scalability through message queue integration (e.g., Kafka, RabbitMQ). As shown in Figure 1, the conceptual architecture illustrates data flow from log collection to reporting.

1. System Components

The system is organized into the following key modules:

1. **Log Collection Module**
   - Collects raw network logs from routers, firewalls, or simulated traffic.
   - Supports log submission via REST API (logs.php).
   - Normalizes logs into a consistent format for processing.

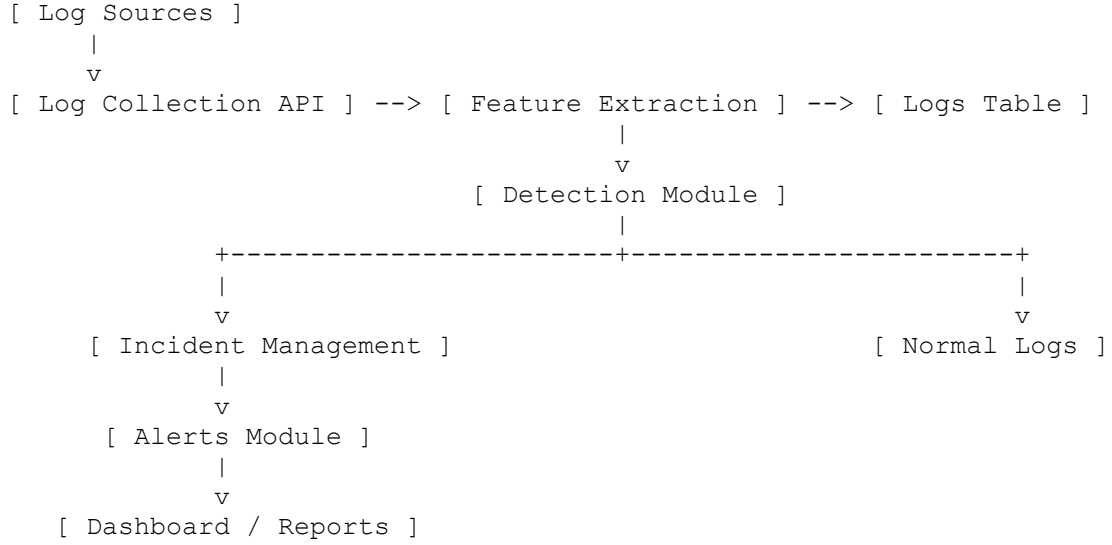
SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

2. **Feature Extraction Module**
   - Parses raw log entries and extracts features (e.g., SRC IP, DST IP, payload size, keywords).
   - Stores both raw and structured log data in the **Logs Table** of the database.
3. **Detection Module**
   - Performs **rule-based detection** (e.g., keyword matching for "DoS", "Malware", "Scan").
   - Assigns severity levels:
     - High = DoS, Flood, Large Payloads
     - Medium = Malware, General Attacks
     - Low = Port Scans, Probes
   - Provides placeholder integration for a **Machine Learning model** (via Python REST API).
4. **Incident Management Module**
   - Creates incidents when suspicious activity is detected.
   - Stores incident metadata: source IP, destination IP, description, severity, status (open/resolved).
   - Links incidents to alerts via foreign keys.
5. **Alerting Module**
   - Generates alerts for each detected incident.
   - Alerts can be sent via email or stored for reporting.
   - Supports escalation based on severity level.
6. **Dashboard & Visualization Module**
   - Provides a **Bootstrap-based web interface**.
   - Displays:
     - Logs (searchable, paginated, filterable)
     - Incidents (color-coded by severity, manageable via resolve/delete actions)
     - Analytics (charts for logs/day, incidents by severity, open vs resolved).
   - Exports reports in **CSV and PDF formats**.

2. Data Flow

1. Logs are submitted via API or generator tools.
2. Logs are stored in the database and features are extracted.
3. Detection module classifies log entries as **Normal** or **Suspicious**.
4. Suspicious entries trigger an **Incident** and **Alert**.
5. Dashboard retrieves logs and incidents for visualization, filtering, and reporting.
6. (Proposed) WebSocket module broadcasts new logs/incidents in real time for instant updates.

3. System Diagram (Conceptual)



4. Proposed Enhancements

- Real-Time Streaming: Replace AJAX polling with WebSockets (Ratchet) for instant log and incident updates.
- Machine Learning Integration: Incorporate supervised ML models for anomaly detection, integrated via Python Flask API.
- Scalability: Extend log ingestion with message queues (e.g., Kafka, RabbitMQ) for high-volume traffic.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

RESULTS (EXPECTED OUTPUT)

The research aimed at developing an intrusion detection framework tailored for wireless campus networks if and when successfully achieved is expected to yield the following results;

1. **Enhanced Detection Accuracy**: The implementation of advanced machine learning algorithms and anomaly detection techniques in the proposed framework is anticipated to improve the accuracy of intrusion detection significantly compared to traditional methods.
2. **Reduced False Positive Rates**: By employing a hybrid approach that integrates multiple detection techniques, the framework expects to reduce false positive rates significantly. This outcome is crucial for maintaining user trust and minimizing unnecessary responses to benign activities, a common issue in traditional IDS.
3. **Real-time Monitoring Capabilities**: The framework is expected to provide real-time analysis and monitoring of campus network traffic, thus enabling immediate detection and response to suspected intrusions. This real-time responsiveness is critical in mitigating potential threats before they escalate.
4. **Scalability and Adaptability**: The research will likely demonstrate that the intrusion detection system can scale with network growth and adapt to evolving threat landscapes. Incorporating dynamic learning mechanisms will allow the system to learn from new data continuously, thereby enhancing its ability to identify previously unknown attack patterns and adapt to the changing wireless network environment.
5. **Comprehensive Security Posture Development**: The outcome of this research is anticipated to furnish a comprehensive security framework that integrates both cyber and physical security measures. This integrated approach reflects emerging trends in cybersecurity, emphasizing the necessity for a unified security strategy that accounts for various attack vectors.
6. **Documentation of Model Performance**: The research will provide quantitative metrics on model performance, including accuracy, detection rate, precision, and recall metrics. Documenting these results will contribute valuable insights to the interplay between different detection techniques and their effectiveness, as outlined by earlier empirical studies in the domain of intrusion detection (Pramila & Gayathri, 2022; Wang et al., 2020).
7. **Provision of a Practical Case Study**: The development of the framework within the NICTM, Uromi campus provides a valuable case study from which other educational institutions can draw insights. It is expected that best practices and lessons learned will be outlined for use in similar environments, thereby contributing to broader discussions and endeavors in network security.
8. **Future Research Directions**: The findings from this research may uncover new avenues for future investigation, such as the exploration of ensemble methods, federated learning for enhanced data privacy, and adaptive learning systems for intrusion detection in IoT devices. Engaging with these emerging trends can help foster further innovation in the field of cybersecurity.

In conclusion, the research is expected to advance the current knowledge of intrusion detection within wireless networks, offering both theoretical contributions and practical solutions to enhance security within educational settings.

DISCUSSION AND CONTRIBUTIONS

This study contributes to IDS research by proposing a modular framework tailored for educational WLANs, bridging academic research and application, and introducing machine learning readiness for future expansion.

Conclusion

This research proposes a modular intrusion detection framework tailored for securing wireless campus networks against cyber-physical threats. The system integrates anomaly detection, modular design, and machine learning readiness, offering a scalable and adaptable solution. Future work will explore federated learning, advanced deep learning algorithms, and IoT-focused deployments.

REFERENCES

1. *Ali, A., Singh, G., Lunardi, W., Bariah, L., Baddeley, M., Lopez, M., … & Muhaidat, S. (2022). Rf jamming dataset: a wireless spectral scan approach for malicious interference detection.. https://doi.org/10.36227/techrxiv.21524508*
2. *Aziz, S., & Bešťák, M. (2024). Insight into anomaly detection and prediction and mobile network security enhancement leveraging K-Means clustering on call detail records. Sensors, 24(6). doi:10.3390/s24061716*
3. *Bağcı, H., & Çelik, H. (2024). An application of robust principal component analysis methods for anomaly detection. Turkish Journal of Science and Technology. doi:10.55525/tjst.1293057*
4. *Fotiadou, M., Mavridis, S., & Tzovaras, D. (2021). Network traffic anomaly detection via deep learning. Information, 12(5). doi:10.3390/info12050215*
5. *Fragkiadakis, A. and Askoxylakis, I. (2013). Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques., 1-6. https://doi.org/10.1109/wowmom.2013.6583469*
6. *Hamamoto, K., Shibata, H., & Tamura, K. (2018). Network anomaly detection system using genetic algorithm and fuzzy logic. Expert Systems with Applications, 91, 85-94. doi:10.1016/j.eswa.2017.09.013*
7. *Hussain, F. (2018). Use of firewall and IDS to detect and prevent network attacks. International Journal of Technical Research & Science, 3(9). doi:10.30780/ijtrs.v3.i9.2018.002*
8. *Imtiaz, N., Ali, M., & Siddiqui, A. (2022). Efficient approach for anomaly detection in Internet of Things traffic using deep learning. Wireless Communications and Mobile Computing. doi:10.1155/2022/8266347*

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

9. *Kurniabudi, A., Adi, M. H., & Yulianto, C. (2019). Network anomaly detection research: a survey. Indonesian Journal of Electrical Engineering and Informatics, 7(1). doi:10.52549/ijeei.v7i1.773*
10. *Li, W., Yi, P., Wu, Y., Pan, L., & Li, J. (2014). A new intrusion detection system based on knn classification algorithm in wireless sensor network. Journal of Electrical and Computer Engineering, 2014, 1-8. https://doi.org/10.1155/2014/240217*
11. *Molina-Coronado, M. A., Caro, J., & Carrillo, J. F. (2020). Survey of network intrusion detection methods from the perspective of the knowledge discovery in databases process. IEEE Transactions on Network and Service Management, 17(2), 1218-1232. doi:10.1109/tnsm.2020.3016246*
12. *Mookiah, P., Walsh, J., Greenstadt, R., & Dandekar, K. (2013). Reconfigurable antenna assisted intrusion detection in wireless networks. International Journal of Distributed Sensor Networks, 9(10), 564503. https://doi.org/10.1155/2013/564503*
13. *Natkaniec, M. and Bednarz, M. (2023). Wireless local area networks threat detection using 1d-cnn. Sensors, 23(12), 5507. https://doi.org/10.3390/s23125507*
14. *Pelati, N., Cibrián, A., & García-Gallego, J. (2022). Traffic anomaly detection using deep semi-supervised learning at the mobile edge. IEEE Transactions on Vehicular Technology, 71(5), 1-10. doi:10.1109/tvt.2022.3174735*
15. *Ramasamy, P., Hema, S., & Senthilkumar, K. (2004). CoBFIT: A component-based framework for intrusion tolerance. In 2004 IEEE International Conference on European Test Symposium (pp. 107-113). doi:10.1109/eurmic.2004.1333427*
16. *Rana, V. (2019). Anomaly detection in network traffic using machine learning and deep learning techniques. Turkish Journal of Computer and Mathematics Education (Turcomat), 10(2). doi:10.17762/turcomat.v10i2.13626*
17. *Shone, N., Natarajan, R., & Hossain, M. J. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50. doi:10.1109/tetci.2017.2772792*
18. *Sodhro, A., Obaidat, M., Abbasi, Q., Pace, P., Pirbhulal, S., Yasar, A., … & Qaraqe, M. (2019). Quality of service optimization in an iot-driven intelligent transportation system. Ieee Wireless Communications, 26(6), 10-17. https://doi.org/10.1109/mwc.001.1900085*
19. *Yang, Y., & Wang, H. (2020). A survey on network security traffic analysis and anomaly detection techniques. International Journal of Engineering and Technology, 4(1). doi:10.62677/ijetaa.2404117*
20. *Yadhu, V., Kumar, A., & Kaur, P. (2023). Machine learning based intrusion detection system. International Research Journal of Modernization in Engineering Technology and Science, 5(3). doi:10.56726/irjmets37056*
21. *Zhang, G., & Liao, Y. (2018). Dynamic link anomaly analysis for network security management. Journal of Network and Systems Management, 26(4), 855-875. doi:10.1007/s10922-018-9478-8*
22. *Zhao, D., Ma, T., & Hu, F. (2009). A network intrusion-tolerant system based on adaptive algorithm. In 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing (pp. 1-5). doi:10.1109/wicom.2009.5301833*
23. *Zhao, X., Chen, W., & Chen, Y. (2021). A review of computer vision methods in network security. IEEE Communications Surveys & Tutorials, 23(3), 2141-2176. doi:10.1109/comst.2021.3086475*

FIGURES

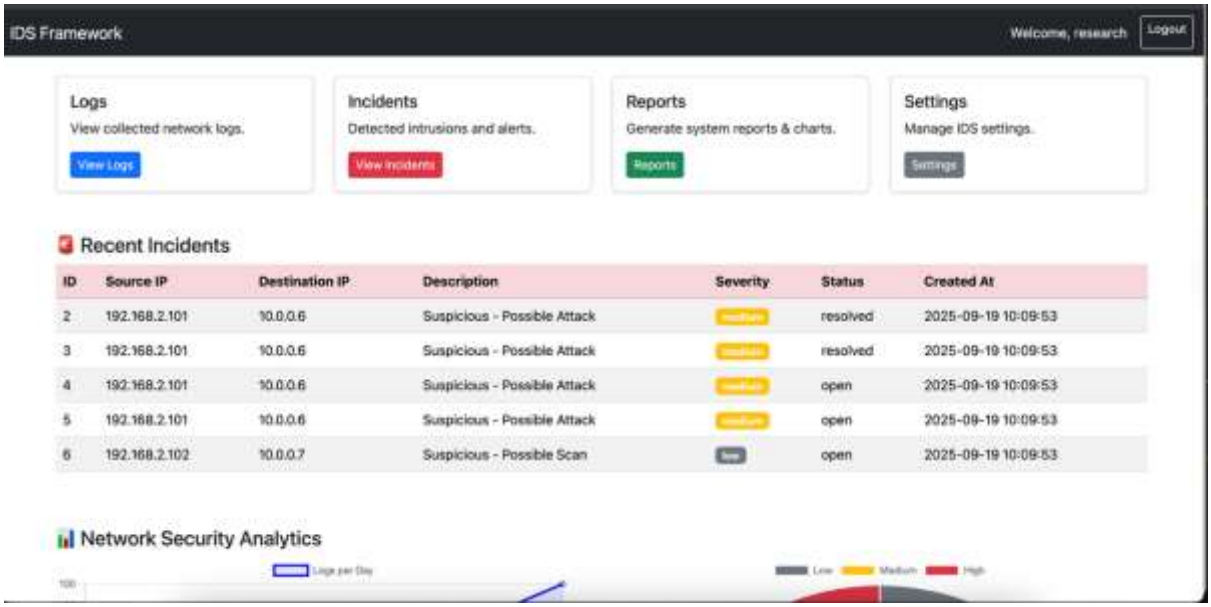


Figure 1
Dashboard interface for monitoring logs and incidents.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal

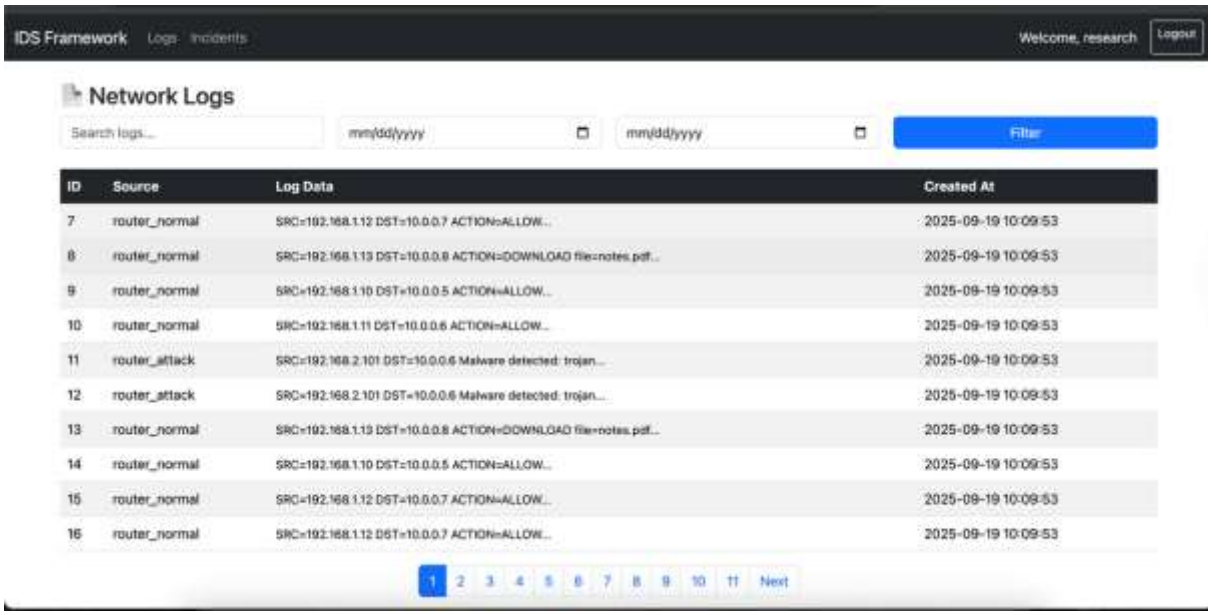


Figure 2
Network Logs Visualization.

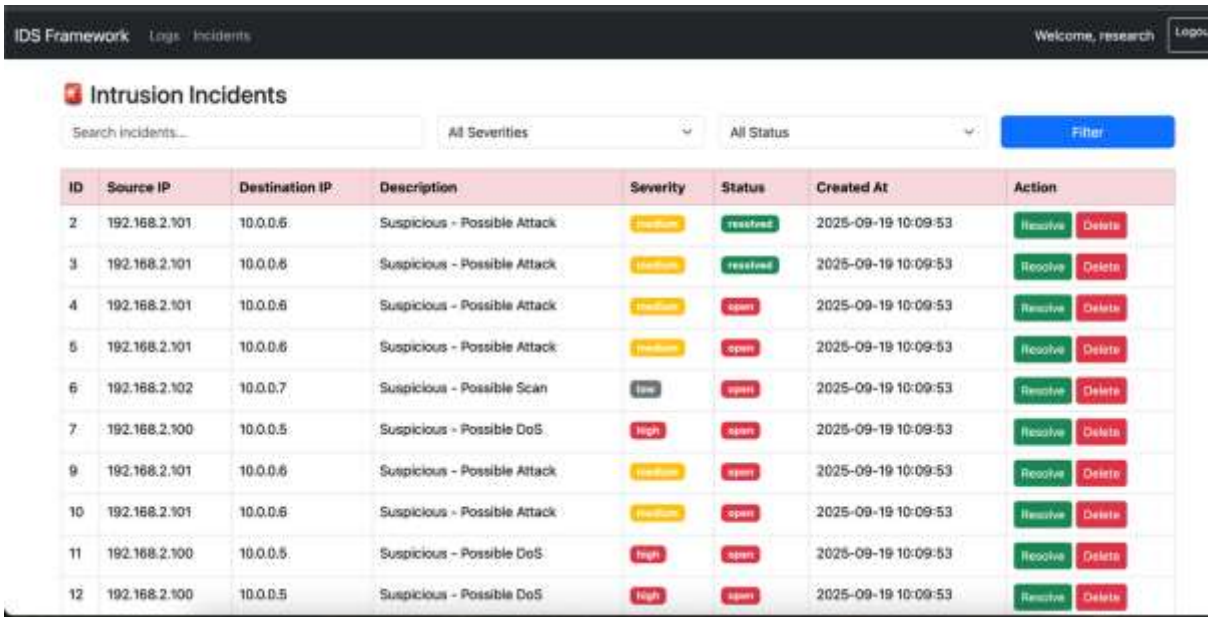


Figure 3
Intrusion Incident Management Interface.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 12 | December 2025 - Peer Reviewed Journal



Figure 4
Reports and Analytics Module.