frontiers | Frontiers in Communications and Networks

TYPE Original Research
PUBLISHED 04 February 2025
DOI 10.3389/frcmn.2025.1416845

OPEN ACCESS

EDITED BY
Ioannis Krikidis,
University of Cyprus, Cyprus

REVIEWED BY
Muhammad Asghar Khan,
Hamdard University, Pakistan
Ajit Muzumdar,
National Institute of Technology, Goa, India
Kapila W. S. Palitharathna,
University of Cyprus, Cyprus

*CORRESPONDENCE
Ramiz Salama,
ramiz.salama@neu.edu.tr
Hitesh Mohapatra,
hiteshmahapatra@gmail.com

RECEIVED 13 April 2024
ACCEPTED 20 January 2025
PUBLISHED 04 February 2025

CITATION
Salama R, Mohapatra H, Tülbentçi T and Al-Turjman F (2025) Deep learning technology: enabling safe communication via the internet of things.
Front. Commun. Netw. 6:1416845.
doi: 10.3389/frcmn.2025.1416845

Deep learning technology: enabling safe communication via the internet of things

Ramiz Salama[1]*, Hitesh Mohapatra[2]*, Tuğşad Tülbentçi[3] and Fadi Al-Turjman[4]

[1]Department of Computer Engineering, AI and Robotics Institute, Research Center for AI and IoT, Near East University, Nicosia, Türkiye, [2]School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT) Deemed to be University, Bhubaneswar, Odisha, India, [3]Faculty of Architecture, Near East University, Nicosia, Türkiye, [4]Artificial Intelligence, Software, and Information Systems Engineering Departments, Research Center for AI and IoT, AI and Robotics Institute, Near East University, Nicosia, Türkiye

Introduction: The Internet of Things (IoT) is a new technology that connects billions of devices. Despite offering many advantages, the diversified architecture and wide connectivity of IoT make it vulnerable to various cyberattacks, potentially leading to data breaches and financial loss. Preventing such attacks on the IoT ecosystem is essential to ensuring its security.

Methods: This paper introduces a software-defined network (SDN)-enabled solution for vulnerability discovery in IoT systems, leveraging deep learning. Specifically, the Cuda-deep neural network (Cu-DNN), Cuda-bidirectional long short-term memory (Cu-BLSTM), and Cuda-gated recurrent unit (Cu-DNNGRU) classifiers are utilized for effective threat detection. The approach includes a 10-fold cross-validation process to ensure the impartiality of the findings. The most recent publicly available CICIDS2021 dataset was used to train the hybrid model.

Results: The proposed method achieves an impressive recall rate of 99.96% and an accuracy of 99.87%, demonstrating its effectiveness. The hybrid model was also compared to benchmark classifiers, including Cuda-Deep Neural Network, Cuda-Gated Recurrent Unit, and long short-term memory (Cu-DNNLSTM and Cu-GRULSTM).

Discussion: Our proposed technique outperforms existing classifiers based on various evaluation criteria such as F1-score, speed efficiency, accuracy, and precision. This shows the strength of the approach in threat detection and highlights the potential of combining SDN with deep learning for IoT vulnerability assessment.

KEYWORDS

Deep learning (DL), SDN, intrusion detection, IoT, Cuda-bidirectional, Long short-term memory

1 Introduction

The widespread use of IoT devices has transformed how we interact with our surroundings in recent years. These gadgets have enabled seamless automation and communication in a range of industries, including smart homes, healthcare, and transportation. However, preserving the security and privacy of data transported across

these networks is a considerable challenge, given their interdependence. Deep learning, a type of artificial intelligence (AI), has emerged as a powerful tool for increasing the effectiveness and security of IoT connections. Deep learning algorithms can spot abnormalities, anticipate potential threats, and respond quickly to security breaches by analyzing massive amounts of data using powerful neural networks. Because of the large quantity and variety of connected devices, traditional security methods may be insufficient in Internet of Things environments. This is why this feature is so vital. The objective of this paper is to provide a basic introduction of deep learning technology and how it might be applied to secure Internet of Things connections. And on this research provides a software-defined networks (SDN)-enabled solution for vulnerability discovery in Internet of Things systems based on deep learning. The most recent Cuda-deep neural network, Cuda-bidirectional long short-term memory (Cu-BLSTM), and Cuda-gated recurrent unit (Cu-DNNGRU) classifiers are used for successful threat detection. We will look at the fundamental ideas behind deep learning, the components that make up its architecture, and how these methods can be tailored to meet the unique challenges that come with IoT environments. We will also discuss specific use cases and real-world applications in which deep learning techniques have enhanced the security and reliability of Internet of Things networks. Deep learning technology has the ability to maintain safe and resilient communication infrastructures, and understanding its principles and capabilities will help IoT ecosystem players—from developers and engineers to policymakers and end users—appreciate this promise. Through this analysis, we seek to highlight deep learning's transformative impact on future IoT security and stimulate innovation in linked technologies. To uncover relevant information for "Deep Learning Technology: Enabling Safe Communication via the Internet of Things," look for research and articles that discuss the relationship between machine learning, specifically deep learning, and IoT security. The following are some important fields and similarly related topics:

- IoT Security Challenges: This segment of the literature focuses on the specific security difficulties that IoT devices provide, such as resource restrictions, heterogeneous networks, and the need for scalable security solutions. Research on Deep Learning for IoT Security In particular, researchers are looking into how deep learning technologies may improve IoT security, such as IoT device behavior analysis, anomaly detection, and intrusion detection. Edge computing and IoT publications are those that address edge computing paradigms for IoT security using deep learning models that can perform well on edge devices with limited resources. The work focused on developing secure communication protocols, such as encryption algorithms, authentication schemes, and key management, primarily for Internet of Things applications.
- Case Studies and Applications: Examples of practical usage or case studies in which deep learning technologies were successfully deployed to increase IoT system security.
- IoT Privacy and Data Protection: Discusses how deep learning may assist safeguard sensitive data and ensure privacy in IoT contexts.
- Cyber-Physical Systems Security: Because the Internet of Things commonly involves the interaction of cyber and physical systems, research utilizing deep learning methodologies to address security concerns in cyber-physical systems (CPS) is relevant.

The term IoT refers to an international network of individually addressable networked things. Its popularity has increased dramatically in recent years. IoT devices use several communication protocols and sensor functions. Because of their powerful CPUs, these devices can analyse data and provide services. Smart factories, smart ecosystems, smart health systems, smart cities, and automotive networks are just a few of the intelligent settings enabled by the IoT, a paradigm that connects millions of digitally aware devices (Tyagi, 2024). Although IoT has many advantages, it also poses a lot of security vulnerabilities. The constantly rising data of the IoT exposes IoT networks to a wide range of threats and assaults (Cherbal et al., 2024; Ahmed et al., 2024).The Internet of Things includes both heterogeneous and homogeneous networks, as well as networking devices that use a range of protocols. This suggests that faults may constitute an undetectable threat to both Internet of Things devices and the infrastructure. Cybersecurity employs a variety of approaches, such as distributed denial-of-service (DDoS) attacks, denial-of-service (DoS) assaults, and other malware types, to exploit different faults in the properties of these dynamic devices (Rehman et al., 2024). Almost 80% of specialists try to fix at least one security issue in a single day, and 60% of cybersecurity experts manage network security and operations for one or 2 h every day (Islam M. M. et al., 2024). There are further reported attacks that use deception and replay. A review of attack detection methods and industrial-level security measures may be found in (Meylani, 2024).

Protocol-obedient devices occur in a vast variety, and each one necessitates a distinct set of security procedures. These security measures, however, are insufficient considering how seamless IoT devices are. The overarching architecture of the Internet of Things is not yet safeguarded by a cohesive strategy. IoT security is complex and still requires a significant amount of security.

Today, an SDN-enabled architecture may simplify network management while also improving the dynamic and diverse environment of the Internet of Things. It provides platform support for underlying devices with limited resources, preventing security solutions from overloading and delivering effective and efficient detection without becoming outdated. One of the most effective ways to monitor SDN is to combine IDS with SDN (Peelam et al., 2024). Because AI is rapidly evolving and SDN is programmable, combining AI-based security solutions with SDN can improve security levels. Various AI techniques, including fuzzy logic, artificial neural networks (ANNs), decision trees, k-nearest neighbor, genetic algorithms, and naïve Bayesian algorithms, have been used to achieve accurate and optimal network traffic results (Hussain, 2024). Finally, our proposal for an SDN-enabled, deep-learning-based intrusion detection system is motivated by the need to provide a dependable and customizable architecture for threat detection in IoT devices.

The key novelties of the presented deep learning architecture lie in its application to IoT security through a hybrid model enabled by SDN for threat detection. By integrating advanced classifiers such as

Cuda-deep neural networks (Cu-DNN), Cuda-bidirectional long short-term memory (Cu-BLSTM), and Cuda-gated recurrent units (Cu-DNNGRU), the architecture excels at discovering vulnerabilities within highly connected IoT systems. Leveraging these novel deep learning mechanisms allows for both temporal and sequential data analysis, crucial for detecting complex cyberattacks. Additionally, the model's use of 10-fold cross-validation and training on the latest CICIDS2021 dataset ensures robust and unbiased threat detection with remarkable performance, achieving a 99.87% accuracy rate. These innovations are particularly beneficial for cybersecurity applications, providing real-time IoT threat monitoring with superior recall and precision over traditional models. The following are the paper's main contributions:

- A highly scalable and cost-effective deep learning-driven system with support for SDN is proposed for risk detection in Internet of Things scenarios.
- IoT devices employ Cu-DNNGRU and Cu-BLSTM classifiers to successfully identify threats.
- To allow for comparison of your results, the same data set is treated to Cu-GRULSTM and Cuda-Cu-DNNLSTM.
- We introduced a novel gating mechanism within the DNNGRU layer, allowing better control of gradient flow compared to standard GRU layers. Similarly, the Cu-BLSTM layer was modified to incorporate an optimized initialization technique, enhancing convergence speed.
- The proposed Cu-DNNGRU + Cu-BLSTM architecture was initially designed with a fixed number of nodes per layer, based on previous studies and initial experiments that demonstrated promising results. To explore the impact of network size on performance, the number of nodes in each layer is parameterized and analyzed
- The proposed method is validated against previous research to improve performance evaluation utilizing the CICIDS data set.
- Finally, 10-fold cross-validation is employed in this study to verify the objectivity of our findings.
- The assessment results show that the proposed method surpasses the others in terms of detection accuracy and computational complexity while also allowing for multiclass detection.

This paper has been organized as follows. Section 2 provides background information and references to relevant works. Section 3 contains additional information about the data set, the suggested strategy, and other aspects. Section 4 shows the experimental design and assessment measures. Section 5 has a full description of the findings. Section 6 marks the conclusion of the paper.

2 Related work

Network topologies like SDN will become more powerful in the future. It is divided into three layers: data, control, and application plane, each with its own set of APIs (northbound and southbound respectively). The SDN control plane can be extended into the SDN data plane to support a wide range of networks, including the internet of things, fog, and edge (Anwar et al., 2024). The control plane can be adjusted in a variety of ways to provide additional capabilities. It outlines the process of creating heterogeneous IoT nodes by connecting connected IoT devices to SDN controllers using Open-Flow switches. The SDN architecture's separation of the control and data planes promotes flexibility and usability. Furthermore, by offering a global perspective and central control functions, it simplifies the process of gathering network information (Paramesha et al., 2024). SDN enables dynamism, scalability, and centralized management. It is critical to improve control decision-making. It is recognized as a critical facilitator of flexible network solutions (Wang, 2024). The combination of SDN and IoT provides accurate network inspection to detect threats, malware, suspicious activity, and assaults. Therefore, SDN implies that the Internet of Things has a bright future. Academics have developed a range of methodologies and tactics to identify potential dangers in the body of existing research. The authors of (Uzoka et al., 2024) created an IDS for a network using a convolutional neural network (CNN).

Using Modbus-TCP network traffic data and long short-term memory (LSTM) analysis, the authors of (Hemamalini et al., 2024) suggested a collection of repeating families for Internet of Things attack and threat detection. In reference (Shafik, 2024), a recurrent neural network (RNN) is used to detect and categorize an assault. The authors compare both non-RNN and RNN approaches. The authors of (Zainuddin et al., 2024) used Wireshark to create Random Forests (RF) classifiers on a self-generated data set to detect DDoS attacks in the Internet of Things. DARPA data sets are used to build support vector machine (SVM) classifiers for intrusion detection systems (IDS) in SDNs (Ullah et al., 2024). The purpose of (Siddique et al., 2024) is to detect compromised intelligent devices in an Internet of Things network using a self-learning algorithm. They employed a Gated Recurrent Unit (GRU) classifier to detect hacked devices. The authors of (Hajlaoui et al., 2024) employed real-time traffic from Czech Technical University (CVUT) to detect botnets with LSTM. The authors of (Adil et al., 2024) found the IRC botnet using a combination of Bayesian, J48, and Naïve Bayes techniques. However, the authors did not specify how accurate their detection was. The inventors of (Vishwakarma et al., 2024) used LSTM to discriminate between attacks and legitimate communications. Multilayer ANN demonstrates a network's anomaly detection capacity (Wang et al., 2024).

According to the authors, the proposed technique detects DoS assaults 99.4% of the time. The authors of (Mu et al., 2024) used a deep model to detect pervasive attacks on the Internet of Things. The system was trained on the NSL-KDD data set and achieved an accuracy of 98.27% (Rejeb et al., 2024). Protects IoT infrastructure with a deep learning-driven SDN solution. Using the KDD99 data set, the scientists trained a Restricted Boltzmann Machine (RBM) that achieved 95% detection accuracy. The authors of (Hakiri et al., 2024) proposed using a flow-based detection technique in the SDN gateway to reduce and identify DoS attacks. However, this technique lacks efficiency analysis and performance statistics to back it up. In recent years, threat detection employing SDN in conjunction with AI-based approaches has shown promise (Van Hoang, 2024). The authors of (Singh and Dwivedi, 2024) proposed an intrusion detection system with training and testing accuracy of 96.22% and 92.73% respectively. Before developing an intrusion detection system (IDS) based on the most relevant security characteristics, the technique ranks the security features.

In (Wen et al., 2024), the authors used SVM, DNN, Naïve Bayes, and j48 classifiers to detect intrusions. The NSL-KDD dataset is used to train these classifiers. DNNs are considered to outperform other classifiers. The authors published a mechanism for packet level identification in botnet research and the Internet of Things (Zormati et al., 2024). The authors achieved 99.3% accuracy with CNN and RNN classifiers trained on the CTU-13 and ISOT datasets. For crossfire attacks, the authors of (Prasad and Thyagaraju, 2024) presented an SDN-based bio-inspired intrusion detection system with an accuracy of 80%. The authors of (Awad et al., 2024) used DeepDefence, a deep learning-based approach, to detect DDoS activity. Various deep learning methods are used to distinguish between harmful and secure communication. In addition, the authors employed LSTM, CNN, RNN, and Blocked-Recurrent-Unit-Neural-Network (GRU) to significantly reduce the rate of traditional techniques. The authors of (Khan et al., 2024) demonstrated that DL and SDN could prevent DDoS attacks with 99% and 98% accuracy, respectively, using the ISCX data set.

The authors of (Eusufzai et al., 2024) developed a source-based DDoS avoidance approach that obtained 98.88% accuracy on the Hogzilla data set. The authors of (Singh K. et al., 2024) offer a DDoS attack detection system that was developed using a layered deep learning methodology. The overall purpose of the intelligent network is to detect DDoS attacks with greater accuracy and success. The authors' progressive transfer learning model in (Casillo et al., 2024) outperformed earlier methods in dealing with DDoS threats. The authors of (Singh S. et al., 2024) created the DADMCNN framework, which employs deep learning to detect DDoS attacks. The authors also suggested an MC-CNN model that optimizes feature information for better recognition. The authors of (Abdi et al., 2024) described an autonomous learning technique based on SDN capabilities. Sophisticated learning strategies employ CNN, LSTM, and ANN to construct the learning model. In addition, the performance of the suggested model will be evaluated using the Mininet Wi-Fi emulation platform. To boost efficiency, the authors of (Owen, 2024) created a deep neural network model including LSTM and an attention mechanism. The model's accuracy was 96.2%. The authors of (Rahman et al., 2025) presented a hybrid technique for early DDoS detection based on CNNs and actual network data. The study employed over 319 million CDRs from Italia Telecom's free CDR data gathering. The results demonstrated that the projected framework can identify under attack cells with greater than 91% accuracy and normal precision.

TABLE 1 A review of the present literature.

Ref	Algorithm	Approach	Data set	D. Accuracy	Time complexity
Hemamalini et al. (2024)	LSTM	Cyber threats detection in a smart device using a deep learning model	Modbus-TCP	High	High
Shafik (2024)	RNN, LSTM, and GRU	Presented ML and DL techniques for intrusion detection	KDDCUP99	Low	N/A
Zainuddin et al. (2024)	RF	Presented a technique using ML classifier for DDoS attack detection in IoT	Self-generated data set by using Wireshark	High	N/A
Ullah et al. (2024)	SVM	Proposed an ML technique for IDS in SDN	DARPA	Medium	N/A
Siddique et al. (2024)	GRU	Proposed a self-learning distribution for identifying infected smart devices	Real Shelf Consumer IoT devices	Low	Medium
Siddique et al. (2024)	LSTM	Proposed a deep-learning-driven technique for botnet detection	CVUT real-time traffic	High	N/A
Adil et al. (2024)	Bayesian, J48, naïve Bayes	Presented a machine learning approach for IRC botnet detection	Dartmouth wireless network	Low	N/A
Vishwakarma et al. (2024)	LSTM-RNN	Propose an ML-driven approach to detected known and unknown threats	NSL-KDD	Low	N/A
Wang et al. (2024)	ANN	Presented ANN learning procedures for intrusion detection by using feed-forward and back learning algorithms	Internet packet traces	High	N/A
Mu et al. (2024)	Deep model	Presented a DL-driven scheme in IoT for the detection of DoS attacks.	NSL-KDD	Medium	Medium
Rejeb et al. (2024)	RBM	SDN-based DL technique for DoS attacks detection in intelligent devices	KDD99	Low	N/A
Hakiri et al. (2024)	RTS-DELM-CSIDS	Presented ML-based approach to develop an intrusion detection system	NSLKDD	Low	High
Wen et al. (2024)	DNN, SVM, J48 and Naive Bayes	Presented different algorithms to improve the learning rate of the algorithm, which can predict attacks in IDS	NSL-KDD	Low	N/A
Zormati et al. (2024)	CNN and RNN	The proposed methodology can detect botnets at the packet level	ISOT and CTU-13	Low	H

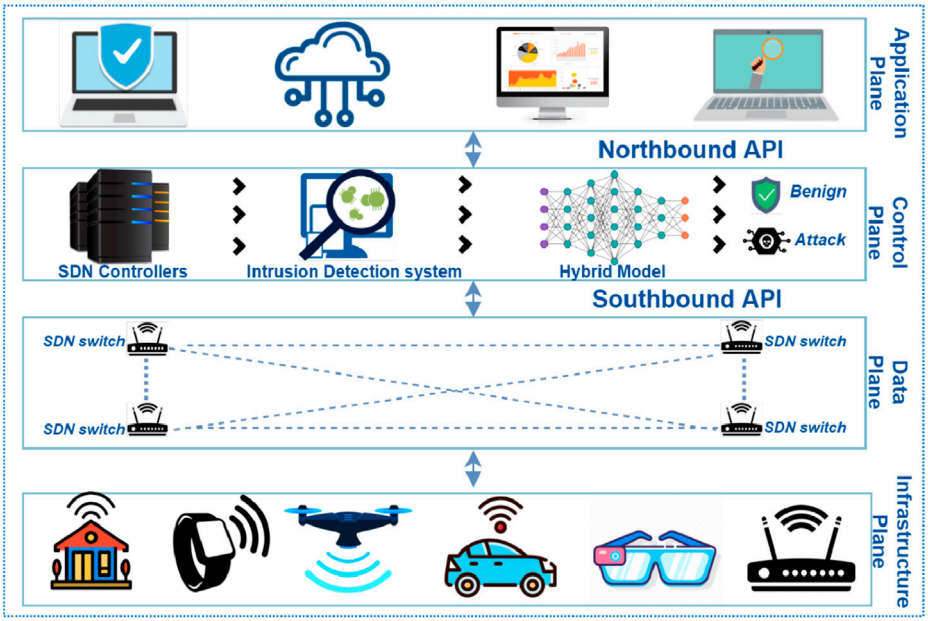

FIGURE 1
Proposal for network model.

Paper (Oliveira et al., 2024) describes a unique CNN architecture based on a multilayer convolution feature-fusion process and categorical crossentropy, which is used to the NSLKDD data set with loss. Based on experimental data, the suggested approach improves accuracy and reduces false alarms. The network design must be tuned for better detection results. Using CAIDA data, the authors of (Kaur et al., 2024) showed a CNN-based anomaly detection method for DDoS attacks. 87.35% of the time, the authors' anomaly detection system detected DDoS attacks. In conjunction with Snort IDS (Islam Z. et al., 2024), proposes a DL-based detection model for detecting IoT-based DDoS attacks. The authors evaluated their findings using a data set acquired from network-based traffic using a variety of methodologies and were able to achieve less than 4% FPR and 95% TPR detection accuracy. The BoT-IoT data set reported by the authors in (CheSuh et al., 2024) is novel and valuable. The data set was created using a realistic testbed and includes both real and simulated Internet of Things network traffic with various attack types. The authors of (Hasan et al., 2024) developed a data set called MQTT set, which is linked to the MQTT protocol. The writers use a range of machine learning methodologies. To validate the data set, they compared the outcomes of balanced and unbalanced data sets. Because there are so many benign disease records, the imbalanced data set compares quite well to other data sets. Finally, a collection of behavioral data from IoT tags, including both benign and (Kaleem et al., 2024) generate dangerous traffic. The data set was compiled from real-time traffic on a medium-sized network including 83 devices. Table 1 presents a detailed summary of the extant literature.

3 Proposed work and methodology

The purpose of this research project is to develop a hybrid deep learning-based intrusion detection solution for Internet of Things devices. This section discusses the suggested work method for the project, the suggested network model, preprocessing, data collecting, and the DL-driven hybrid framework. The motivation behind selecting Cu-DNNGRU and Cu-BLSTM layers in the proposed architecture lies in their combined strengths in handling sequential data and improving the model's efficiency. Firstly, the Gated Recurrent Unit (GRU), specifically in its CUDA-accelerated (Cu-DNNGRU) form, was chosen because of its ability to efficiently process long sequences without suffering from the vanishing gradient problem often encountered in traditional Recurrent Neural Networks (RNNs). GRU is computationally lighter than Long Short-Term Memory (LSTM) networks while still retaining the essential gating mechanisms for controlling the flow of information. This makes Cu-DNNGRU ideal for fast training and testing in resource-constrained environments, such as IoT systems, where timely detection of threats is critical. On the other hand, Bidirectional LSTM (BLSTM) layers were included to capture dependencies in both forward and backward directions in the data. IoT network traffic often exhibits complex temporal patterns, and using BLSTM allows the model to account for future as well as past dependencies, enhancing the model's ability to detect intricate patterns in cyberattacks. The combination of Cu-DNNGRU and Cu-BLSTM layers leverages the strengths of both techniques—GRU's efficiency and BLSTM's comprehensive sequence learning capability—creating a hybrid model that offers higher accuracy, robustness, and faster processing times compared to using either approach in isolation.

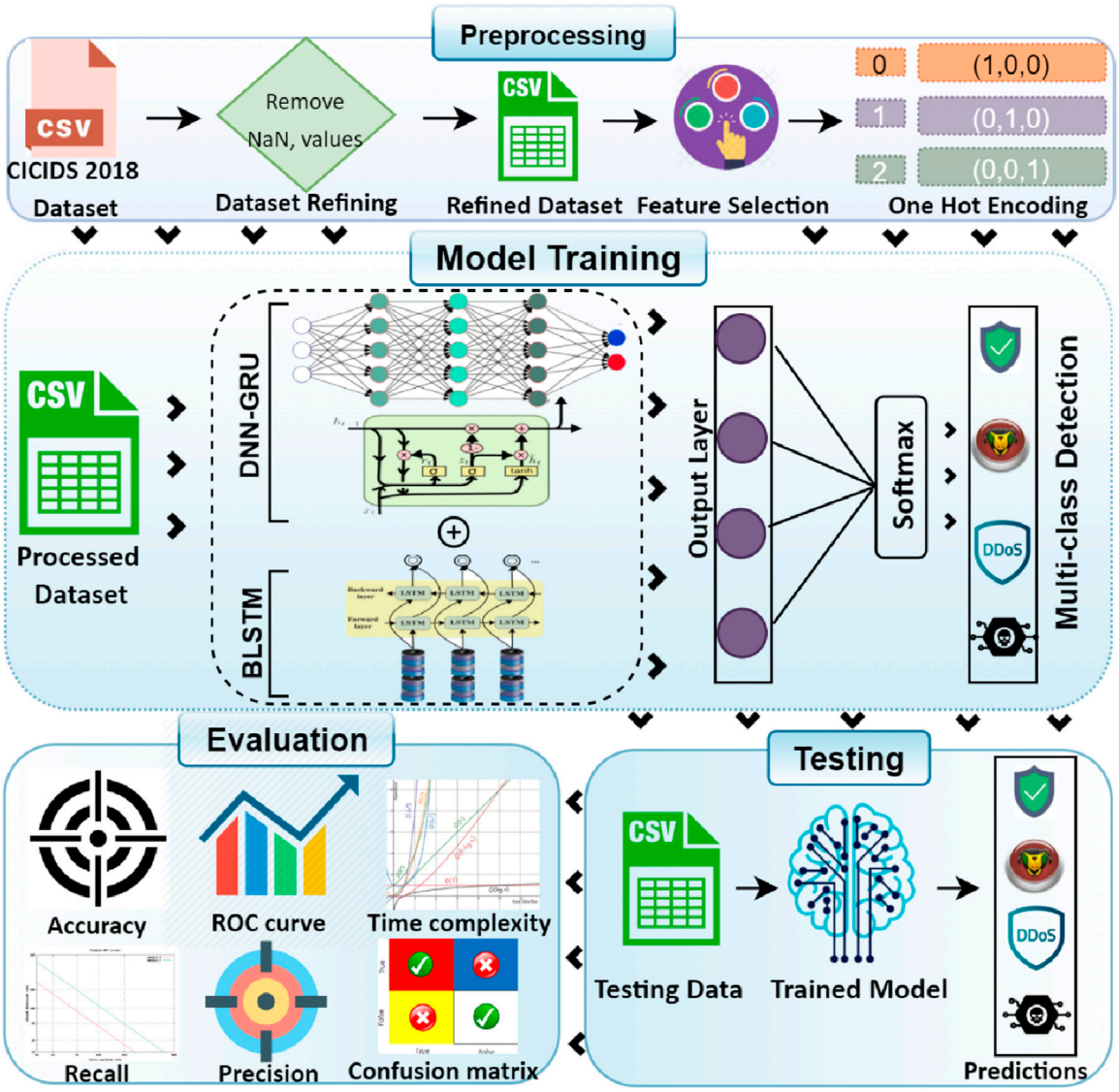

FIGURE 2
A framework for hybrid detection is presented.

3.1 Network model suggestion

The motivation for selecting an SDN-capable, DL-driven architecture lies in SDN's simplicity, flexibility, and ability to separate the control and data planes. This design offers programmability, a global network view, and centralized control, facilitating easier network data collection. The hybrid model (Cu-DNNGRU + Cu-BLSTM) is positioned on the control plane to efficiently handle the expansion and heterogeneity of IoT devices, ensuring effective threat detection while maintaining cost efficiency and scalability in diverse IoT environments. SDN has emerged as a useful technique for integrated network design in recent years. Because the control and data planes are kept separate, SDN design is simple and flexible. It also includes features like global network view and central control, which make collecting network data easier. We offer a hybrid, SDN-capable, DL-driven architecture for IoT intrusion and threat detection. Figure 1 shows the suggested hybrid model (Cu-DNNGRU + Cu-BLSTM) in the control plane. The hybrid threat detection model is located on the control plane for several reasons. First, SDN's data plane provides complete programmability and the expansion of Internet of Things devices. Second, it makes use of open-flow switches, which provide tools for managing heterogeneity in SDN controllers and Internet of Things devices. Third, the ability to use the key IoT devices without growing exhausted is what truly distinguishes the control plane in the IoT space. The combination of SDN and IoT integration allows for effective analysis of network data to detect threats, assaults, and unlawful conduct. The structure being offered is fairly priced and conveniently located. Furthermore, the data plane of SDN is comprised of a diverse set of IoT devices, including smart gadgets, sensors, and other wireless technologies.

TABLE 2 An explanation of hybrid algorithms.

Algorithm	Layers	AF	Neurons	LF	Optimizer	Batch-size	Epochs
Cu-DNNGRU + Cu-BLSTM	Cu-DNNGRU (1)	Relu	(200)	CC-E			
	Cu-BLSTM (1)	Relu	(100)	CC-E			
	Dropout	–	(0.3)	–	Adamax	32	05
	Output Layer (1)	Softmax	07				
	Dense (3)	–	(200,100,50)	–			
Cu-GRULSTM	GRU Layer (1)	Relu	(200)	CC-E			
	LSTM Layer (1)	Relu	(100)	CC-E			
	Dropout	–	(0.3)	–	Adamax	32	05
	Dense (3)	–	(200,100,50)	–			
	Output Layer (1)	Softmax	07				
Cu-DNNLSTM	DNN Layer (1)	Relu	(200)	CC-E			
	LSTM Layer (1)	Relu	(100)	CC-E			
	Dropout	–	(0.3)	–	Adamax	32	05
	Dense (3)	–	(200,100,50)	–			
	Output Layer (1)	Softmax	07				

TABLE 3 CICIDS2021, description of the data set.

Classes	Attack	Instances
Benign	–	69,654
Bot	–	2,977
Brute force	FTP	3,066
DDoS	Loic-UDP	3,015
	Hoic	3,037
Infiltration	–	3,043
Total		84,702

TABLE 4 Configuring an experiment.

CPU	7700, i7, 7th generation with 2.80 GHz processor
OS	Windows 10, 64 Bit
GPU	Nvidia GeForce 1060 6 GB
RAM	16 GB
Libraries	Pandas, TensorFlow, Numpy, Scikitlearn, and Keras
Language	Python with version 3.8

3.2 Dual-mode DL-powered detection system

The motivation for selecting the hybrid Cu-DNNGRU + Cu-BLSTM architecture is its ability to deliver a versatile, high-performing, and cost-effective solution for IoT intrusion detection. This design enhances malware and threat detection accuracy while minimizing false positives, leveraging deep learning models optimized with GPU processing. The use of different neuron layers and activation functions further refines the model's performance, ensuring efficient and scalable threat detection across various IoT environments. The authors present a hybrid solution to IoT intrusion detection powered by DL. IoT networks use Cu-DNNGRU + Cu-BLSTM, which is powered by DL, to identify threats. A versatile, powerful, and reasonably priced threat detection module is designed to identify threats across multiple categories. Figure 2 provides a detailed summary of the proposed paradigm. The proposed technique detects intrusions in Internet of Things environments by utilizing the CU-DNNGRU and Cu-BLSTM models for malware and advanced threat detection. The proposed model is tested and trained using hybrid approaches that reduce false positives (FP) while improving detection accuracy. The model consists of numerous layers; Cu-DNNGRU, for example, comprises 200 neurons in a single layer. Cu-BLSTM, on the other hand, has a single layer and 100 neurons. The activation function in the output layer is softmax, while the Relu function is used in the other levels. To achieve satisfactory findings, we ran trials throughout five epochs with batches of thirty-two participants each. We experimented with Cuda-enabled versions that use GPU processing to improve performance.

Furthermore, the proposed endeavor combined TensorFlow for Python's backend with the Keras framework. The comparison uses two classifiers: the Gated Recurrent Unit Long Short-Term Memory (GRU-LSTM) classifier, which has two layers: an LSTM layer with 100 neurons and a GRU layer with 200 neurons. One layer of the deep neural network (DNNLSTM) classifier has 200 neurons in the DNN layer and 100 neurons in the LSTM layer. Furthermore, as Table 6 shows, we have compared our hybrid model to earlier research. Cu-DNNGRU + Cu-BLSTM performs rapid matrix

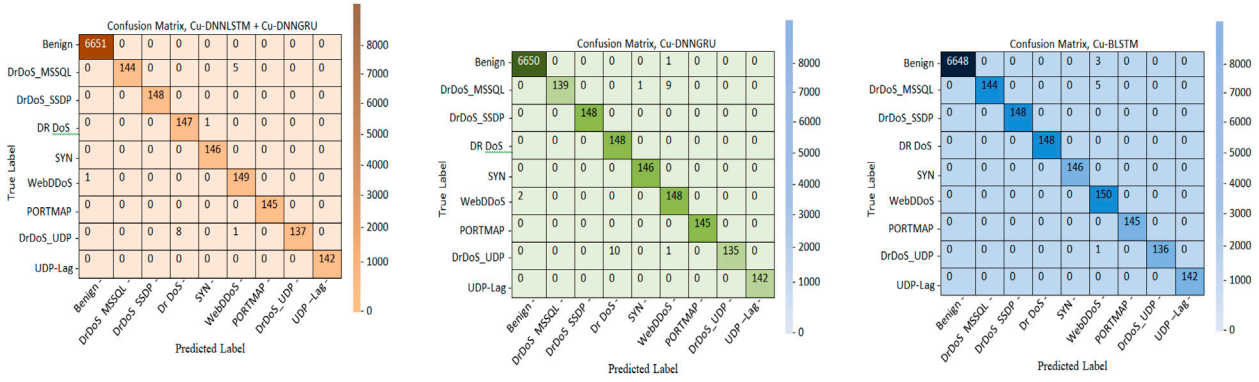

FIGURE 3
Confusion metrics for Cu-DNNGRU + Cu-BLSTM, Cu-GRULSTM, and Cu-DNNLSTM.

TABLE 5 The outcomes of a cross-validation ten times.

.Parameter	DL models	1	2	3	4	5	6	7	8	9	10
Accuracy (%)	*Cu-DNNGRU + Cu-BLSTM*	99.81	99.77	99.85	99.91	99.88	99.90	99.90	99.90	99.92	99.87
	Cu-GRULSTM	98.85	99.83	99.81	98.86	98.59	99.72	99.15	99.56	99.84	99.85
	Cu-DNNLSTM	99.81	99.85	99.81	99.74	99.72	99.71	99.72	99.74	99.62	99.71
F1-score (%)	*Cu-DNNGRU + Cu-BLSTM*	99.97	99.91	99.98	99.98	99.91	100	100	100	100	99.94
	Cu-GRULSTM	99.89	99.92	99.95	99.95	99.96	99.98	99.65	99.95	99.91	99.95
	Cu-DNNLSTM	99.92	99.89	99.95	99.89	99.97	99.91	99.94	99.88	99.81	99.82
Recall (%)	*Cu-DNNGRU + Cu-BLSTM*	99.97	99.91	99.98	99.98	99.91	100	100	100	100	99.94
	Cu-GRULSTM	99.89	99.92	99.95	99.95	99.45	99.86	99.95	99.89	99.91	99.95
	Cu-DNNLSTM	99.92	99.89	99.95	99.89	99.83	99.87	99.86	99.89	99.90	99.91
Precision (%)	*Cu-DNNGRU + Cu-BLSTM*	99.79	99.81	99.84	99.91	99.94	99.88	99.88	99.88	99.91	99.89
	Cu-GRULSTM	99.85	99.87	99.81	99.18	99.66	99.84	99.85	99.78	99.76	99.51
	Cu-DNNLSTM	99.84	99.85	99.85	99.88	99.69	99.76	99.69	99.88	99.82	99.87

multiplication, increasing the system's overall efficiency. Table 2 contains a full overview of the suggested DL classifiers. The proposed scheme uses Cu-DNNGRU and Cu-BLSTM layers instead of more complex architectures like LSTMs. GRU (Gated Recurrent Unit) layers are often more computationally efficient than LSTM layers because they use fewer gates and have simpler computations, resulting in lower computational overhead.

3.3 Set of data

Choosing the correct data collection method is an effective way to analyze the efficacy of a threat detection strategy. The authors of the recently published literature used a variety of data sets for threat detection in the Internet of Things environment, including NSLKDD, KDD99, and others. Nonetheless, the majority of these data sets lack the IoT's advantageous qualities. Some scammers utilize websites to locate and control nearby Internet of Things devices. They also use DNS rebinding and malicious JavaScript to detect and target adjacent IoT devices (Musarat et al., 2024). As a result, the proposed effort relied on the cutting-edge, publicly accessible CICIDS 2021 data collection (Gozuoglu et al., 2024). The network flow aspects in this data collection contribute to the Internet of Things. Furthermore, it is multiclass, with both benign and hazardous samples. There are over 80 traffic features, seven categories, and fourteen current threats (including DDoS, botnet, brute force, and bot). Nonetheless, the proposed study separates the general distribution into six groups, which include both benign and aggressive varieties. Furthermore, we selected every attribute in this dataset. The data collection includes 84,702 cases, of which 15,138 are considered assaults and 69,654 are benign. Table 3 provides complete information on the various attack and benign classifications.

3.4 Preparing the data set

Feeding the data directly into a categorization system is unreliable due to the data set's presentation. We first deleted any rows with blank

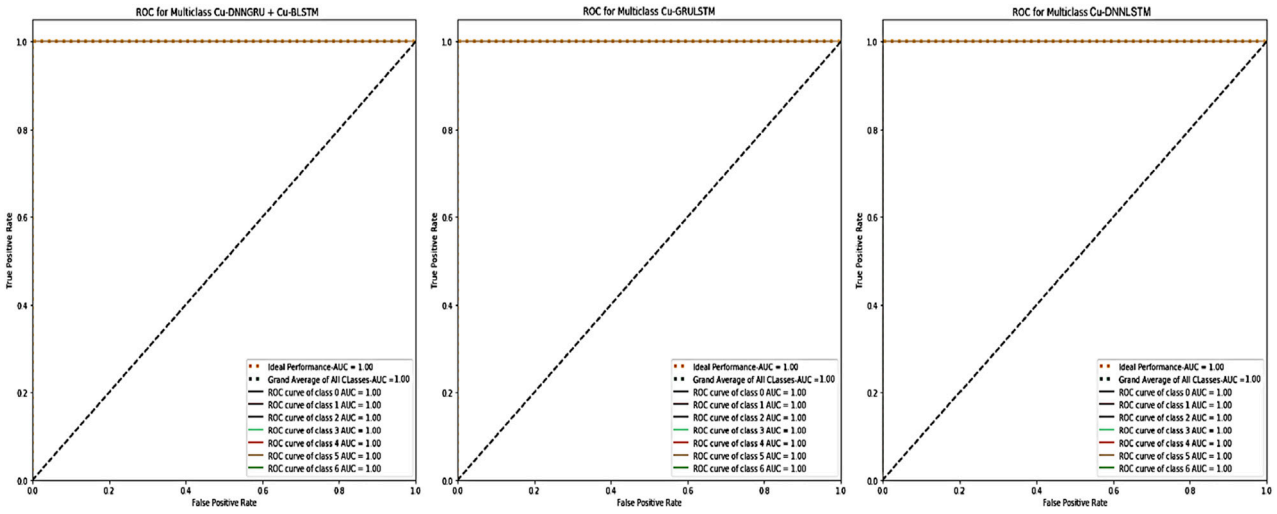

FIGURE 4
ROC curves for Cu-DNNGRU + Cu-BLSTM, Cu-GRULSTM, and Cu-DNNLSTM.

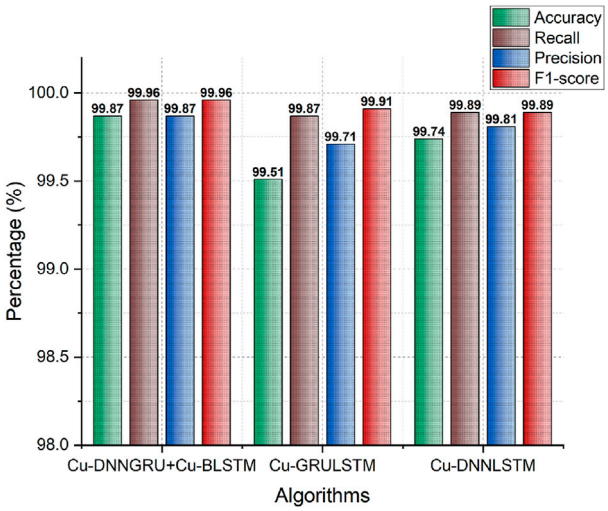

FIGURE 5
Accuracy, recall, precision, and F1-score.

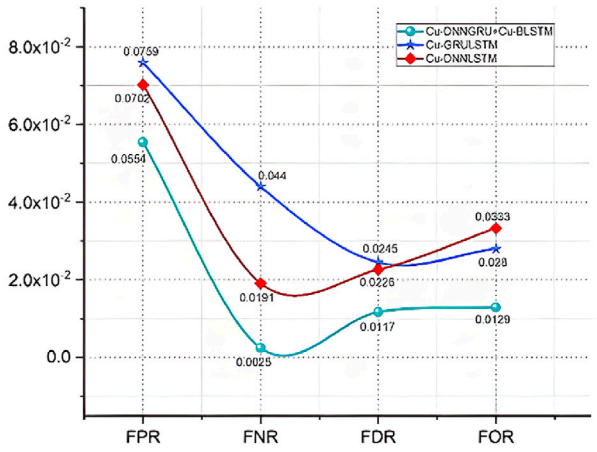

FIGURE 6
Obtained values for FPR, FNR, FDR, and FOR.

or Nan values to ensure that they did not have an impact on the data's quality or the evaluation model. Because DL techniques work with numerical data, we employed the label encoder, also known as sklearn, to convert any non-numerical objects to numerical values. Furthermore, one-hot encoding was used for the output label since category ordering may have an inadvertent detrimental impact on model performance. Additionally, data normalization is performed to improve the model's efficacy. When obtaining data, we used the MinMax scalar function.

4 Setup for an experiment

For our investigation, we used an Intel Core i7-7700 processor and a graphics processing unit (GPU). Furthermore, the recommended module was trained with Keras and Python 3.8. Table 4 has a full description of both the hardware and software.

4.1 Common assessment criteria

For the suggested design, standard performance assessment measures include recall, precision, accuracy, F1-score, and so on. To acquire the required numbers, we must first compute the following: false positive (FP), true positive (TP), false omission (FOR), Matthews correlation coefficient (MCC), false negative (FN), and true negative (TN).

5 Findings and discussion

This section shows the whole output of the proposed hybrid model (Cu-DNNGRU + Cu-BLSTM). We thoroughly evaluated the

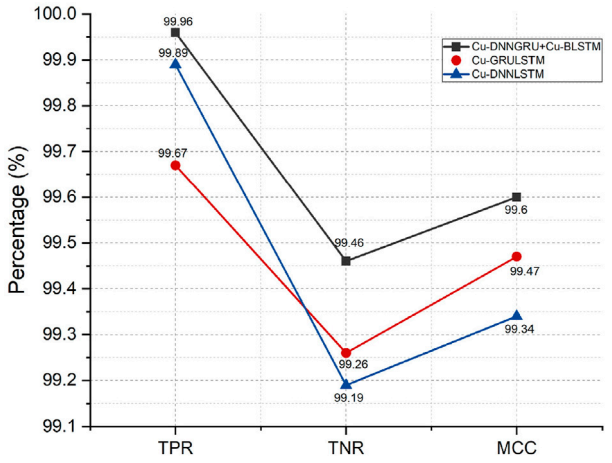

FIGURE 7
TNR, MCC, and TPR.

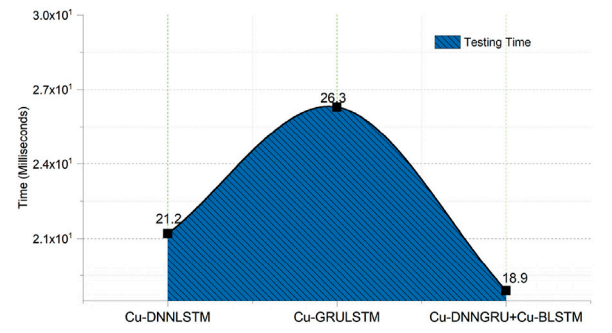

FIGURE 8
Testing times for Cu-DNNGRU + Cu-BLSTM, Cu-DNNGRU, and Cu-DNNLSTM.

performance of our proposed hybrid model by comparing it to two other studies and two DL-driven hybrid models that we had previously developed, Cu-GRULSTM and DNNLSTM. The proposed model is evaluated using the usual assessment metrics provided below.

5.1 Analysis of confusion matrix

It is used to present the results of the categorization model. When the confusion matrix is properly analyzed, it is clear that Cu-DNNGRU + Cu-BLSTM accurately identifies classes. The figure displays the confusion metrics for each of the three models. Figure 3 shows that the suggested model, Cu-DNNGRU + Cu-BLSTM, outperforms Cu-GRULSTM and Cu-DNNLSTM in terms of data classification accuracy.

5.2 Cross-checking

The 10-fold cross-validation was used to verify the impartiality of our findings. Table 5 provides a full description of each fold. However, for assessment measures, the study project displays the average results of ten times the number of parts.

5.3 Analysis of Roc curves

The Roc is a key component of any intrusion detection system (IDS). When comparing true negative rates (TNR) and true positive rates (TPR), the results are shown with the Roc. Figure 4 exhibits the Roc curves for our proposed models, highlighting the link between true positives and true negatives.

5.4 Precision, F1-score, accuracy, and recall

Accuracy determines a classifier's efficacy and efficiency. It displays how many samples the model properly identified. Figure 5 shows the accuracy of our suggested model, Cu-DNNGRU + Cu-BLSTM. 99.96% recall and 99.87% accuracy demonstrate that the hybrid model functioned well. The precision indicates the number of records that were accurately detected. With an F1-score of 99.96% and a precision of 99.87%, our proposed model works well. Table 5 shows the memory, F1 score, accuracy, and precision scores for each fold.

TABLE 6 The proposed model is contrasted with the corpus of recent research.

Ref	Data set	Accuracy	T.Time	Algorithm	10 fold	Cu-E	Precision	F1-score	Recall
Proposed model	CICIDS2018	99.87%	18.9 ms	Cu-DNNGRU + Cu-BLSTM	√	√	99.87%	99.96%	99.96%
Abbas et al. (2024)	CICIDS2018	91.50%	–	CNN	–	–	–	–	–
Abdallah et al. (2024)	CICIDS2017	89.00%	–	GRU-RNN	–	–	99.00%	99.00%	99.00%
Namakshenas et al. (2024)	CICIDS2017	98.60%	296 ms	LSTM-CNN	√	√	99.37%	99.35%	99.50%
Ouaissa et al. (2024)	CICIDS2018	96.11%	–	2L-ZED-IDS	–	–	93.20%	–	96.90%

5.5 Analysis of FPR, FOR, FNR, and FDR

We calculated the false positive rate (FPR), false omission rate (FOR), false discovery rate (FDR), and false negative rate (FNR) to provide a more comprehensive evaluation of our proposed hybrid model. The Cu-DNNGRU + Cu-BLSTM model we gave has FPR and FOR values of 0.0554% and 0.0129%, respectively, with FNR and FDR values of 0.0025% and 0.0117%, as shown in Figure 6. As illustrated in Figure 6, the suggested model outperforms the other two models. In addition, DNNLSTM outperforms GRULSTM.

5.6 Analysis of TNR, TPR, and MCC

To thoroughly study and evaluate the proposed model, the values of TNR, TPR, and MCC are calculated using a confusion matrix. Figure 7 shows the Tpr, Tnr, and MCC scores, which are 99.96%, 99.43%, and 99.60% respectively. Figure 7 shows that the suggested paradigm produces superior results.

5.7 Velocity and effectiveness

Figure 8 depicts the suggested model's testing timeframe. Because the training part is mostly conducted offline, it is not taken into account. Nonetheless, because testing demonstrates the model's usefulness and efficiency, it is regarded to be critical. The proposed hybrid model, which combines Cu-DNNGRU and Cu-BLSTM, demonstrates computational efficiency with an acceptable testing time of 18.90 ms. Furthermore, DNNLSTM takes less testing time than GRULSTM.

5.8 Comparison of the suggested model with current DL algorithms

To show the effectiveness of our suggested model, Cu-DNNGRU + Cu-BLSTM, we compared it to the two hybrid DL models currently in use in this study, Cu-GRULSTM and Cu-DNNLSTM. Each of these models is trained using the CICIDS 2021 data set, which uses identical assessment metrics. Table 2 displays the complete architecture of these vehicles. We also conducted a comparison examination of our proposed model and the current benchmark methodologies. Table 6 shows a comparison with the most recent benchmarks. The suggested model, Cu-DNNGRU + Cu-BLSTM, outperforms the other models on assessment criteria such as accuracy, precision, F1-score, and speed efficiency. Furthermore, Cu-DNNGRU + Cu-BLSTM has a testing time of only 18.9 (ms), much less than the current benchmarks.

6 Conclusion

IoT requires a flexible, reliable, and secure infrastructure. Due to its successes, deep learning has recently drawn attention from all across the world. In order to defend the Internet of Things environment from malware and cyberattacks, such as DDoS, brute force, bot, and infiltration, this study suggests a hybrid DL-driven architecture made possible by SDN. We have used the existing models, Cuda-DNNGRU and Cuda-BLSTM classifiers, to effectively identify threats. The suggested architecture is very scalable and reasonably priced. Additionally, two alternative hybrid algorithms that are trained and assessed on the same dataset, Cuda-GRULSTM and Cuda-DNNLSTM, are compared to the performance of our suggested model. The data unequivocally demonstrates that the suggested model performs better than the two hybrid models as well as the current benchmarks. By contrasting the evaluation criteria of accuracy, recall, precision, F1 20, and speed efficiency, the model's performance benefits are verified. Our suggested model is more efficient than those found in the literature in terms of speed efficiency and detection accuracy, as evidenced by its testing time of only 18.9 ms and accuracy of 99.87% with an FPR of 0.0554%. In the future, the authors intend to use blockchain technology, SDN, and hybrid deep learning algorithms to identify security flaws and intrusions in Internet of Things systems. Finally, we draw the conclusion that hybrid deep learning models significantly affect Internet of Things security.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

RS: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing–original draft. HM: Formal Analysis, Funding acquisition, Project administration, Resources, Supervision, Validation, Visualization, Writing–review and editing. TT: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing–original draft, Writing–review and editing. FA-T: Formal Analysis, Funding acquisition, Project administration, Resources, Supervision, Validation, Visualization, Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Abass, T., Eruaga, M. A., Itua, E. O., and Bature, J. T. (2024). Advancing food safety through iot: real-time monitoring and control systems. *Int. Med. Sci. Res. J.* 4 (3), 276–283. doi:10.51594/imsrj.v4i3.919

Abdallah, B., Khriji, S., Chéour, R., Lahoud, C., Moessner, K., and Kanoun, O. (2024). Improving the reliability of long-range communication against interference for non-line-of-sight conditions in industrial internet of things applications. *Appl. Sci.* 14 (2), 868. doi:10.3390/app14020868

Abdi, N., Albaseer, A., and Abdallah, M. (2024). The role of deep learning in advancing proactive cybersecurity measures for smart grid networks: a survey. *IEEE Internet Things J.* 11, 16398–16421. doi:10.1109/jiot.2024.3354045

Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., et al. (2024). Healthcare internet of things: security threats, challenges and future research directions. *IEEE Internet Things J.* 11, 19046–19069. doi:10.1109/jiot.2024.3360289

Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Taher, S. B., Kabir, M., et al. (2024). Toward a secure 5G-enabled internet of things: a survey on requirements, privacy, security, challenges, and opportunities. *IEEE Access* 12, 13125–13145. doi:10.1109/access.2024.3352508

Anwar, T., Khan, G. A., Ashraf, Z., Ansari, Z. A., Ahmed, R., and Azrour, M. (2024). The combination of blockchain and the internet of things (IoT): applications, opportunities, and challenges for industry. *Blockchain Mach. Learn. IoT Secur.*, 56–76. doi:10.1201/9781003438779-4

Awad, A. I., Babu, A., Barka, E., and Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: a review and future vision. *J. Inf. Secur. Appl.* 82, 103748. doi:10.1016/j.jisa.2024.103748

Casillo, M., Cecere, L., Colace, F., Lorusso, A., and Santaniello, D. (2024). Integrating the internet of things (IoT) in SPA medicine: innovations and challenges in digital wellness. *Computers* 13 (3), 67. doi:10.3390/computers13030067

Cherbal, S., Zier, A., Hebal, S., Louail, L., and Annane, B. (2024). Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *J. Supercomput.* 80 (3), 3738–3816. doi:10.1007/s11227-023-05616-2

CheSuh, L. N., Fernández-Diaz, R. Á., Alija-Perez, J. M., Benavides-Cuellar, C., and Alaiz-Moreton, H. (2024). Improve quality of service for the Internet of Things using blockchain & machine learning algorithms. *Internet Things* 26, 101123. doi:10.1016/j.iot.2024.101123

Eusufzai, F., Bobby, A. N., Shabnam, F., and Sabuj, S. R. (2024). Personal internet of things networks: an overview of 3GPP architecture, applications, key technologies, and future trends. *Int. J. Intelligent Netw.* 5, 77–91. doi:10.1016/j.ijin.2024.02.001

Gozuoglu, A., Ozgonenel, O., and Gezegin, C. (2024). CNN-LSTM based deep learning application on jetson nano: estimating electrical energy consumption for future smart homes. *Internet Things* 26, 101148. doi:10.1016/j.iot.2024.101148

Hajlaoui, R., Moulahi, T., Zidi, S., El Khediri, S., Alaya, B., and Zeadally, S. (2024). Towards smarter cyberthreats detection model for industrial Internet of Things (IIoT) 4.0. *J. Industrial Inf. Integration* 39, 100595. doi:10.1016/j.jii.2024.100595

Hakiri, A., Gokhale, A., Yahia, S. B., and Mellouli, N. (2024). A comprehensive survey on digital twin for future networks and emerging Internet of Things industry. *Comput. Netw.* 244, 110350. doi:10.1016/j.comnet.2024.110350

Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., and Ghazal, T. M. (2024). A survey on key agreement and authentication protocol for internet of things application. *IEEE Access* 12, 61642–61666. doi:10.1109/access.2024.3393567

Hemamalini, V., Mishra, A. K., Tyagi, A. K., and Kakulapati, V. (2024). Artificial intelligence–blockchain-enabled–internet of things-based cloud applications for next-generation society. *Automated Secure Comput. Next-Generation Syst.*, 65–82. doi:10.1002/9781394213948.ch4

Hussain, I. (2024). Secure, sustainable smart cities and the internet of things: perspectives, challenges, and future directions. *Sustainability* 16 (4), 1390. doi:10.3390/su16041390

Islam, M. M., Hasan, M. K., Islam, S., Balfaqih, M., Alzahrani, A. I., Alalwan, N., et al. (2024). Enabling pandemic-resilient healthcare: narrowband Internet of Things and edge intelligence for real-time monitoring. *CAAI Trans. Intell. Technol.* doi:10.1049/cit2.12314

Islam, Z., Bhuiyan, M. R. I., Poli, T. A., Hossain, R., and Mani, L. (2024). Gravitating towards internet of things: Prospective applications, challenges, and solutions of using IoT. *Int. J. Relig.* 5 (2), 436–451. doi:10.61707/awg31130

Kaleem, S., Sohail, A., Babar, M., Ahmad, A., and Tariq, M. U. (2024). A hybrid model for energy-efficient Green Internet of Things enabled intelligent transportation systems using federated learning. *Internet Things* 25, 101038. doi:10.1016/j.iot.2023.101038

Kaur, N., Sahay, S., and Dixit, S. (2024). "Role of artificial intelligence (AI)-aided internet of things (IoT) technologies in business and production," in *Advanced IoT technologies and applications in the Industry 4.0 digital Economy* (CRC Press), 29–41.

Khan, A., Jhanjhi, N. Z., Haji, D. H. T. B. A., and Omar, H. A. H. B. H. (2024). Internet of things (IoT) impact on inventory management: a review. *Cybersecurity Meas. Logist. Industry Framew.*, 224–247.

Meylani, R. (2024). Transforming education with the internet of things: a journey into smarter learning environments. *Int. J. Res. Educ. Sci.* 10 (1), 161–178. doi:10.46328/ijres.3362

Mu, W., Kleter, G. A., Bouzembrak, Y., Dupouy, E., Frewer, L. J., Radwan Al Natour, F. N., et al. (2024). Making food systems more resilient to food safety risks by including artificial intelligence, big data, and internet of things into food safety early warning and emerging risk identification tools. *Compr. Rev. Food Sci. Food Saf.* 23 (1), e13296. doi:10.1111/1541-4337.13296

Musarat, M. A., Alaloul, W. S., Khan, A. M., Ayub, S., and Jousseaume, N. (2024). A survey-based approach of framework development for improving the application of internet of things in the construction industry of Malaysia. *Results Eng.* 101823.

Namakshenas, D., Yazdinejad, A., Dehghantanha, A., and Srivastava, G. (2024). Federated quantum-based privacy-preserving threat detection model for consumer internet of things. *IEEE Trans. Consumer Electron.* 70, 5829–5838. doi:10.1109/tce.2024.3377550

Oliveira, F., Costa, D. G., Assis, F., and Silva, I. (2024). Internet of Intelligent Things: a convergence of embedded systems, edge computing and machine learning. *Internet Things* 26, 101153. doi:10.1016/j.iot.2024.101153

Ouaissa, M., Ouaissa, M., Khan, I. U., Boulouard, Z., and Rashid, J. (2024). *Low-power wide Area network for large Scale internet of things: architectures, communication protocols and recent Trends* (CRC Press).

Owen, J. (2024). *Securing the industrial internet of things (IIoT) through flexible cryptography in trust-deficit environments*.

Paramesha, M., Rane, N. L., and Rane, J. (2024). Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. *Partners Univers. Multidiscip. Res. J.* 1 (2), 110–133.

Peelam, M. S., Rout, A. A., and Chamola, V. (2024). Quantum computing applications for internet of things. *IET Quantum Commun.* 5 (2), 103–112. doi:10.1049/qtc2.12079

Prasad, S. R., and Thyagaraju, G. S. (2024). Leaf analysis based early plant disease detection using Internet of Things, Machine Learning and Deep Learning: a comprehensive review. *J. Integr. Sci. Technol.* 12 (2), 734.

Rahman, A., Islam, J., Kundu, D., Karim, R., Rahman, Z., Band, S. S., et al. (2025). Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: present perspectives and future directions. *Int. J. Commun. Syst.* 38 (1), e5429. doi:10.1002/dac.5429

Rehman, Z., Tariq, N., Moqurrab, S. A., Yoo, J., and Srivastava, G. (2024). Machine learning and internet of things applications in enterprise architectures: solutions, challenges, and open issues. *Expert Syst.* 41 (1), e13467. doi:10.1111/exsy.13467

Rejeb, A., Rejeb, K., Appolloni, A., Jagtap, S., Iranmanesh, M., Alghamdi, S., et al. (2024). Unleashing the power of internet of things and blockchain: a comprehensive analysis and future directions. *Internet Things Cyber-Physical Syst.* 4, 1–18. doi:10.1016/j.iotcps.2023.06.003

Shafik, W. (2024). Blockchain-based internet of things (B-IoT): challenges, solutions, opportunities, open research questions, and future trends. *Blockchain-based internet things*, 35–58.

Siddique, A. A., Alasbali, N., Driss, M., Boulila, W., Alshehri, M. S., and Ahmad, J. (2024). Sustainable collaboration: federated learning for environmentally conscious forest fire classification in green internet of things (IoT). *Internet Things* 25, 101013. doi:10.1016/j.iot.2023.101013

Singh, D., and Dwivedi, R. K. (2024). Designing blockchain based secure autonomous vehicular internet of things (IoT) architecture with efficient smart contracts. *Int. J. Inf. Technol.*, 1–17.

Singh, K., Singh, Y., Khang, A., Barak, D., and Yadav, M. (2024). "Internet of things (IoT)-Based technologies for reliability evaluation with artificial intelligence (AI)," in *AI and IoT technology and applications for smart healthcare systems* (Auerbach Publications), 387–395.

Singh, S., Chhabra, R., and Arora, J. (2024). A systematic review of waste management solutions using machine learning, Internet of Things and blockchain technologies: state-of-art, methodologies, and challenges. *Archives Comput. Methods Eng.* 31 (3), 1255–1276. doi:10.1007/s11831-023-10008-z

Tyagi, A. K. (2024). "Blockchain and artificial intelligence for cyber security in the era of internet of things and industrial internet of things applications," in *AI and blockchain applications in industrial Robotics* (IGI Global), 171–199.

Ullah, A., Anwar, S. M., Li, J., Nadeem, L., Mahmood, T., Rehman, A., et al. (2024). Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment. *Complex & Intelligent Syst.* 10 (1), 1607–1637. doi:10.1007/s40747-023-01175-4

Uzoka, A., Cadet, E., and Ojukwu, P. U. (2024). The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications. *Compr. Res. Rev. Sci. Technol.* 2 (02), 055–073. doi:10.57219/crrst.2024.2.2.0037

Van Hoang, T. (2024). Impact of integrated artificial intelligence and internet of things technologies on smart city transformation. *J. Tech. Educ. Sci.* 19 (Special Issue 01), 64–73. doi:10.54644/jte.2024.1532

Vishwakarma, A. K., Chaurasia, S., Kumar, K., Singh, Y. N., and Chaurasia, R. (2024). Internet of things technology, research, and challenges: a survey. *Multimedia Tools Appl.*, 1–36. doi:10.1007/s11042-024-19278-6

Wang, C. (2024). Intelligent agricultural greenhouse control system based on internet of things and machine learning. arXiv preprint arXiv:2402.09488.

Wang, T., Tang, T., Cai, Z., Fang, K., Tian, J., Li, J., et al. (2024). Federated learning-based information leakage risk detection for secure medical internet of things. *ACM Trans. Internet Technol.* doi:10.1145/3639466

Wen, J., Nie, J., Kang, J., Niyato, D., Du, H., Zhang, Y., et al. (2024). From generative ai to generative internet of things: Fundamentals, framework, and outlooks. *IEEE Internet Things Mag.* 7 (3), 30–37. doi:10.1109/iotm.001.2300255

Zainuddin, A. A., Zakirudin, M. A. Z., Zulkefli, A. S. S., Mazli, A. M., Wardi, M. A. S. M., Fazail, M. N., et al. (2024). Artificial intelligence: a new paradigm for distributed sensor networks on the internet of things: a review. *Int. J. Perceptive Cognitive Comput.* 10 (1), 16–28. doi:10.31436/ijpcc.v10i1.414

Zormati, M. A., Lakhlef, H., and Ouni, S. (2024). Review and analysis of recent advances in intelligent network softwarization for the Internet of Things. *Comput. Netw.*, 110215. doi:10.1016/j.comnet.2024.110215