Journal of Computer Science and Technology Application (CORISINTA)
Vol. 3, No. 2, August, 2026, pp. 171∼184
E-ISSN: 3064-3597 | P-ISSN: 3046-7616, DOI: 10.33050

Deep Learning Enabled Security Monitoring for Intrusion Detection in Smart Campus Networks

Ruli Supriati[1], Nuke Puji Lestari Santoso[2], Steven Harazaki Lase[3], Carlos Perez[4*]
[1]Faculty of Science and Technology, Universitas Raharja, Indonesia
[2,3]Faculty of Economics and Business, Universitas Raharja, Indonesia
[4]Department of Computer Science, Ilearning Incorporation, Colombia
[1]rulisupriati@raharja.info, [2]nuke@raharja.info, [3]steven.harazaki@raharja.info, [4]carloszz11@ilearning.co
***Corresponding Author**

Article Info

Article history:

Submission February 20, 2026
Revised July 6, 2026
Accepted July 16, 2026
Published July 17, 2026

Keywords:

Deep Learning
IDS
Smart Campus Networks
CNN-LSTM
Cybersecurity

ABSTRACT

The increasing complexity of smart campus networks has heightened the need for advanced cybersecurity measures to protect sensitive data and ensure seamless operations. Traditional Intrusion Detection Systems (IDS) often struggle to cope with the dynamic and heterogeneous nature of network traffic in smart campus environments, necessitating the development of more effective solutions. **This study aims** to propose a deep learning-based intrusion detection system for smart campus networks, utilizing a Hybrid CNN-LSTM model to enhance security monitoring. **The proposed methodology** integrates Convolutional Neural Networks (CNN) for feature extraction and Long Short-Term Memory (LSTM) networks for capturing temporal dependencies in network traffic. The model was trained and evaluated on a combination of publicly available datasets and simulated smart campus data, measuring performance through key metrics such as accuracy, precision, recall, and F1-score. **Results** show that the Hybrid CNN-LSTM model outperforms traditional machine learning models, achieving an accuracy of 97.3% and a ROC-AUC of 0.99, demonstrating superior detection of both known and unknown intrusions. **The findings** suggest that deep learning models, especially when tailored to smart campus contexts, offer significant advantages in real-time threat detection and adaptive learning. This research contributes to the growing body of knowledge on AI-driven network security and provides practical insights for improving cybersecurity infrastructures in higher education institutions.

DOI: https://doi.org/10.33050/corisinta.v3i2.187

1. INTRODUCTION

The advancement of digital transformation in higher education has driven the development of smart campus ecosystems, where universities utilize emerging technologies such as Internet of Things (IoT), cloud computing, digital platforms, and intelligent information systems to enhance educational services, operational effectiveness, and institutional decision-making processes [1]. A smart campus environment consists of various interconnected applications and infrastructures, including e-learning platforms, automated attendance systems, intelligent access management, surveillance technologies, environmental monitoring sensors, and digital administrative services. Although these integrated technologies provide significant benefits in improving campus efficiency and user experience, they also introduce greater reliance on interconnected networks and increase

the complexity of the digital environment. Consequently, cybersecurity has become a fundamental challenge for smart campus infrastructures, as the increasing number of connected devices, users, and digital services enlarges the attack surface and exposes university networks to diverse cyber risks and potential security breaches [2].

Cybersecurity challenges within smart campus networks continue to grow as cyber attacks become more adaptive, complex, and difficult to identify through conventional security techniques. Existing protection mechanisms, especially signature-based intrusion detection approaches, often face limitations in recognizing zero-day attacks, hidden malicious activities, and rapidly changing network behaviors [3, 4]. Furthermore, the diverse and large-scale traffic generated by smart campus infrastructures creates additional challenges for traditional monitoring methods and rule-based detection systems, which may not provide sufficient responsiveness in real-time scenarios. These conditions highlight the necessity of intelligent security monitoring solutions capable of analyzing network behaviors, differentiating legitimate activities from potential threats, and enabling faster incident response. Therefore, intrusion detection systems have become a crucial element in strengthening cybersecurity strategies and maintaining the reliability of modern smart campus infrastructures [5].

Recent advances in artificial intelligence, especially deep learning, have provided promising opportunities for improving intrusion detection performance in complex network environments [6]. Deep learning models are able to automatically extract high-level representations from raw or preprocessed traffic data, allowing them to capture hidden, nonlinear, and sequential patterns that are often difficult to identify through traditional machine learning or manual feature engineering. Architectures such as Deep Neural Networks (DNN), CNN, Recurrent Neural Networks (RNN), and LSTM networks have shown strong potential in anomaly detection and cybersecurity applications. Their ability to process large-scale and multidimensional data makes them particularly relevant for intrusion detection tasks in smart campus networks, where data variability and temporal behavior play an important role in security analysis [7, 8].

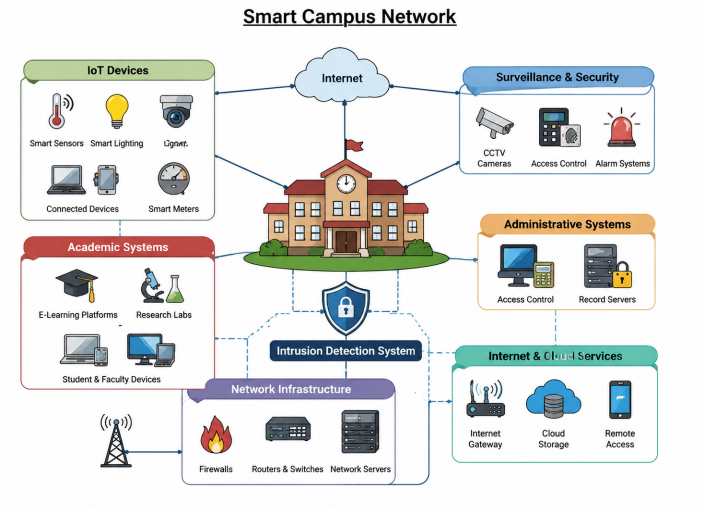

Figure 1. Smart Campus Network Diagram

Figure 1 presents the architecture of a smart campus network by depicting the relationships among major components, including IoT devices, academic platforms, surveillance systems, network infrastructure, and cloud-based services. The figure positions the Intrusion Detection System (IDS) as a central security mechanism responsible for continuously monitoring network activities and protecting interconnected campus resources from potential threats [9]. The surrounding components represent various smart campus services, such as intelligent sensors and automated facilities within IoT environments, e-learning and research platforms in academic systems, CCTV-based monitoring solutions, and network security components including firewalls and routers. This architecture demonstrates the highly interconnected nature of smart campus ecosystems, where diverse digital services and devices require an adaptive and comprehensive cybersecurity framework to ensure secure communication, reliable operation, and protection against emerging cyber threats [10].

Despite the extensive investigation of CNN-LSTM-based intrusion detection approaches in cybersecurity research, previous studies have largely concentrated on general-purpose network datasets, enterprise in-

frastructures, IoT environments, and cloud computing scenarios. Most existing works primarily evaluate model effectiveness through classification metrics, including accuracy, precision, recall, and F1-score, while providing limited consideration of the unique operational characteristics and security requirements of smart campus networks. In contrast to traditional network environments, smart campus infrastructures combine diverse digital services, including academic platforms, administrative systems, IoT devices, mobile users, surveillance technologies, and cloud-based applications within a highly interconnected ecosystem [11]. This complexity generates dynamic and heterogeneous traffic patterns that require security monitoring solutions capable of understanding contextual network behavior. Therefore, this study introduces a Hybrid CNN-LSTM model as an adaptive security monitoring framework rather than merely a classification method, specifically tailored to address intrusion detection challenges in smart campus environments. By combining spatial feature extraction, temporal dependency analysis, and real-time monitoring capabilities, this research extends existing CNN-LSTM IDS approaches toward a more context-aware and practical cybersecurity solution for smart campus networks [12, 13].

Based on this background, this study proposes a deep learning enabled security monitoring approach for intrusion detection in smart campus networks. The main objective of the research is to examine how deep learning techniques can enhance network security monitoring by detecting intrusive activities more accurately and efficiently in a smart campus environment. This study also seeks to contribute to the intersection of artificial intelligence, cybersecurity, and computer networks. From a theoretical perspective, the research is expected to enrich the literature on intelligent intrusion detection in higher education network environments [14]. From a practical perspective, the findings may provide a foundation for developing smarter, more responsive, and more scalable campus network security systems capable of supporting sustainable digital transformation in universities [15].

While existing research on intrusion detection in network security has extensively explored the application of machine learning techniques, there is a notable gap in studies focusing on deep learning for smart campus networks. Most existing models have been designed for general enterprise networks, IoT systems, or cloud infrastructures, where the complexity of data traffic differs significantly from that in smart campus environments [16]. A smart campus network, by nature, involves multiple interconnected services, including academic applications, administrative systems, IoT devices, mobile platforms, and surveillance networks. Each of these systems generates diverse types of traffic, creating unique challenges in identifying and classifying potential intrusions. Additionally, many traditional IDS are not well-suited to handle the scale and dynamism of smart campus environments. While deep learning has been successfully applied to other sectors, research addressing its application in the specific context of smart campus security remains limited. Furthermore, the integration of deep learning-based IDS into real-time security monitoring processes, which would enhance the operational response to cyber threats, has not been sufficiently explored [17].

This research introduces an innovative approach by leveraging deep learning-based security monitoring specifically tailored for smart campus networks. Unlike conventional IDS that rely on predefined signatures or rule based systems, this study employs advanced deep learning models to automatically detect complex intrusion patterns in network traffic without relying on human engineered features [18, 19]. The novelty of this research lies in applying state-of-the-art deep learning architectures such as CNN, RNN, and LSTM networks to address the unique characteristics of smart campus traffic. The study aims to improve detection accuracy while minimizing false positives, which are crucial for operational efficiency in a campus environment. Moreover, this research proposes an integrated security monitoring framework that not only detects intrusions but also allows for real-time alerts and automated responses, an area that has received limited attention in previous studies focused on traditional campus networks [20].

This study contributes to the achievement of the Sustainable Development Goals (SDGs), particularly SDG 4 (Quality Education) and SDG 9 (Industry, Innovation, and Infrastructure), by strengthening the security and sustainability of digital education infrastructures. The implementation of a deep learning-enabled IDS for smart campus networks supports SDG 4 by ensuring the availability, reliability, and continuity of digital learning environments through improved protection against cyber threats targeting academic platforms, administrative systems, and connected educational services [21]. Furthermore, the proposed Hybrid CNN-LSTM framework aligns with SDG 9 by promoting innovative and resilient digital infrastructure through the integration of artificial intelligence, deep learning, and intelligent cybersecurity mechanisms [22]. By enabling accurate threat detection, adaptive monitoring, and proactive security responses, the proposed approach supports universities in developing secure, scalable, and sustainable smart campus ecosystems capable of accommodating

future digital transformation. Therefore, this research demonstrates that AI-driven cybersecurity solutions play an important role in building trusted educational infrastructures and advancing sustainable digital innovation.

2. LITERATURE REVIEW

2.1. Smart Campus Networks

The smart campus paradigm has become an important strategy for accelerating digital transformation in higher education institutions by integrating advanced technologies into academic and operational ecosystems. Through the adoption of IoT, cloud computing, big data analytics, and intelligent information systems, universities can enhance service delivery, improve infrastructure management, and optimize institutional processes. Various implementations, including smart lighting systems, energy monitoring solutions, automated attendance platforms, and connected campus services, demonstrate how digital technologies contribute to creating more efficient, innovative, and data-driven educational environments [23, 24]. Nevertheless, the increasing interconnection among devices, applications, and network services also expands the potential attack surface of university infrastructures. Consequently, smart campus environments face growing cybersecurity risks, particularly involving the protection of sensitive academic information, personal data, and critical network resources.

Securing smart campus networks remains a complex challenge due to the integration of diverse devices, services, and digital applications within a single interconnected environment. These infrastructures combine conventional information systems with emerging technologies, where each component introduces different security vulnerabilities and potential attack vectors. The resulting network traffic is highly dynamic and heterogeneous, involving various data sources such as academic information, personal records, device-to-device communication, and real-time interactions generated by IoT-based services. Such complexity requires advanced cybersecurity mechanisms capable of processing large-scale network data, detecting abnormal behaviors, and responding effectively to emerging threats in real-time. Therefore, the development of intelligent Intrusion Detection Systems (IDS) that can adapt to the unique characteristics and evolving requirements of smart campus environments has become increasingly important [25].

2.2. Intrusion Detection Systems

An IDS serves as an essential security mechanism in modern network infrastructures by continuously analyzing network activities to identify suspicious behaviors, unauthorized access attempts, data breaches, and other malicious actions. In general, IDS approaches are divided into two main categories: signature-based detection and anomaly-based detection. Signature-based IDS identify threats by comparing network activities against predefined patterns or known attack signatures, making them effective for recognizing previously identified attacks [26]. However, this approach has limited capability in detecting zero-day attacks that exploit unknown vulnerabilities and do not match existing signatures. Conversely, anomaly-based IDS detect deviations from established normal network behavior, providing greater adaptability in identifying emerging and previously unknown threats.

Although anomaly based IDS provide greater flexibility in identifying previously unseen threats, these approaches often generate a higher number of false alarms and require advanced analytical techniques to accurately distinguish legitimate deviations from actual cyber attacks. In smart campus environments, conventional IDS approaches face additional limitations due to their inability to efficiently process the large-scale, diverse, and continuously evolving network data produced by interconnected digital systems. The complexity of smart campus traffic, combined with the difficulty of separating normal user activities from malicious behaviors, highlights the need for more intelligent security approaches. Therefore, artificial intelligence and machine learning based techniques have emerged as promising solutions for improving intrusion detection capability, scalability, and adaptability in complex network environments [27].

2.3. Machine Learning and Deep Learning in Intrusion Detection

Machine learning, particularly deep learning, has become a prominent technique in the field of intrusion detection. Deep learning models, such as CNN, RNN, and LSTM networks, offer significant advantages over traditional IDS approaches due to their ability to learn complex patterns in data without the need for manual feature engineering [28].

CNNs are particularly useful for spatial data analysis and can be applied to detect spatial anomalies in network traffic, while RNNs and LSTMs are adept at modeling temporal dependencies in data, making them suitable for analyzing sequential patterns in network behavior [29, 30]. Autoencoders, another deep

learning model, have been widely used for anomaly detection by learning a compressed representation of normal network traffic and identifying deviations from this norm as potential intrusions. These models excel in environments where the data exhibits complex, non-linear relationships and where traditional algorithms might struggle to identify novel attack strategies [31].

Deep learning models in IDS have proven to enhance detection performance significantly. For example, LSTM networks can capture long-term dependencies in sequential data, allowing for better prediction and detection of attack patterns that develop over time. Similarly, CNNs are well-suited for analyzing high-dimensional data, extracting useful features automatically, and classifying traffic based on learned patterns. Despite their advantages, challenges still remain in applying deep learning models effectively for IDS, such as the need for large and diverse datasets, the risk of overfitting, and the lack of interpretability, which is crucial for security decision-making [32].

2.4. Deep Learning-Based Intrusion Detection in Smart Campus Networks

While deep learning has shown great promise in network security, there is limited research specifically focused on smart campus networks. A smart campus network, unlike typical enterprise or IoT networks, involves a dynamic and diverse set of systems that generate highly variable traffic patterns. These networks often include a mix of academic data, administrative systems, IoT devices, mobile devices, and surveillance cameras, each with different network behavior [33, 34]. The heterogeneous nature of these systems complicates intrusion detection because the model must not only detect traditional attacks but also understand the behavior of various devices operating in a shared network. Some studies have started to address this gap by proposing deep learning models specifically for smart campuses. For example, LSTM networks have been used to detect DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks that target campus network infrastructure. These models demonstrated an improvement in detecting threats that would otherwise be missed by traditional IDS. However, challenges remain in terms of model scalability and real-time applicability for large-scale campus deployments [35].

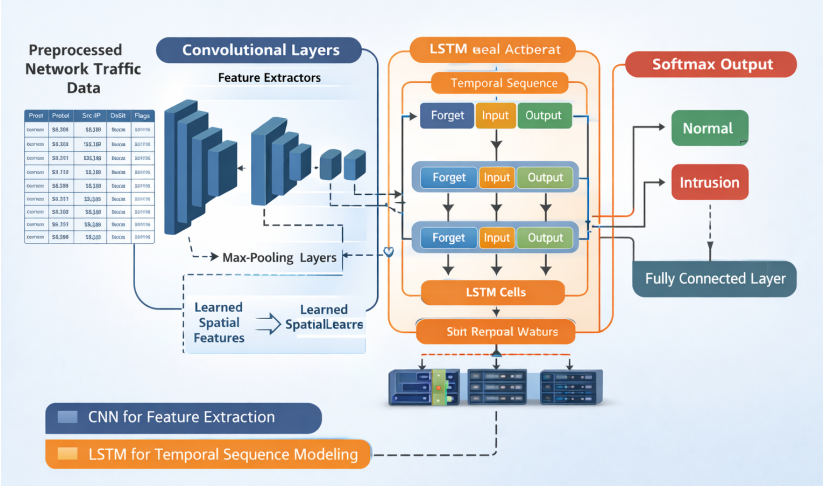

Figure 2. Deep Learning Model Architecture for IDS

Figure 2 illustrates the proposed Hybrid CNN-LSTM architecture developed for intrusion detection in smart campus networks. The framework begins with the preprocessing of network traffic data, which is subsequently fed into the CNN layers to automatically extract significant spatial characteristics from traffic patterns. The extracted representations are then transferred to the LSTM layers, where temporal relationships and sequential dependencies within network activities are learned to identify evolving attack behaviors. The final classification stage applies a softmax-based output layer to categorize network activities into normal traffic or intrusion classes. By integrating the feature extraction capability of CNN with the sequence learning capability of LSTM, the hybrid architecture provides a more adaptive and effective approach for detecting complex and dynamic cyber threats in smart campus network environments [36].

Hybrid models that combine machine learning and deep learning have also shown promise. By integrating Random Forest for feature selection with CNN for classification, hybrid models can achieve a higher

detection rate and reduced false positives in smart campus networks. These hybrid models may provide a balanced approach to IDS by combining the strengths of both traditional machine learning methods and advanced deep learning techniques [22].

2.5. Evaluation Metrics for IDS

The effectiveness of an IDS is measured using several key performance metrics, including accuracy, precision, recall, F1-score, and detection rate. Accuracy measures the proportion of correct predictions (both true positives and true negatives) over all predictions, while precision and recall focus on the balance between detecting attacks (true positives) and minimizing false positives. The F1-score provides a combined measure of both precision and recall, offering a balanced view of the system's performance. These metrics are crucial in ensuring that an IDS for smart campus networks is both accurate and efficient [37].

In addition to the traditional evaluation metrics, scalability and interpretability are important factors when assessing deep learning models for IDS. Scalability refers to the ability of a model to handle increasing amounts of data and traffic as the campus network grows, while interpretability ensures that administrators can understand how the model arrives at its decisions. This is vital in a security context where quick and informed decision-making is essential [38].

3. METHODOLOGY

3.1. Research Design

This research adopts an experimental and quantitative approach to explore the effectiveness of deep learning-based intrusion detection within smart campus networks. The experimental design focuses on developing a robust security monitoring framework using deep learning techniques and testing its performance in identifying intrusions in real-time network traffic. Given the complexity of the smart campus environment, this study integrates multiple data sources to create a comprehensive IDS that addresses both traditional and novel cyber threats [39].

3.2. Research Framework

The proposed methodology follows a systematic framework that includes several key phases:

- Data Collection and Preprocessing.
- Feature Selection and Extraction.
- Deep Learning Model Development.
- Model Training and Evaluation.
- Performance Comparison with Traditional Methods.
- Real-Time Security Monitoring Integration.

Each phase is designed to ensure the accuracy, scalability, and operational relevance of the IDS, particularly for deployment in a smart campus environment [40].

3.3. Dataset

The dataset used in this study was constructed by integrating three publicly available intrusion detection datasets, namely NSL-KDD, CICIDS2017, and UNSW-NB15, with simulated smart campus network traffic. The dataset merging process was conducted by harmonizing common network traffic features, including protocol type, packet duration, source and destination flow characteristics, service type, packet size, connection state, and attack category [41, 42]. Features that were not available across all datasets were either transformed into comparable attributes or excluded to maintain consistency. After feature alignment, all datasets were converted into a unified tabular format and mapped into two main label groups, namely normal traffic and intrusion traffic, while multi-class attack labels such as DoS, DDoS, malware, port scanning, and botnet activities were retained for detailed classification analysis [43].

The dataset consists of a diverse range of network activities, both normal and malicious, representing a variety of cyber-attacks such as DoS, DDoS, malware, port scans, and other forms of intrusions typically

encountered in campus network environments. Data labeling is performed manually, and preprocessing techniques such as normalization, one-hot encoding, and data balancing are applied to ensure that the dataset is suitable for training the deep learning models [44, 45].

3.4. Data Preprocessing

Given the nature of the raw network traffic data, several preprocessing steps are applied to prepare the dataset for model training:

- Data Cleaning: Removing redundant, incomplete, or noisy data entries.
- Handling Missing Values: Missing values are either imputed using statistical methods (mean/median imputation) or removed based on the percentage of missing data in each feature.
- Normalization/Standardization: Continuous features are normalized or standardized to ensure that the input data is on a similar scale, which helps improve model convergence.
- Feature Selection: Irrelevant or highly correlated features are removed using statistical tests or feature importance measures (e.g., Random Forest feature importance or mutual information). This step is crucial for improving model performance by reducing dimensionality and overfitting.

Additionally, a windowing technique is applied to segment continuous network traffic data into fixed-size windows to allow the model to analyze time-series data effectively.

3.5. Deep Learning Model Development

Considering the diverse and sequential nature of network traffic characteristics, this study investigates multiple deep learning architectures to improve the effectiveness of intrusion detection systems. Convolutional Neural Networks (CNN) are employed to automatically learn spatial representations from network traffic patterns and identify complex irregularities within data flows, whereas RNN and Long Short-Term Memory (LSTM) networks are utilized to model temporal dependencies and detect evolving attack behaviors over sequential traffic streams. Furthermore, Autoencoders are incorporated as an unsupervised learning mechanism capable of identifying abnormal activities by learning normal traffic patterns and detecting significant deviations. By combining the advantages of these approaches, the proposed Hybrid CNN-LSTM architecture integrates CNN-driven feature extraction with LSTM-based temporal analysis, enabling more robust detection of both static and dynamic intrusion patterns in complex network environments [46].

The proposed model receives preprocessed network traffic data represented in sequential window formats, where normalized features are organized into time-step sequences containing multiple network attributes. The CNN module is designed with two one-dimensional convolutional layers to extract meaningful spatial patterns from traffic data. The first convolutional layer employs 64 filters with a kernel size of 3 and ReLU activation, while the subsequent layer utilizes 128 filters with the same kernel configuration. Max-pooling operations are applied after each convolutional layer to reduce feature complexity and retain the most relevant traffic characteristics. The resulting feature representations are then forwarded to the LSTM module, which includes two layers with 128 and 64 units to learn long-term temporal dependencies within network behaviors. Additionally, a dropout mechanism with a rate of 0.30 is implemented after both CNN and LSTM layers to reduce overfitting risks and enhance the model's generalization capability across different network conditions [47].

The output layer of the proposed model applies softmax activation to perform multi-class intrusion classification, while sigmoid activation is utilized for binary classification tasks that distinguish between normal and malicious network activities. Model training is conducted using the Adam optimizer with a learning rate of 0.001, a batch size of 32, and 50 training epochs. For optimization, categorical cross-entropy is employed for multi-class classification, whereas binary cross-entropy is used for binary intrusion detection scenarios [48, 49]. To improve model stability and avoid overfitting, an early stopping mechanism based on validation loss is incorporated during the training process. The implementation is developed using Python with the TensorFlow/Keras framework and executed within a GPU-supported computing environment to accelerate deep learning operations. In addition, hyperparameter tuning is performed by optimizing critical parameters, including learning rate, network depth, batch size, and epoch configuration, through grid search or random search approaches. The final model configuration is selected based on validation performance and comprehensive evaluation metrics to achieve optimal intrusion detection capability [50].

3.6. Model Training and Evaluation

The training process of the deep learning models is performed through backpropagation using the Adam optimization algorithm, with the dataset divided into 80% for training and 20% for validation. An early stopping mechanism is applied during training to reduce the risk of overfitting and improve model generalization. The effectiveness of each model is assessed using several classification metrics, including accuracy, precision, recall, F1-score, confusion matrix, and Area Under the Receiver Operating Characteristic Curve (ROC-AUC), which provide comprehensive measurements of detection performance and class separation capability [51]. In addition, the proposed deep learning approaches are benchmarked against conventional machine learning algorithms, including Support Vector Machines (SVM), Random Forest, and K-Nearest Neighbors (KNN), using identical datasets and evaluation procedures to analyze the performance improvements provided by the deep learning-based intrusion detection framework [52].

3.7. Real-Time Security Monitoring Integration

Finally, the research integrates the best-performing deep learning model into a real-time security monitoring framework. This framework continuously analyzes incoming network traffic and flags any suspicious activities based on the learned patterns. The integration will involve a dynamic alerting system that notifies security administrators about potential threats in real-time, enabling prompt response and mitigation [53–55].

4. RESULTS AND DISCUSSION

4.1. Dataset Overview

The dataset used for evaluating the proposed deep learning-based intrusion detection system consists of a combination of publicly available network traffic datasets (e.g., NSL-KDD, CICIDS2017, UNSW-NB15) and simulated traffic from a smart campus network environment. The simulated dataset reflects a real-world smart campus infrastructure, including network traffic generated by IoT devices, academic services, surveillance cameras, administrative networks, and mobile devices.

The dataset includes several classes of normal and attack traffic, such as DoS, DDoS, port scans, malware, and botnet activities, typical of threats targeting smart campus networks. The traffic patterns exhibit both spatial and temporal dependencies, which were essential for evaluating the performance of deep learning models in capturing these intricate patterns.

Table 1. Dataset Summary

Dataset	Instances	Features	Classes
NSL-KDD	125,973	41	23
CICIDS2017	3,000,000	78	15
UNSW-NB15	2,540,044	49	10
Smart Campus Simulated	500,000	55	8

Table 1 presents the summary of the datasets used in this study, including the number of instances, extracted features, and classification classes. The evaluation incorporates widely used intrusion detection datasets, namely NSL-KDD, CICIDS2017, and UNSW-NB15, along with a Smart Campus Simulated dataset designed to represent realistic network conditions in educational environments. Among the datasets, CICIDS2017 provides the largest number of instances with 3,000,000 samples and 78 features, enabling comprehensive evaluation of model scalability. The NSL-KDD dataset contains 125,973 instances with 41 features, while UNSW-NB15 includes 2,540,044 instances with 49 features representing diverse attack scenarios. Furthermore, the Smart Campus Simulated dataset consists of 500,000 instances, 55 features, and 8 attack classes, allowing the proposed model to be evaluated in a context-specific smart campus environment. The combination of benchmark and simulated datasets ensures that the proposed deep learning-based intrusion detection approach is assessed across diverse network characteristics and attack patterns.

4.2. Model Training and Performance Metrics

The CNN, LSTM, and Hybrid CNN-LSTM models were trained using an 80%-20% division between training and validation datasets to ensure reliable performance assessment. During the optimization process, the Adam optimizer was configured with a learning rate of 0.001, a batch size of 32, and a maximum of 50 epochs. An early stopping strategy was incorporated by monitoring validation performance to minimize

overfitting and enhance model generalization. The effectiveness of the proposed models was measured using several classification metrics, including accuracy, precision, recall, F1-score, and ROC-AUC. The experimental evaluation shows that the deep learning approaches provide improved intrusion detection capability across multiple datasets, demonstrating their effectiveness in identifying both previously recognized and emerging attack patterns compared with conventional detection methods.

Table 2. Model Performance Comparison

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
CNN	95.2%	94.5%	93.8%	94.1%	0.98
LSTM	96.1%	95.7%	94.3%	94.9%	0.98
Hybrid CNN-LSTM	97.3%	96.5%	95.8%	96.1%	0.99
SVM (Baseline)	91.4%	89.7%	87.6%	88.6%	0.91
Random Forest	92.3%	90.4%	88.2%	89.3%	0.92

As shown in Table 2, the Hybrid CNN-LSTM model achieved the best overall performance compared with CNN, LSTM, SVM, and Random Forest models, with an accuracy of 97.3%, precision of 96.5%, recall of 95.8%, F1-score of 96.1%, and ROC-AUC of 0.99. However, overall accuracy alone is not sufficient to evaluate intrusion detection performance, especially in smart campus networks where attack traffic may be less frequent than normal traffic. Therefore, the results were further interpreted by considering false positives, false negatives, class imbalance, and detection performance across different attack categories.

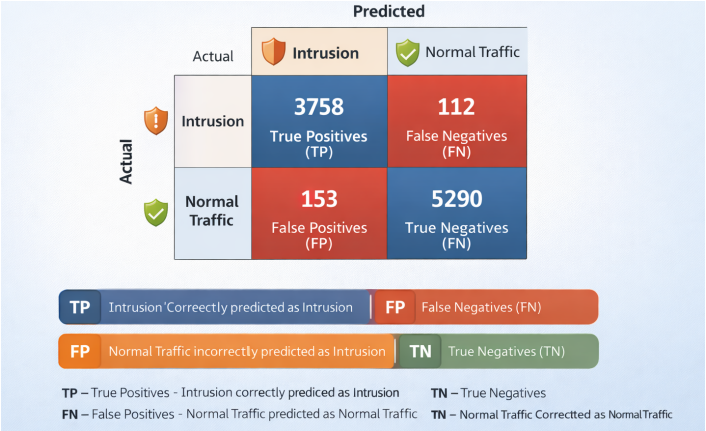

Figure 3. Confusion Matrix for Hybrid CNN-LSTM Model

Figure 3 presents the confusion matrix for the Hybrid CNN-LSTM model, which classifies network traffic into two categories: “Intrusion” and “Normal Traffic.” The matrix displays True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN), providing a clear assessment of the model’s classification performance. True Positives represent intrusion traffic correctly identified as attacks, while False Positives indicate normal traffic incorrectly classified as intrusion. True Negatives show normal traffic correctly classified, whereas False Negatives indicate intrusion traffic misclassified as normal. This visual representation demonstrates the model’s ability to distinguish between normal and malicious network traffic while minimizing classification errors.

The confusion matrix analysis of the Hybrid CNN-LSTM model evaluates classification performance based on TP, TN, FP, and FN. The results indicate that the model achieves strong classification capability across different attack categories by accurately identifying malicious activities while maintaining reliable detection of normal traffic. The model demonstrates minimal false positive and false negative rates, reducing the risk of misclassifying legitimate network behavior as attacks or failing to detect actual intrusions. In particular, the Hybrid CNN-LSTM approach shows effective detection performance for critical threats such as DDoS and botnet attacks commonly found in smart campus network environments, confirming its capability to provide accurate and adaptive intrusion detection.

4.3. Model Comparison with Baseline Methods

For further evaluation, the proposed deep learning approaches were compared with conventional machine learning algorithms, including Support Vector Machine (SVM), Random Forest, and KNN. As presented in Table 2, the CNN, LSTM, and Hybrid CNN-LSTM models achieved superior performance compared with traditional classifiers, particularly in terms of recall, demonstrating their ability to reduce missed intrusion detections. Although conventional machine learning methods provide acceptable classification results, their performance is relatively limited when processing high-dimensional and sequential network traffic characteristics commonly found in smart campus environments. The improved results achieved by deep learning models are primarily attributed to their capability to automatically extract complex feature representations and capture hidden patterns within large-scale network traffic data.

4.4. Real-Time Security Monitoring Performance

The real-time security monitoring framework was evaluated in a simulated smart campus environment to assess its capability in processing and classifying network traffic under controlled benchmark conditions. The experiment used traffic streams representing e-learning access, administrative system transactions, IoT sensor communication, CCTV data transmission, mobile device access, and cloud-based academic services. Malicious traffic was injected into the stream to represent DDoS, malware communication, port scanning, botnet activity, and unauthorized access attempts. The benchmark scenario was designed to evaluate whether the proposed Hybrid CNN-LSTM model could generate intrusion alerts with low latency while maintaining stable detection performance.

The system successfully detected various types of cyber threats, including DDoS, malware, and unauthorized access attempts, and sent timely alerts to network administrators. The integration of deep learning into the monitoring framework enabled continuous adaptive learning, allowing the system to fine-tune itself over time based on evolving network behaviors.

5. MANAGERIAL IMPLICATIONS

The findings of this study have several significant managerial implications for university administrators, network security teams, and decision-makers involved in the implementation and maintenance of smart campus networks. As smart campuses evolve into complex, interconnected environments, the need for advanced security monitoring solutions becomes paramount to safeguard sensitive data and ensure the continuity of critical services. The use of deep learning-based IDS provides an effective and adaptive approach to meet these security challenges.

5.1. Improved Threat Detection and Response

The integration of deep learning models, such as the Hybrid CNN-LSTM model proposed in this study, enables the real-time detection of intrusions with high accuracy and minimal false positives. This capability is essential for network administrators, as it allows them to identify and respond to threats more quickly, minimizing the impact of attacks on the smart campus network. By incorporating automated alerting mechanisms, this IDS model empowers security teams to make informed decisions in real-time, reducing the time between detection and mitigation. As a result, universities can enhance their response times to cyber threats, protecting not only academic data but also personal information, financial records, and intellectual property.

5.2. Cost-Effectiveness and Resource Optimization

One of the key advantages of implementing a deep learning-based IDS is its potential to reduce the costs associated with network security. Traditional security measures, such as manual monitoring, signature-based systems, and periodic vulnerability assessments, are not only labor-intensive but also less effective in detecting evolving or novel threats. By contrast, deep learning models automate the detection process, requiring fewer manual interventions and thereby freeing up security personnel to focus on strategic tasks. Additionally, the ability to continuously improve the model through adaptive learning means that the system becomes more efficient over time, leading to long-term cost savings and resource optimization.

5.3. Scalability and Future-Proofing

As smart campuses expand, so does the volume of data and the complexity of the network. The scalability of deep learning models allows universities to future-proof their security infrastructure. Unlike traditional systems, which often require significant adjustments or upgrades as the network grows, deep learning models

can be trained on larger datasets and fine-tuned to handle more traffic without compromising performance. This scalability ensures that as universities adopt more IoT devices, cloud-based services, and digital platforms, their security systems can grow in tandem without requiring a complete overhaul. For university administrators, this offers a long-term solution that evolves with the institution's digital transformation.

5.4. Proactive Security Management and Risk Mitigation

By providing continuous monitoring and advanced threat detection capabilities, deep learning-based IDS models promote a proactive security approach. Rather than reacting to attacks after they occur, network administrators can anticipate and mitigate potential threats before they escalate into significant incidents. The system's ability to detect novel intrusions that were not part of previous attack signatures makes it a more comprehensive tool for risk management. Universities can use this proactive approach to not only safeguard their infrastructure but also to comply with data protection regulations, such as GDPR or FERPA, by ensuring that sensitive student and faculty data is protected against cyber threats.

5.5. Enhanced Decision-Making and Strategic Planning

The real-time data insights generated by the IDS can also aid in strategic decision-making. By providing administrators with detailed reports on network activities, traffic patterns, and potential threats, the system supports informed decision-making processes. Security teams can analyze these reports to identify vulnerabilities, optimize security protocols, and refine policies for access control, network segmentation, and incident response. Moreover, this data-driven approach ensures that the security infrastructure remains aligned with the evolving needs of the institution, fostering a culture of continuous improvement in network security practices.

6. CONCLUSION

This study has proposed a deep learning-enabled security monitoring system for intrusion detection in smart campus networks, addressing the growing cybersecurity challenges faced by educational institutions. By leveraging the Hybrid CNN-LSTM model, which combines CNN for feature extraction and LSTM networks for sequential pattern analysis, this research has demonstrated a significant improvement in detecting intrusions with high accuracy and minimal false positives. The model's ability to learn both spatial and temporal patterns in network traffic makes it particularly suitable for the dynamic and interconnected environment of a smart campus.

The results presented in this paper show that the deep learning-based model outperforms traditional machine learning methods, such as SVM and Random Forest, in terms of detection accuracy, precision, recall, and F1-score. The Hybrid CNN-LSTM model achieved superior performance in detecting both known and novel attack patterns, demonstrating the potential of deep learning for real-time network security monitoring. Moreover, the real-time integration of this model into a smart campus network allows for continuous, adaptive learning, offering a scalable and proactive solution to network security that can evolve with the increasing complexity of digital campuses.

In conclusion, the integration of AI-driven intrusion detection systems in smart campus networks not only enhances security but also provides long-term benefits in terms of cost reduction, resource optimization, and strategic decision-making. By adopting such technologies, universities can create safer, more resilient environments for students, faculty, and staff, ensuring the protection of sensitive data and maintaining the integrity of their digital infrastructure. Future research could explore the further refinement of this model, including its application to real-world campus environments and its integration with other IoT security frameworks. Ultimately, this study contributes to the advancement of cybersecurity in higher education and provides a foundation for future innovations in smart campus security.

7. DECLARATIONS

7.1. About Authors

Ruli Supriati (RS) https://orcid.org/0009-0005-0315-5088
Nuke Puji Lestari Santoso (NP) https://orcid.org/0000-0002-4414-2102
Steven Harazaki Lase (SH) https://orcid.org/0009-0002-6647-7541
Carlos Perez (CP) https://orcid.org/0009-0006-5344-6833

7.2. Author Contributions

Conceptualization: RS; Methodology: NP; Software: SH; Validation: CP and RS; Formal Analysis: NP and SH; Investigation: CP; Resources: RS; Data Curation: NP; Writing Original Draft Preparation: SH and CP; Writing Review and Editing: RS and NP; Visualization: SH; All authors, RS, NP, SH, and CP have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] J. Li, N. B. Linsangan, and H. Dong, "Campus network traffic prediction and anomaly detection based on deep learning," *International Journal of Emerging Technologies and Advanced Applications*, vol. 1, no. 7, pp. 8–13, 2024.

[2] Z. Chen, "Campus network security intrusion detection based on feature segmentation and deep learning," *Journal of Cyber Security and Mobility*, vol. 13, no. 4, pp. 775–802, 2024.

[3] K. Richard, B. O. Sadiq, and V. Maniniti, "Securing campus networks with intelligence: a review of machine learning techniques for ddos and arp protection," *Discover Networks*, vol. 2, no. 1, p. 11, 2026.

[4] B. Any, S. Four, and C. Tariazela, "Technology integration in tourism management: Enhancing the visitor experience," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 81–88, 2024.

[5] Y. Zhu and W. Wei, "A study on predicting campus tailgating intrusion using data fusion technology based on iot and cloud computing in the security management of smart campuses at private universities," in *2025 5th Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS)*. IEEE, 2025, pp. 321–325.

[6] F. S. Alsubaei, "Smart deep learning model for enhanced iot intrusion detection," *Scientific Reports*, vol. 15, no. 1, p. 20577, 2025.

[7] M. Imran, N. Haider, M. Shoaib, I. Razzak *et al.*, "An intelligent and efficient network intrusion detection system using deep learning," *Computers and Electrical Engineering*, vol. 99, p. 107764, 2022.

[8] H. Safitri, M. H. R. Chakim, and A. Adiwijaya, "Strategy based technology-based startups to drive digital business growth," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 2, pp. 207–220, 2023.

[9] U. AlHaddad, A. Basuhail, M. Khemakhem, F. E. Eassa, and K. Jambi, "Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks," *Sensors*, vol. 23, no. 17, p. 7464, 2023.

[10] M. F. Mustafa, M. R. M. Isa, M. A. Khairuddin, M. S. F. M. Yunus, and N. A. A. Jamaluddin, "Enhancing security in smart campus networks: Implementation of network detection and response (ndr) platform," *JOIV: International Journal on Informatics Visualization*, vol. 10, no. 3, pp. 1112–1120, 2026.

[11] F. Al-Quayed, Z. Ahmad, and M. Humayun, "A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0," *Ieee Access*, vol. 12, pp. 34 800–34 819, 2024.

[12] Y. Zhang, Y. Zheng, C. Yin, and L. Sun, "Performance evaluation of deep learning algorithms in intelligent campus security monitoring and management system," in *Proceedings of the International Conference on Algorithms, Software Engineering, and Network Security*, 2024, pp. 455–459.

[13] J. Jones, E. Harris, Y. Febriansah, A. Adiwijaya, and I. N. Hikam, "Ai for sustainable development: Applications in natural resource management, agriculture, and waste management," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 143–149, 2024.

[14] S. Tsimenidis, T. Lagkas, and K. Rantos, "Deep learning in iot intrusion detection," *Journal of network and systems management*, vol. 30, no. 1, p. 8, 2022.

[15] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for iot networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, p. 107810, 2022.

[16] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for sdn-enabled intrusion detection system in iot networks," *Information*, vol. 14, no. 1, p. 41, 2023.

[17] A. Odeh and A. Abu Taleb, "Ensemble-based deep learning models for enhancing iot intrusion detection," *Applied Sciences*, vol. 13, no. 21, p. 11985, 2023.

[18] N. W. Khan, M. S. Alshehri, M. A. Khan, S. Almakdi, N. Moradpoor, A. Alazeb, S. Ullah, N. Naz, and J. Ahmad, "A hybrid deep learning-based intrusion detection system for iot networks," *Math. Biosci. Eng*, vol. 20, no. 8, pp. 13 491–13 520, 2023.

[19] A. Alwiyah and W. Setyowati, "A comprehensive survey of machine learning applications in medical image analysis for artificial vision," *International Transactions on Artificial Intelligence*, vol. 2, no. 1, pp. 90–98, 2023.

[20] J. Ogbiti, "Development of campus security surveillance system using smart device," *Journal of Institutional Research, Big Data Analytics and Innovation*, vol. 1, no. 4, pp. 8–16, 2025.

[21] N. Yadav, S. Pande, A. Khamparia, and D. Gupta, "Intrusion detection system on iot with 5g network using deep learning," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 9304689, 2022.

[22] M. F. A. M. F. ALI, "Enhancing iot network security through deep learning-based intrusion detection," *Wasit Journal of Computer and Mathematics Science*, vol. 4, no. 2, pp. 74–85, 2025.

[23] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for iot attacks using deep learning technique," *Computers and Electrical Engineering*, vol. 107, p. 108626, 2023.

[24] R. Ahli, M. F. Hilmi, and A. Abudaqa, "Moderating effect of perceived organizational support on the relationship between employee performance and its determinants: A case of entrepreneurial firms in uae," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 199–212, 2024.

[25] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "Enhanced ids with deep learning for iot-based smart cities security," *Tsinghua Science and Technology*, vol. 29, no. 4, pp. 929–947, 2024.

[26] L. Tan, "Huge-graph-based risk communities mining and prediction: a smart campus security protection system toward effective students management," *Progress in Artificial Intelligence*, pp. 1–21, 2026.

[27] E. U. H. Qazi, M. H. Faheem, and T. Zia, "Hdlnids: hybrid deep-learning-based network intrusion detection system," *Applied Sciences*, vol. 13, no. 8, p. 4921, 2023.

[28] Y. Otoum, D. Liu, and A. Nayak, "Dl-ids: a deep learning–based intrusion detection framework for securing iot," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3803, 2022.

[29] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced intelligent smart home control and security system based on deep learning model," *Wireless communications and mobile computing*, vol. 2022, no. 1, p. 9307961, 2022.

[30] Y. Shino, H. Kenta, and I. K. Mertayasa, "Media promotional for art in tangerang city with audio visual adobe creative," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 4, no. 2, pp. 192–204, 2022.

[31] O. A. Mahmood, "Enhancing intrusion detection in wireless sensor networks through machine learning techniques and context awareness integration," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, pp. 244–258, 2024.

[32] Y. Kayode Saheed, O. Harazeem Abdulganiyu, and T. Ait Tchakoucht, "A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and scada systems for smart city infrastructures," *Journal of King Saud University Computer and Information Sciences*, vol. 35, no. 5, p. 101532, 2023.

[33] I. A. Kandhro, S. M. Alanazi, F. Ali, A. Kehar, K. Fatima, M. Uddin, and S. Karuppayah, "Detection of real-time malicious intrusions and attacks in iot empowered cybersecurity infrastructures," *IEEE Access*, vol. 11, pp. 9136–9148, 2023.

[34] A. Nuche, O. Sy, and J. C. Rodriguez, "Optimizing efficiency through sustainable strategies: The role of management and monitoring in achieving goals," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 167–174, 2024.

[35] U. Ahmed, M. Nazir, A. Sarwar, T. Ali, E.-H. M. Aggoune, T. Shahzad, and M. A. Khan, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Scientific Reports*, vol. 15, no. 1, p. 1726, 2025.

[36] K. Chakal, M. Korkiakoski, H. Mehmood, T. Anagnostopoulos, P. Alavesa, and P. Kostakos, "Augmented

reality integration for real-time security and maintenance in iot-enabled smart campuses," in *2023 IEEE 31st International Conference on Network Protocols (ICNP)*. IEEE, 2023, pp. 1–6.

[37] K. Sivaprasad Yerneni, A. Ravi Teja, K. Sri Harsha, and Y. Naresh Kiran Kumar Reddy, "Towards proactive cloud security: A survey on ml and deep learning-based intrusion detection systems," *J Contemp Edu Theo Artific Intel: JCETAI-116*, 2025.

[38] H. Shah, D. Shah, N. K. Jadav, R. Gupta, S. Tanwar, O. Alfarraj, A. Tolba, M. S. Raboaca, and V. Marina, "Deep learning-based malicious smart contract and intrusion detection system for iot environment," *Mathematics*, vol. 11, no. 2, p. 418, 2023.

[39] H. Zhang, X. Zhai, and J. Sun, "Application prospects of optical fiber sensing technology in smart campus construction: A review," in *Photonics*, vol. 12, no. 10. MDPI, 2025, p. 1026.

[40] M. Y. Ayub, U. Haider, A. Haider, M. T. A. Tashfeen, H. Shoukat, and A. Basit, "An intelligent machine learning based intrusion detection system (ids) for smart cities networks," *EAI Endorsed Transactions on Smart Cities*, vol. 7, no. 1, p. e4, 2023.

[41] S. Abdel-Hamid, I. Hegazy, M. Aref, and M. Roushdy, "Studying the impact of dataset balancing on machine learning-based intrusion detection systems for iot," *International Journal of Intelligent Computing and Information Sciences*, vol. 24, no. 3, pp. 41–57, 2024.

[42] U. Rahardja, "Risk assessment, risk identification, and control in the process of steel smelting using the hiradc method," *APTISI Transactions on Management*, vol. 7, no. 3, pp. 261–272, 2023.

[43] S. Vijayalakshmi, S. Bose, G. Logeswari, and N. Maheswaran, "Smart parking: intelligent intrusion detection system in vanet enabled car parking system," *Automatika*, vol. 66, no. 2, pp. 281–299, 2025.

[44] K. Noor, A. L. Imoize, C.-T. Li, and C.-Y. Weng, "A review of machine learning and transfer learning strategies for intrusion detection systems in 5g and beyond," *Mathematics*, vol. 13, no. 7, p. 1088, 2025.

[45] OECD, *Evaluating, Updating and Monitoring Anti-Fraud Strategies: A Methodology*, ser. OECD Public Governance Reviews. Paris: OECD Publishing, 2026. [Online]. Available: https://doi.org/10.1787/4b442c1a-en

[46] K. Setaei, "Ontology-enhanced neuro-symbolic defense against adversarial attacks in iot-enabled cyber-physical systems: Experimental validation in smart campus infrastructure," *Scientific Journal of Research Studies in Future Computer Sciences*, vol. 2, no. 1, pp. 22–32, 2024.

[47] B. I. Farhan and A. D. Jasim, "Survey of intrusion detection using deep learning in the internetof things," *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 1, p. 9, 2022.

[48] S. N. Ashraf, S. Manickam, S. S. Zia, A. A. Abro, M. Obaidat, M. Uddin, M. Abdelhaq, and R. Alsaqour, "Iot empowered smart cybersecurity framework for intrusion detection in internet of drones," *Scientific reports*, vol. 13, no. 1, p. 18422, 2023.

[49] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and R. Efendy, "Innovation and key benefits of business models in blockchain companies," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 24–35, 2023.

[50] K. Polin, T. Yigitcanlar, M. Limb, and T. Washington, "The making of smart campus: A review and conceptual framework," *Buildings*, vol. 13, no. 4, p. 891, 2023.

[51] R. Chaganti, A. Mourade, V. Ravi, N. Vemprala, A. Dua, and B. Bhushan, "A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things," *Sustainability*, vol. 14, no. 19, p. 12828, 2022.

[52] A. A. Laghari, A. A. Khan, A. Ksibi, F. Hajjej, N. Kryvinska, A. Almadhor, M. A. Mohamed, and S. Alsubai, "A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture," *Scientific Reports*, vol. 15, no. 1, p. 26843, 2025.

[53] L. Idouglid, S. Tkatek, K. Elfayq, and A. Guezzaz, "Next-gen security in iiot: integrating intrusion detection systems with machine learning for industry 4.0 resilience." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 14, no. 3, 2024.

[54] D. Robert, F. P. Oganda, A. Sutarman, W. Hidayat, and A. Fitriani, "Machine learning techniques for predicting the success of ai-enabled startups in the digital economy," *CORISINTA*, vol. 1, no. 1, pp. 61–69, 2024.

[55] N. Sahani, R. Zhu, J.-H. Cho, and C.-C. Liu, "Machine learning-based intrusion detection for smart grid computing: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 2, pp. 1–31, 2023.