Revolutionary Advances in Computing and Electronics (RACE): An International Journal
Volume 02, Issue 03, pp.11-26, 2026
ISSN (Online): 3107-8540

Received: 05/06/2026, Accepted: 05/08/2026

A Temporal Deep Learning Framework for Multi-Class Intrusion Detection in Industrial IoT Networks

Hala Hayajneh, Qasem Abu Alhaija

Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid, Jordan

hahayajneh24@cit.just.edu.jo, q.abualhaija@psut.edu.jo

Abstract

The rapid proliferation of the Industrial Internet of Things (IIoT) has significantly expanded the cyberattack surface of connected industrial systems, creating an urgent need for intelligent, reliable intrusion detection mechanisms to safeguard edge computing environments. This paper proposes a deep learning-based Intrusion Detection System (IDS) that integrates Long Short-Term Memory (LSTM) networks with the Synthetic Minority Over-sampling Technique (SMOTE) to address the challenges of temporal traffic modelling and severe class imbalance in multi-class intrusion detection. The proposed framework employs sequential feature learning to capture temporal dependencies in IIoT network traffic while applying SMOTE exclusively to the training data to improve the representation of minority attack classes and prevent data leakage. Experimental evaluation on the Edge-IIoTset dataset, comprising more than 15 traffic classes, demonstrates that the proposed model achieves training accuracy of 86.24% and validation accuracy of 74.60%, with balanced precision, recall, and F1-score of 0.76, 0.74, and 0.75, respectively. These findings demonstrate that combining temporal feature learning with effective data balancing provides a practical and scalable approach for enhancing multi-class intrusion detection and supporting real-time cybersecurity monitoring in Industrial IoT environments.

Keywords: *Industrial Internet of Things (IIoT), Intrusion Detection System (IDS), Long Short-Term Memory (LSTM), SMOTE, Deep Learning, Cybersecurity.*

1. Introduction

In the contemporary era, the vast majority of objects were not connected to the computer network, but this is changing significantly and rapidly. Entities that were not connected to the internet in the past are now Capable of engaging with other people and entities. Let’s hypothesise about our current global scale, where everything we can think of is connected to the internet and communicates with devices and people to improve our lives by enabling emerging functionalities. The Internet of Things era began between 2008 and 2009. During this period, the number of internet-connected devices exceeded the world's population. With more "things" connected to the internet than there are people in the world, a new era began: the Internet of Things. The term "Internet of Things" was coined by Kevin Ashton [1]. While working at Procter & Gamble in 1999, Kevin used this term to describe a new concept for connecting the company's supply chain to the internet. Kevin later explained that the Internet of Things currently includes adding senses to computers. Previously, computers relied on humans to input data and knowledge through barcodes.

*Corresponding author: Qasem Abu Alhaija, Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid, Jordan. (q.abualhaija@psut.edu.jo)

The Internet of Things is altering this paradigm; in the 21st century, computers are becoming more than just "sensing" things.

A. Internet of Things (IoT)-Overview

The world today is witnessing significant technological advancements and a massive transformation across the technology domain. We know this paradigm shift as the Internet of Things (IoT). Through IoT, we enable devices to sense and control the physical world by making things highly intelligent and connecting them via a cognitive network. We strive to achieve greater integration between the physical world and computers, and to make this integration more robust. The Internet of Things (IoT) is a vast, multifaceted world that may initially seem a bit complex due to the numerous protocols and components it encompasses. While the IoT ecosystem delivers numerous benefits in automation and productivity, it also presents new challenges related to the sheer volume of data that needs to be processed and the scaling up of countless devices. Kevin Ashton coined the term "Internet of Things," explaining that, in our time, it incorporates sensors connected to computers [1]. In this Internet network architecture, we provide a detailed overview of the Internet of Things (IoT) gateway or device. Figure 1 shows the key peripherals for transmitting and receiving data related to operation and sensing. The figure illustrates a comprehensive architecture for multi-radio IoT devices or gateways, with diverse communication components and their interoperability. The IoT device draws power from communication units that transmit data over various wireless access technologies. These communication units comprise baseband chips, RF front-end units, RF chips, and antennas [2]. Figure 2 shows the diverse applications of the IoT ecosystem.

B. Technical Implementation of IoT

People envision autonomous vehicles, or self-driving cars, and this long-term vision is becoming a tangible reality with well-known projects like Google's self-driving car project. For us, the Internet of Things (IoT) is also a key element in implementing an integrated transportation infrastructure. This will enable self-driving vehicles to interact more effectively with the surrounding transportation system by leveraging two-way data exchange, providing passengers with vital information. In cars, we have essential sensors that monitor oil pressure, engine temperature, and tyre pressure, providing data on the car's basic functions. Let’s take another example: in factories, the equipment on the factory floor is becoming smarter at sending and receiving massive amounts of diagnostic data and information instantly [1]. Let's take another example: In factories, the equipment on the factory floor has become more intelligent in its capability to send and receive vast quantities of diagnostic and informational data Instantaneous. More devices that support the Internet Protocol are being added to factories, such as smart diagnostic devices, video cameras, and other manufacturing equipment [1]. IoT is entering the realm of smart buildings as buildings have become increasingly complex over the past few decades, with their systems overlapping and forming intricate intersections among mechanical, structural, electrical, and information technology components. However, over time, the operational networks that support the building environment have evolved into sophisticated systems. To exemplify this, many buildings are now deploying sensors throughout to detect people. We will notice that these devices are usually actually video camera sensors or motion sensors [1]. Contrary to popular belief, the Internet of Things is not limited to connected machines and inanimate objects; we can also connect living beings, such as animals and insects, to the Internet [1].

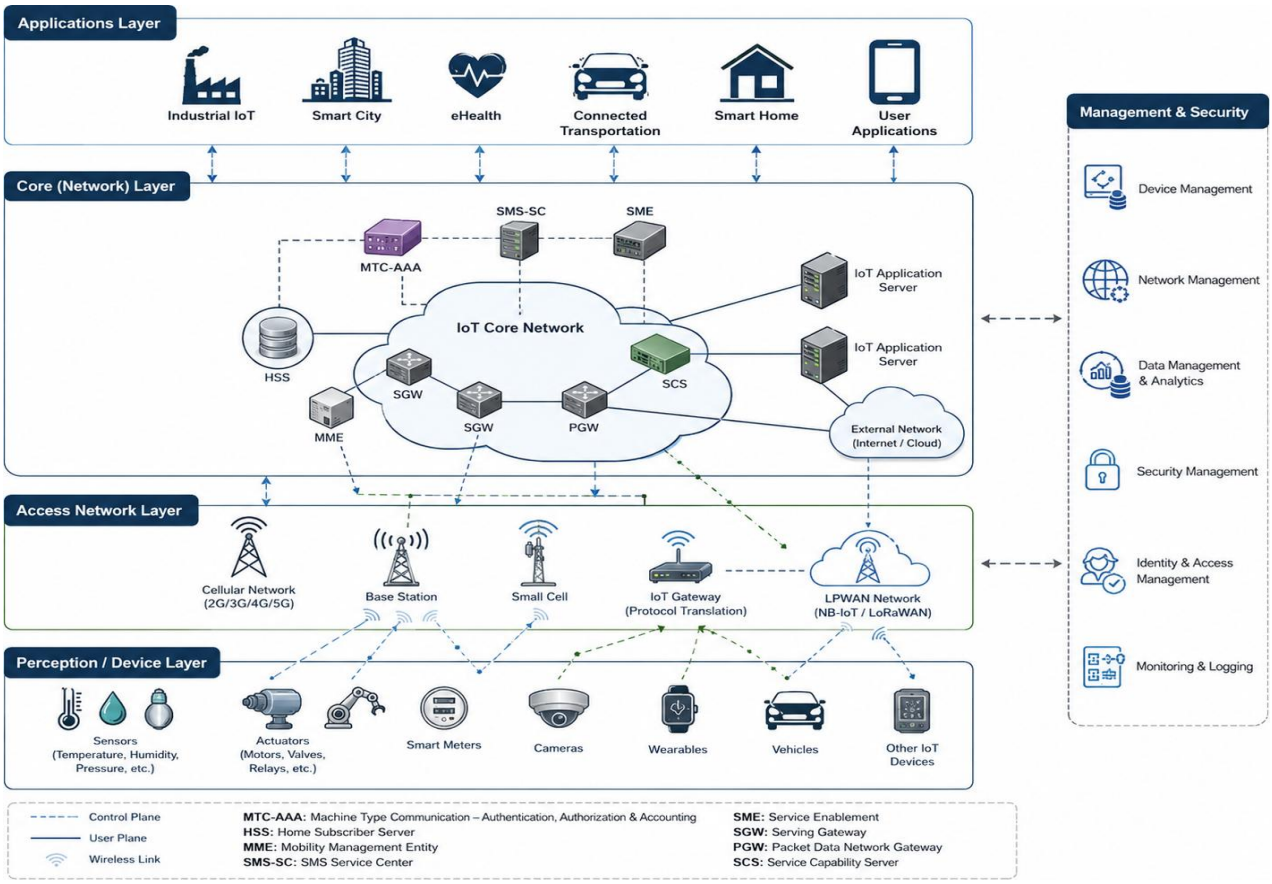


Figure 1. IoT Network Architecture.[2]

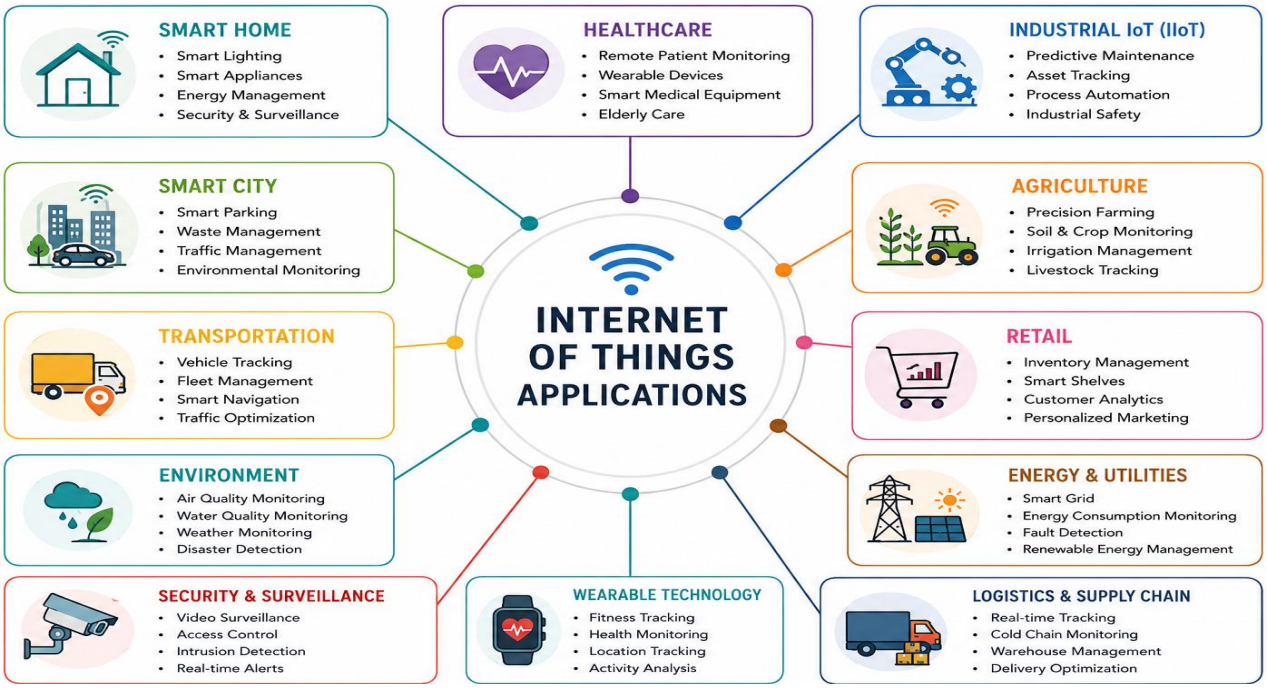


Figure. 2. IoT Applications. [3]

C. IoT Attacks

People often view IoT devices as easy targets for hackers. Known vulnerabilities are not merely software bugs; they are tools that attackers can exploit to turn these devices into platforms for large-scale cyberattacks. But why are these devices so technically vulnerable? The vulnerability of IoT devices is not due to a single cause, but rather to a combination of structural and technical factors.

1) **Attack Area:** IoT devices have several drawbacks, such as low resource consumption and processing speed. This results in a lack of necessary security features to protect against attacks.[4]
2) **Device Diversity:** IoT devices differ from one another in their operating systems, network connectivity, and design. Consequently, the adopted security measures are more complex, thereby making some devices highly vulnerable to attacks.[4]
3) **Physical Impact:** We humans use IoT devices in essential systems for daily life, such as healthcare devices. Therefore, any cyberattack on these devices could have serious material consequences for us in the future.[4]
4) **Legacy Devices:** IoT devices have a longer lifespan, resulting in a massive number of older devices connected and in use. These older devices cannot receive security or software updates, making them more vulnerable to breaches.[4]

D. Problem Statement

There are many research gaps, such as the inability of current intrusion detection systems to effectively distinguish between normal operational fluctuations and low-frequency attacks, including distributed denial-of-service (DDoS), reconnaissance, and man-in-the-middle (MitM) attacks [11]. Unlike existing IDS approaches that rely on static feature learning, this work leverages temporal sequence modelling and data balancing to improve the detection of rare IIoT attacks. Table 1 summarizes the fundamental differences between IoT and traditional IT systems from a cybersecurity perspective. Unlike conventional IT environments, IoT systems are characterized by resource-constrained devices, heterogeneous architectures, and direct interactions with the physical world, making them more vulnerable to cyber threats and increasing the complexity of implementing effective security mechanisms.

Table 1. Illustrates the differences between IoT and IT attacks.

Category	IOT Attacks	IT Attacks
Attack Surface	Restricted Resources, greater vulnerability	Strong security, lower vulnerability
Diversity of devices	Complicated security	Standardized
Ramifications	Harmful physical consequences	Information theft
Outdated hardware	Outed Devices	Lesser Risk

E. Main Contributions

The main contributions of this work are summarized as follows:

- We propose a temporal-aware intrusion detection framework for Industrial IoT using deep LSTM networks capable of learning sequential attack behavior.
- We integrate SMOTE only during the training phase to address severe class imbalance while preventing data leakage.
- We evaluate the proposed framework on the Edge-IIoTset dataset containing more than fifteen attack categories under a multi-class classification setting.
- We demonstrate that temporal feature learning improves the detection of minority attack classes compared with conventional feature-based learning approaches.
- The proposed framework provides a lightweight architecture suitable for real-time IIoT edge security monitoring.

2. Literature Review

Recent advancements in data-driven modeling and intelligent systems have significantly enhanced predictive analytics and cybersecurity applications, particularly within Internet of Things (IoT) and Industrial IoT (IIoT) environments. There have been many works on integrating artificial intelligence techniques into optimization frameworks. For example, W. Chen et al. [5] proposed a hybrid of artificial neural networks (ANN) and Data Envelopment Analysis (DEA) to measure and predict the country's performance in international sports tournaments. The GEFF model takes demographic and economic indicators, such as population and GDP, as inputs and medal count as outputs. ANN part predicted with high accuracy and very little deviation from actual results. Furthermore, the study suggested a potential combination of IoT and IIoT technologies to gather real-time data from smart infrastructures, thereby improving prediction accuracy and system responsiveness.

Various machine learning and deep learning techniques have been explored in cybersecurity for detecting Distributed Denial-of-Service (DDoS) attacks in IoT environments. Obetta and Moldovan [6] conducted a comparative analysis of a new urban IoT dataset using Random Forest (RF), Deep Neural Network (DNN), Autoencoder (AEN), and Feedforward Neural Network (FNN). The results showed that the DNN model achieved a training accuracy of 95.9% and a testing accuracy of 88.6%. Besides these Islam et al. [7] also used different classification models such as Support Vector Machine (SVM), K-Nearest Neighbors (KNN) and Random Forest (RF) to enhance the detection of DDoS. Their results revealed the best performance of SVM with 99.5% accuracy, followed by KNN (97.5%) and RF (98.74%). This shows that classical machine learning approaches can be useful when properly optimized.

In industrial IoT applications, Abubakar et al. [8] introduced a unified framework that integrates TinyML, embedded systems, and federated learning (FL) with advanced machine learning models, including RF, SVM, Decision Trees (DT), and Elastic Net. Their results showed that decentralised Random Forest models achieved up to 97.9% accuracy in monitoring equipment status, highlighting the potential of lightweight, distributed intelligence in industrial environments. Awad et al. [9] developed an intrusion detection system tailored for IIoT environments using both machine learning and deep learning techniques. Utilizing the Edge-IIoTset dataset, their system was designed to detect 14 different attack types. Experimental results demonstrated exceptionally high performance, with Decision Tree models achieving up to 100% accuracy, emphasizing the effectiveness of ML-based IDS solutions in structured datasets.

Advances in deep learning architectures for cybersecurity have enhanced data processing capabilities. For example, the AMNet model proposed in [10] improves the image super-resolution

by addressing the limitations of the traditional Multi-Scale Residual Networks (MSRN). The model is equipped with an Adaptive Multi-branch Block (AMB) to reduce the computational complexity and an Adaptive Feature Fusion Block (AFFB) to improve the feature weighting. Experiments demonstrate AMNet is more efficient and achieves better reconstruction quality than the state-of-the-art methods. However, there are still several gaps in IoT systems with data science despite these advances. Cao [12] gave a comprehensive review of data science, but not on the applications of IoT. On the contrary, Tsai et al. [13] conducted a comprehensive review of data mining techniques in IoT and emphasised the importance of extracting meaningful patterns from large volumes of sensor data. Gubbi et al. [14] also proposed IoT architectures and the importance of data-driven intelligence for enabling smart environments and real-time analytics.

Xu et al. [15] discussed the role of IoT in industrial environments from an architectural perspective, addressing system design, services, and communication models. Similarly, Atzori et al. [16] presented a seminal survey of IoT architectures, protocols and enabling technologies, which has become a fundamental reference in the field. However, while these studies cover infrastructure and system-level aspects, they have limited integration with data science. Chen et al. [17] studied big data analytics techniques, focusing on their utility in the presence of large-scale, heterogeneous data, which is highly relevant to IoT ecosystems. Li et al. [18] studied IoT applications and data management challenges such as scalability, interoperability and data processing.

Recently, the research has been focused on intelligent and resilient security mechanisms for IIoT and IoT environments. Abu Al-Haija and Tamimi [19] provide a comprehensive survey of adversarial reinforcement learning for IoT intrusion detection. They discussed the potential benefits and challenges of applying reinforcement learning methods to help IDS adapt more effectively to evolving cyber threats. Another work by Aljundi et al. [20] introduced an AI-based Physical Unclonable Function (PUF) authentication framework for MQTT-enabled IoT systems. They proposed using machine learning and multi-factor authentication to strengthen device authentication and communication security. Furthermore, Al Tamimi et al. [21] proposed a blockchain-based protocol with an intrusion response mechanism to secure distributed IoT systems. They also proved the effectiveness of decentralised trust management and automatic response to attacks. The papers underscore the growing importance of intelligent intrusion detection, secure authentication, and blockchain-based defence mechanisms in securing next-generation IoT and IIoT.

Although recent studies have shown significant progress in IoT and IIoT security through machine learning, deep learning, blockchain, and intelligent authentication mechanisms [19]- [21], some research challenges remain. Most existing intrusion detection methods rely on static feature representations that are ineffective at capturing temporal dependencies in sequential network traffic. Furthermore, the detection performance of minority attack classes is still degraded by severe class imbalance in realistic IIoT environments. Driven by these limitations, this work proposes a time-aware deep LSTM framework, along with SMOTE-based data balancing, to enhance multi-class intrusion detection performance and the detection of both common and rare cyberattacks. In general, studies have treated IoT infrastructure and data analytics as distinct entities, even though there has been substantial progress in applying machine learning and deep learning techniques to the IoT and IIoT domains. There is still a clear need for comprehensive frameworks that tightly couple data science methodologies with real-time IoT data processing and cybersecurity applications, paving the way for more adaptive, scalable and intelligent systems. To

better compare existing approaches, we summarise key studies in Table II by technique, application domain, strengths, and limitations. As shown in Table 2, existing works are either concentrated on high-accuracy detection, compromising scalability and real-time constraints, or on architectural frameworks that are not integrated with advanced data analytics. Moreover, little attention has been paid to unified frameworks that integrate IoT data processing, machine learning, and cybersecurity intelligence.

Table 2. Comparison of Related Works in IoT, IIoT, and Cybersecurity Analytics

Ref.	Study / Authors	Domain	Techniques Used	Dataset / Environment	Key Strengths	Limitations
[5]	W. Chen et al.	Sports Analytics	ANN + DEA (GEFF Model)	Olympic datasets	High prediction accuracy; hybrid modeling	Limited to structured inputs; not real-time IoT
[6]	Obetta et al.	IoT Security	RF, DNN, AEN, FNN	Urban IoT dataset	Comparative evaluation: strong DNN performance	Moderate generalization; limited real-world noise
[7]	Islam et al.	DDoS Detection	SVM, KNN, RF	Network traffic datasets	High accuracy (SVM 99.5%); efficient models	Lacks scalability and real-time deployment
[8]	Abubakar et al.	IIoT / Industry	TinyML, FL, RF, SVM, DT	Industrial environments	Decentralized learning; energy-efficient models	Limited security evaluation
[9]	Awad et al.	IIoT Security	ML + DL (DT, NN)	Edge-IIoTset	Very high accuracy (≈100%); multi-attack detection	Possible overfitting; dataset dependency
[10]	AMNet Study	Image Processing	Deep Learning (AMB, AFFB)	Image datasets	High efficiency and resolution improvement	Not applicable to cybersecurity
[13]	Tsai et al.	IoT Data Mining	Data mining techniques	General IoT	Comprehensive analytics overview	Lacks implementation frameworks
[14]	Gubbi et al.	IoT Systems	Architecture + data-driven models	Conceptual framework	Strong IoT vision and architecture	Limited practical validation

[15]	Xu et al.	IIoT Architecture	Industrial IoT frameworks	Industrial systems	Focus on industrial applications	Limited AI/data science integration
[16]	Atzori et al.	IoT Architecture	Protocols and architectures	General IoT	Foundational reference	Outdated for modern AI-driven IoT
[17]	Chen et al.	Big Data	Big data analytics	General	Strong data processing foundation	Not IoT-specific
[18]	Li et al.	IoT Data Management	Data management techniques	IoT systems	Highlights scalability issues	Limited ML-based intelligence
[19]	Abu Al-Haija et al.	IoT Intrusion Detection	Adversarial Reinforcement Learning (Survey)	IoT IDS literature	Comprehensive review of adversarial RL techniques, challenges, and future research directions for adaptive IoT intrusion detection	Survey paper without experimental validation
[20]	Aljundi et al.	IoT Authentication	AI, PUF, Multi-Factor Authentication	MQTT-enabled IoT Systems	Lightweight and secure authentication framework with AI-assisted device verification	Focused on authentication rather than intrusion detection
[21]	Al Tamimi et al.	Distributed IoT Security	Blockchain-based Security Protocol with Integrated Intrusion Response	Distributed IoT Networks	Decentralized trust management, secure communication, and automated intrusion response	Does not incorporate temporal deep learning for traffic classification

Although previous studies report high detection accuracies, most rely on static feature learning or decision-tree-based classifiers. Few studies investigate temporal dependencies in industrial traffic while simultaneously addressing severe class imbalance. Furthermore, many reported results are obtained on balanced datasets that do not reflect practical IIoT deployments. These limitations motivate the proposed temporal learning framework.

3. Experimental Model and Results

The methodology of this study consists of five key stages for developing a reliable and effective intrusion detection system, as shown in Figure 3 below. In this paper, we propose a temporal-aware intrusion detection framework for the Industrial Internet of Things (IIoT) environments. The proposed framework combines data balancing and deep sequential learning to improve the ability to detect both frequent and rare cyberattacks.

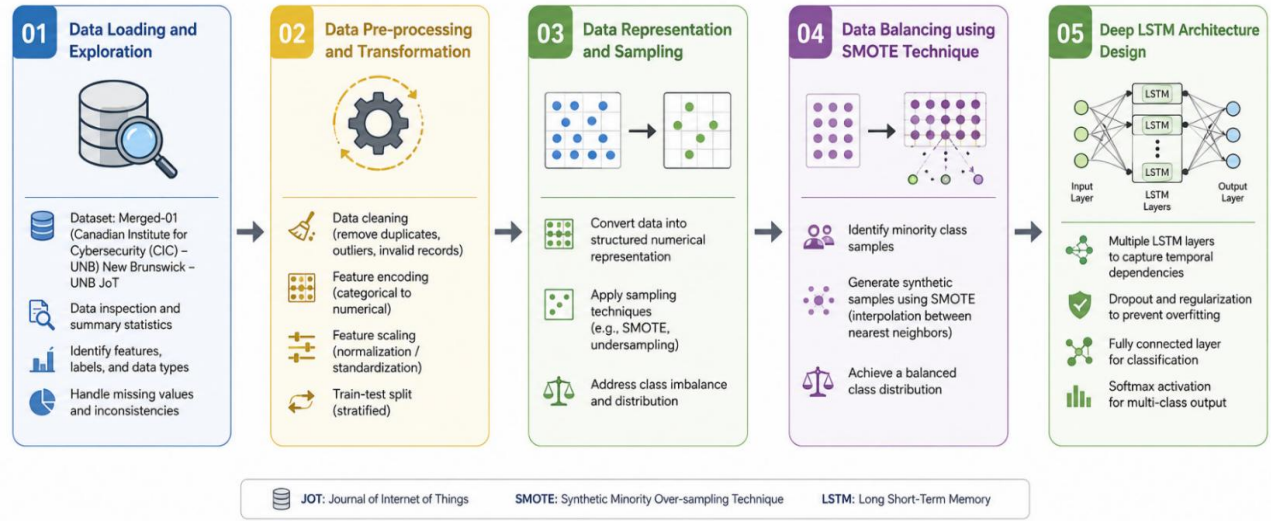


Figure 3. IIOT Methodology Workflow.

A. Dataset Description

The experiments were performed on a realistic Industrial Internet of Things (IIoT) cybersecurity dataset, namely, Edge-IIoTset (Merged-01), developed by the Canadian Institute for Cybersecurity (CIC). The dataset consists of 157,800 labelled network traffic samples and 61 extracted features. It supports multi-class intrusion detection with 15 classes: 14 attack categories and 1 normal traffic class. Making it suitable for evaluating deep learning models in realistic IIoT attack scenarios. Table 3 presents the characteristics of the Edge-IIoTset (Merged-01) dataset, including the total number of samples, extracted features, classification classes, and the distribution of normal and attack traffic.

Table 3. Summary of the Edge-IIoTset (Merged-01) dataset used for training and evaluating the proposed intrusion detection model.

Property	Value
Dataset	Edge-IIoTset (Merged-01)
Total Samples	**157,800**
Network Features	**61**
Classification Classes	**15** (14 attack classes + 1 Normal)

Normal Samples	16,214
Attack Samples	141,586

B. Data Preprocessing

Data preprocessing was performed to ensure consistency and improve model performance:

- **Label Encoding:** Attack categories were converted into numerical labels.
- **Feature Scaling:** The StandardScaler was applied to normalize feature distributions.
- **Missing Values Handling:** Any incomplete records were removed or imputed.

C. Data Balancing using SMOTE

To solve the class imbalance, we used the Synthetic Minority Over-sampling Technique (SMOTE) only on the training dataset to prevent data leakage. This step helps the model learn rare attack patterns, such as SQL injection and backdoors. Figure 4 illustrates the attack distribution before and after SMOTE. The original dataset exhibited substantial imbalance, with several minority classes containing significantly fewer samples than dominant attack categories. After applying SMOTE only to the training data, the class distribution became considerably more balanced, allowing the LSTM model to learn representative temporal patterns across all attack classes.

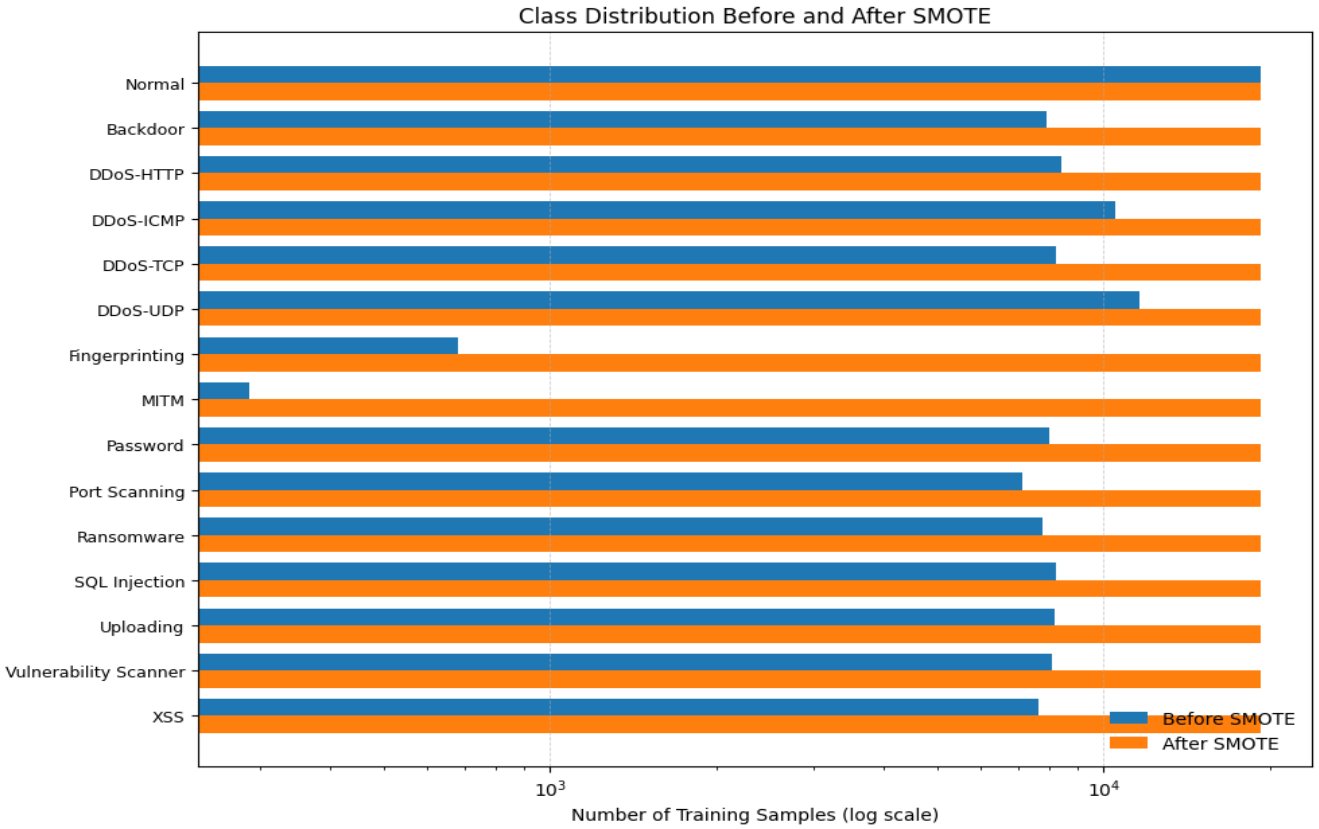


Figure 4. Class distribution of the Edge-IIoTset training subset before and after applying SMOTE.

D. Temporal Feature Modeling using LSTM

A deep learning architecture based on Long Short-Term Memory (LSTM) networks was designed to capture temporal dependencies in network traffic. The proposed model consists of:

- **Input Layer:** Sequential network traffic features
- **LSTM Layer 1:** 128 units (captures long-term dependencies)
- **LSTM Layer 2:** 64 units (refines temporal features)
- **Global Max Pooling Layer:** Extracts dominant temporal features
- **Dropout Layer (0.3):** Reduces overfitting
- **Batch Normalization:** Stabilizes training
- **Dense Layer:** Fully connected classification layer
- **Output Layer:** Softmax activation for multi-class classification

The model was trained using the Adam optimizer with categorical cross-entropy loss. As illustrated in Figure 5, the proposed deep LSTM architecture processes sequential IIoT traffic through two stacked LSTM layers containing 128 and 64 hidden units, respectively. Batch normalization is applied between the recurrent layers to stabilize training, while global max pooling extracts the most informative temporal features from the input sequence. A dropout layer is then used to reduce overfitting, followed by a dense classification layer and a Softmax output layer that produces the final probabilities for the 15 traffic classes.

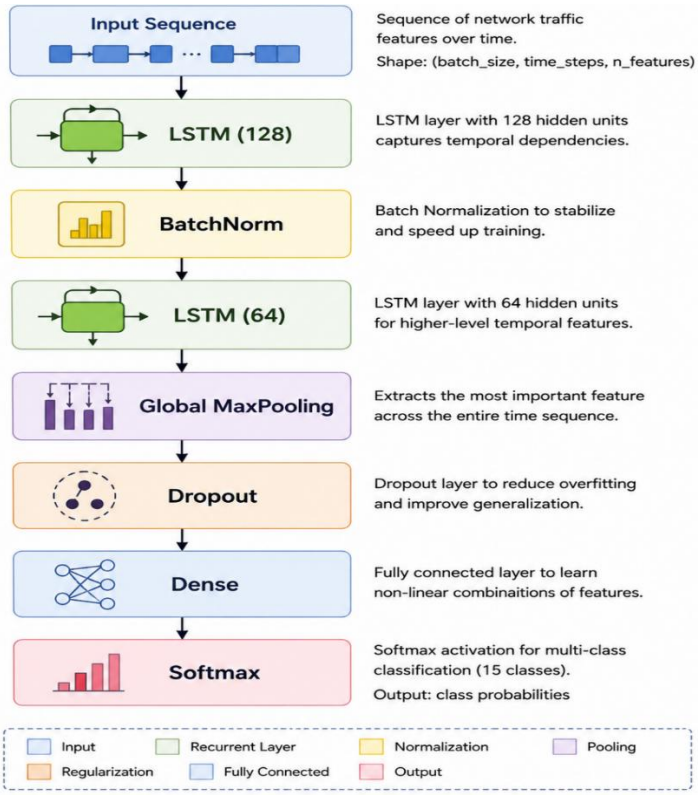


Figure 5. Proposed deep LSTM architecture for temporal feature learning and multi-class intrusion detection in IIoT networks.

E. Training Configuration

The proposed deep LSTM model was trained using the hyperparameter configuration summarized in Table 4. The model employs the Adam optimizer with a learning rate of 0.001 and categorical cross-entropy loss. Training was performed for 50 epochs with a batch size of 64, and a dropout rate of 0.3 to improve generalization. A fixed random seed of 42 was used to ensure the reproducibility of the experimental results.

Table 4. Hyperparameter settings used for training the proposed deep LSTM-based intrusion detection model.

Parameter	**Value**
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Epochs	50
Dropout	0.3
Loss	Cross Entropy
Activation	Softmax
Random Seed	42

F. Experimental Results

The experimental results showed that the proposed Deep LSTM model achieves high throughput in classifying 15 different types of cyber-attacks. The results proved a training accuracy of 86.24% and a verification accuracy of 74.6% in overall. The interoperability of SMOTE technology improved the detection of less common categories, such as SQL injection and backdoor attacks, which are often ignored in imbalanced datasets. The Global MaxPooling layer helped the model efficiently learn the most important features of malicious traffic. The minimum loss of 0.29 indicates very good confidence in the classification process. The data makes this approach applicable for real-time security monitoring in industrial edge computing environments for IIoT. Table 5 summarizes the overall performance of the proposed deep LSTM-based intrusion detection model on the Edge-IIoTset dataset. The model achieved a training accuracy of 86.24% and a validation accuracy of 74.60%, with corresponding precision, recall, and F1-score values of 0.76, 0.74, and 0.75, respectively. Furthermore, the relatively low training and validation loss values indicate stable convergence, demonstrating the effectiveness of the proposed temporal learning framework for multi-class intrusion detection in IIoT environments despite the inherent challenges posed by imbalanced attack distributions.

Table 5. Final Performance Metrics of the Deep LSTM Model on Edge-IIoTest.

Metric	Value
Training Accuracy	86.24%
Validation Accuracy	74.60%
Precision	0.76
Recall	0.74
F1-score	0.75
Training Loss	0.296
Validation Loss	0.421

Among all attack categories, minority attacks benefited most from SMOTE augmentation, whereas majority attack categories maintained stable detection performance. The LSTM network successfully captured temporal dependencies within sequential network traffic, resulting in improved robustness despite severe dataset imbalance. Also, Figure 6 shows the training and validation accuracy. Training accuracy increases steadily to about 86%, but validation accuracy falls to about 74.6%. The two curves converge, indicating that the model successfully learned the underlying patterns of industrial IoT attacks without much overfitting.

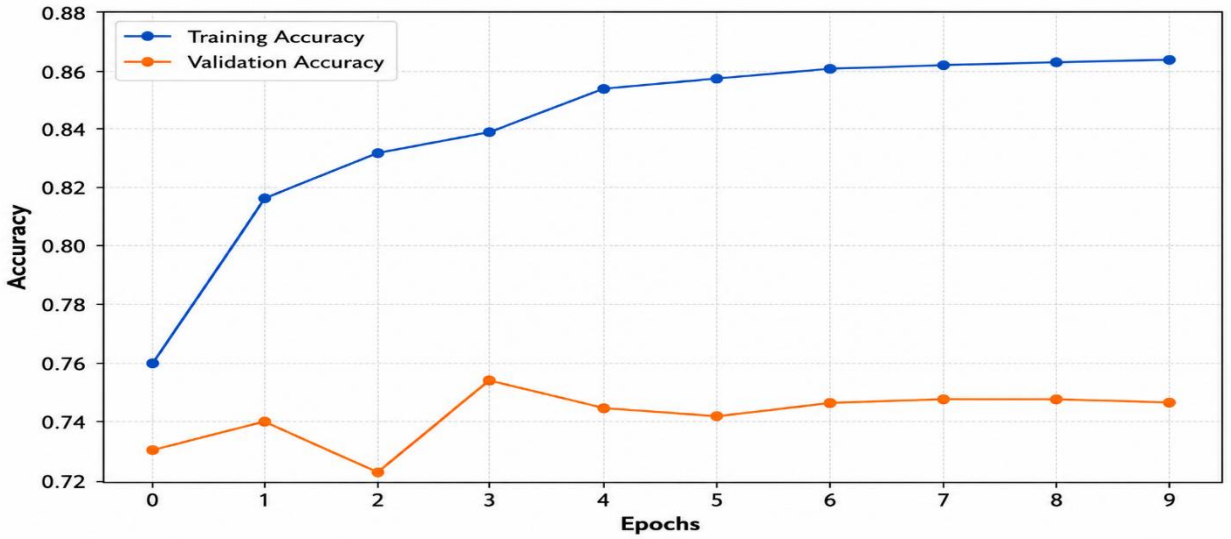


Figure 6. Training vs Validation Accuracy over Epochs in IIOT.

The results show that the proposed LSTM-based model effectively captures temporal patterns in IIoT traffic and achieves strong classification performance across multiple attack categories. The combination of SMOTE enhances the detection of minority classes, which are often overlooked in imbalanced datasets. However, the gap between training and validation accuracy indicates moderate overfitting, suggesting that additional optimization (e.g., regularization or hybrid models) could improve generalization. The proposed LSTM-based approach shows a better

ability to model the temporal dependencies of IIoT traffic compared with traditional machine learning models, especially in detecting low-frequency attack behaviours. Although the proposed model achieves lower overall accuracy than several existing approaches, it focuses on a considerably more challenging multi-class setting with temporal sequence learning and class imbalance mitigation. Unlike decision-tree models, the proposed framework explicitly captures sequential dependencies in IIoT traffic.

Table 6 compares the proposed deep LSTM-based intrusion detection framework with representative state-of-the-art approaches for IIoT and IoT intrusion detection. Although several existing methods report higher classification accuracies, many rely on conventional machine learning models, balanced datasets, or different experimental settings. In contrast, the proposed framework focuses on learning temporal features using stacked LSTM layers and combining them with SMOTE-based class balancing to address the challenges of multi-class intrusion detection in highly imbalanced IIoT environments. These results demonstrate the effectiveness of the proposed approach and highlight opportunities for further performance improvements through advanced architectures and optimisation techniques. Compared with traditional machine learning classifiers, LSTM can model temporal correlations between consecutive network packets. This capability becomes particularly important for detecting stealthy, low-rate attacks whose malicious behaviour only becomes evident over multiple time steps. The integration of SMOTE further improves the learning of minority attack classes without introducing data leakage, since oversampling is applied exclusively to the training set.

Table 6. Comparison of the proposed model with representative state-of-the-art IIoT intrusion detection methods.

Study	Dataset	Model	Accuracy
Awad et al.	Edge-IIoTset	DT	100
Islam et al.	CIC	SVM	99.5
Obetta	Urban IoT	DNN	88.6
Proposed	Edge-IIoTset	LSTM	74.6

4. Conclusions

Despite encouraging results, several limitations remain. First, only a single deep learning architecture was evaluated. Second, experiments were conducted on one public dataset without cross-dataset validation. Third, computational latency on embedded edge hardware was not investigated. These limitations provide directions for future work. This work proposed a specialized Intrusion Detection System (IDS) for Industrial Internet of Things (IIoT) environments, based on a deep Long Short-Term Memory (LSTM) architecture. To address class imbalance in cybersecurity telemetry data, the Synthetic Minority Over-sampling Technique (SMOTE) was strategically integrated into the data pre-processing workflow. Empirical results show that the proposed model can effectively detect sophisticated rare-event anomalies and high-volume cyberattacks in the dataset. The results, with training and validation accuracies of 86.24% and 74.6%, respectively, demonstrate the successful implementation of a combination of recurrent temporal modelling and advanced data balancing techniques to enhance the robustness of the IIoT

security infrastructure. Future work will investigate Transformer-based temporal models, explainable artificial intelligence techniques, federated learning for distributed IIoT environments, adversarial robustness against poisoning attacks, and lightweight deployment on resource-constrained edge devices.

5. References

[1] D.Hanes, G.Salgueiro, P.Grossetete, R. Barton, and J.Henry, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things.IN: Cisco Press,2017, Indianapolis.

[2] Z.Abbas and W.Yoon, "A Survey on Energy Conserving Mechanisms for the Internet of Things: Wireless Networking Aspects, “Sensors, vol.15, no.10, pp. 24818-24847, 2015.

[3] I. Al-Barazanchi, Z. A. Jaaz, H. R. Abdulshaheed, and H. H. Abbas, "Practical Application of IoT and its Implications on Existing Software," Journal of Advanced Research in Dynamical and Control Systems, vol. 10, no. 10, pp. 1546-1552, 2018.

[4] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges," Journal of Information Security and Applications, vol. 78, p. 103598, Nov. 2023, doi: 10.1016/j.jisa.2023.103598.

[5] W. Chen, F. Wang and M. Edwards, "Active Countermeasures for Email Fraud," 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), Delft, Netherlands, 2023, pp. 39-55, doi: 10.1109/EuroSP57164.2023.00012.

[6] A. K. B. Arnob, M. F. Mridha, M. Safran, M. Amiruzzaman, and M. R. Islam, "An Enhanced LSTM Approach for Detecting IoT-Based DDoS Attacks Using Honeypot Data," Jan. 2025.

[7] U. Islam et al., "Detection of Distributed Denial of Service (DDoS) Attacks in IoT-Based Monitoring System of Banking Sector Using Machine Learning Models," Sustainability, vol. 14, no. 14, p. 8374, Jul. 2022, doi: 10.3390/su14148374.

[8] M. Abubakar, A. Sattar, H. Manzoor, K. Farooq, and M. Yousif, "IIOT: An Infusion of Embedded Systems, TinyML, and Federated Learning in Industrial IoT," *Journal of Computing & Biomedical Informatics*, vol. 8, no. 2, pp. 1-14, Mar. 2025, doi: 10.56979/802/20245.

[9] O. F. Awad, L. R. Hazim, A. A. Jasim, and O. Ata, "Enhancing IIoT Security with Machine Learning and Deep Learning for Intrusion Detection," *Malaysian Journal of Computer Science*, vol. 37, no. 2, pp. 139–153, Apr. 2024, doi: 10.22452/mjcs.vol37no2.3.

[10] J. Ji, B. Zhong, and K. -K. Ma, "Single Image Super-Resolution Using Asynchronous Multi-Scale Network," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 11, pp. 4231-4244, Nov. 2021, doi: 10.1109/TCSVT.2021.3050186.

[11] M. A. Ferrag, L. Maglaras, S. T. Moschoyiannis, and H. Janicke, "Deep Learning for Cyber Security in Industrial IoT: A Survey," *IEEE Access*, vol. 8, pp. 104939-104966, 2020, doi: 10.1109/ACCESS.2020.2999659.

[12] Cao L. Data science: a comprehensive overview. ACM Computing Surveys (CSUR). 2017 Jun 29;50(3):1-42.

[13] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, “Data mining for Internet of Things: A survey,” IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 77–97, 2014.

[14] A. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[15] L. Da Xu, W. He, and S. Li, “Internet of Things in industries: A survey,” IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[16] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[17] M. Chen, S. Mao, and Y. Liu, “Big data: A survey,” Mobile Networks and Applications, vol. 19, no. 2, pp. 171–209, 2014.

[18] S. Li, L. Da Xu, and S. Zhao, “The Internet of Things: A survey,” Information Systems Frontiers, vol. 17, no. 2, pp. 243–259, 2015.

[19] Q. A. Al-Haija and S. A. Tamimi, “A State-of-the-Art Survey of Adversarial Reinforcement Learning for IoT Intrusion Detection,” Computers, Materials & Continua, vol. 87, no. 1, p. 2, 2026, doi: 10.32604/cmc.2025.073540.

[20] I. M. Aljundi, Q. Abu Al-Haija, and M. Al-Dala’ien, “AI-Driven PUF-Based Authentication for Secure MQTT-IoT Systems,” in Proc. 7th International Conference on Intelligent Autonomous Systems (ICoIAS), 2025, pp. 169–174, doi: 10.1109/ICoIAS69065.2025.00032.

[21] S. Al Tamimi, Q. A. Al-Haija, and A. AlShuaibi, “Securing Distributed IoT Systems: Blockchain-Based Protocol with Integrated Intrusion Response,” in Proc. 2025 IEEE 22nd International Conference on Mobile Ad-Hoc and Smart Systems (MASS), 2025, pp. 700–704, doi: 10.1109/MASS66014.2025.00114.