Tikrit Journal of Engineering Sciences (2025); 32(Sp1): 2526
DOI: http://doi.org/10.25130/tjes.sp1.2025.2

IRAQI Academic Scientific Journals

ISSN: 1813-162X (Print); 2312-7589 (Online)
Tikrit Journal of Engineering Sciences
available online at: http://www.tj-es.com

TJES Tikrit Journal of Engineering Sciences

Hybrid Convolutional Neural Network-Based Intrusion Detection System for Secure IoT Networks

Sami Qawasmeh [a], Ahmad Habboush [b], Bassam Elzaghmouri [*c], Qasem Kharma [a], Da'ad Albalawneh [d]

a Department of Computer Science, Information Technology, Jadara University, Irbid, Jordan.
b Department of Software Engineering, Information Technology, Al-Ahliyya Amman University, Amman, Jordan.
c Department of Computer Science, Information Technology, Al-Ahliyya Amman University, Amman, Jordan.
d Department of Computer Science, University College in Umluj, University of Tabuk, Tabuk, Saudi Arabia.

Keywords:
Intrusion detection system; Hybrid convolutional neural network; Attack detection; Machine learning; Deep learning; IoT.

Highlights:

- *Proposes an innovative IoT-based system for early lung cancer detection Integrates machine learning with homomorphic encryption for secure data processing.*
- *Dataset: Utilizes a curated dataset of 460,292 patient records from Kaggle Includes demographics, lifestyle factors, medical history, and IoT-sensor data Dataset split into training (322,204), validation (69,044), and test sets (69,044).*
- *ML Models: Compares performance of five ML algorithms: SVM, NBM, KNN, PART, and RF Implements advanced techniques for optimal prediction accuracy.*
- *Superior Performance of PART Algorithm PART model achieves the highest accuracy at 91% Outperforms other models: SVM (89%), NBM (86%), KNN (83%), and RF (80%).*

ARTICLE INFO

Article history:

Received	27 Mar. 2025
Received in revised form	01 July 2025
Accepted	08 July 2025
Final Proofreading	20 July 2025
Available online	12 Aug. 2025

Citation: Qawasmeh S, Habboush A, Elzaghmouri B, Kharma Q, Albalawneh D. **Hybrid Convolutional Neural Network-Based Intrusion Detection System for Secure IoT Networks**. *Tikrit Journal of Engineering Sciences* 2025; **32**(Sp1): 2526.
http://doi.org/10.25130/tjes.sp1.2025.2

*Corresponding author:
Bassam Elzaghmouri
Department of Computer Science, Information Technology, Al-Ahliyya Amman University, Amman, Jordan.

Abstract: Security vulnerabilities are a growing concern due to the increasing prevalence of Internet of Things (IoT) devices. This paper presents a hybrid Convolutional neural network (CNN)-based intrusion detection system (IDS) for IoT networks that detects threats. The research tackles the shortcomings of existing IDSs, which focus on individual threats and are computationally expensive. The proposed method outperforms the traditional machine learning and deep learning models in identifying IoT network attacks. The goal of this study is to create an effective IDS for IoT networks that can detect a range of anomalies and malicious attacks. The research aims to address the limitations of existing intrusion detection systems (IDSs) by enhancing their ability to detect a broader range of attacks with improved performance through the addition of a "long short-term memory (LSTM)" component and the utilization of a hybrid CNN model. The proposed model includes data gathering, preprocessing, network training, and attack identification. System logs and their features are selected for data collection, followed by preprocessing to remove noise. The training model defines the convolutional layer's structure, sliding window size, neuron connection weights, and outputs using the improved data. The training period is used for attack detection, and the weights are calculated from trained and real-time data. Using the UNSW NB15 dataset, the suggested IDS is tested against a recurrent neural network (RNN) system. The suggested model outperforms the RNN model in several performance parameters, achieving a 99.1% detection accuracy, 4% higher. CNN-based intrusion detection in IoT networks is stressed in the study. It shows how hybrid CNN-based techniques can improve IoT network security and resilience. The proposed IDS introduces a novel approach that utilizes a hybrid CNN model and incorporates LSTM to enhance the detection capabilities of IoT network attacks. The study highlights the significance of leveraging advanced machine learning techniques to maintain the integrity and privacy of IoT systems.

النظام القائم على الشبكة العصبية الالتفافية الهجينة لكشف التسلل في شبكات إنترنت الأشياء الآمنة

سامي القواسمة [١]، أحمد حبوش [٢]، بسام الزغموري [٣]، قاسم خرما [١]، دعد البلاونة [٤]

[١] قسم علوم الحاسوب/ تكنولوجيا المعلومات/ جامعة جدارا/ إربد – الأردن.

[٢] قسم هندسة البرمجيات/ تكنولوجيا المعلومات/ جامعة عمان الأهلية/ عمان – الأردن.

[٣] قسم علوم الحاسوب/ تكنولوجيا المعلومات/ جامعة عمان الأهلية/ عمان – الأردن.

[٤] قسم علوم الحاسوب/ الكلية الجامعية في أملج/ جامعة تبوك/ تبوك - المملكة العربية السعودية.

الخلاصة

تُشكّل الثغرات الأمنية مصدر قلق متزايد نظرًا للانتشار المتزايد لأجهزة إنترنت الأشياء. تُقدّم هذه الورقة البحثية نظامًا هجينًا لكشف التسلل (IDS) قائمًا على الشبكة العصبية التلافيفية (CNN) لشبكات إنترنت الأشياء، قادر على اكتشاف التهديدات. يتناول البحث أوجه القصور في أنظمة كشف التسلل الحالية، التي تُركّز على التهديدات الفردية، وتُعد مكلفة حسابيًا. تتفوق الطريقة المُقترحة على نماذج التعلم الآلي والتعلم العميق التقليدية في تحديد هجمات شبكات إنترنت الأشياء. تهدف هذه الدراسة إلى إنشاء نظام كشف تسلل فعّال لشبكات إنترنت الأشياء، قادر على اكتشاف مجموعة من الشذوذ والهجمات الخبيثة. يهدف البحث إلى معالجة قيود أنظمة كشف التسلل الحالية من خلال تعزيز قدرتها على اكتشاف مجموعة أوسع من الهجمات مع تحسين الأداء، وذلك من خلال إضافة مُكوّن "ذاكرة طويلة المدى قصيرة المدى" (LSTM) واستخدام نموذج CNN هجين. يشمل النموذج المُقترح جمع البيانات، والمعالجة المُسبقة، وتدريب الشبكة، وتحديد الهجمات. يتم اختيار سجلات النظام وخصائصها لجمع البيانات، تليها معالجة مسبقة لإزالة التشويش. يحدد نموذج التدريب بنية الطبقة التلافيفية، وحجم نافذة الانزلاق، وأوزان اتصال الخلايا العصبية، والمخرجات باستخدام البيانات المُحسّنة. تُستخدم فترة التدريب للكشف عن الهجمات، وتُحسب الأوزان من البيانات المُدرّبة والبيانات اللحظية. باستخدام مجموعة بيانات UNSW NB15، يتم اختبار نظام الكشف عن التسلل المقترح على نظام شبكة عصبية متكررة (RNN). يتفوق النموذج المقترح على نموذج RNN في العديد من معايير الأداء، محققًا دقة اكتشاف تبلغ ٩٩,١٪، أي أعلى بنسبة ٤٪. تُركّز الدراسة على كشف التسلل القائم على CNN في شبكات إنترنت الأشياء. تُظهر الدراسة كيف يُمكن للتقنيات الهجينة القائمة على CNN تحسين أمان شبكات إنترنت الأشياء ومرونتها. يُقدّم نظام الكشف عن التسلل المقترح نهجًا جديدًا يستخدم نموذج CNN هجينًا ويدمج LSTM لتعزيز قدرات الكشف عن هجمات شبكات إنترنت الأشياء. تُسلّط الدراسة الضوء على أهمية الاستفادة من تقنيات التعلم الآلي المتقدمة للحفاظ على سلامة وخصوصية أنظمة إنترنت الأشياء.

الكلمات الدالة: جمع القمامة، إنترنت الأشياء، LoRa، خالٍ من التلوث، الرصد في الزمن الحقيقي، RecycleCnn، إدارة النفايات.

1.INTRODUCTION

The Internet of Things (IoT) has rapidly transformed various industries, including healthcare, smart cities, and industrial automation, by enabling seamless connectivity and data exchange [1-6]. However, the increasing adoption of IoT devices has also introduced significant security risks, as these devices often operate in resource-constrained environments with limited security features. Cyber threats such as denial-of-service (DoS) attacks, malware injections, and data breaches pose severe challenges to IoT networks, necessitating the development of robust and intelligent intrusion detection mechanisms [7-9]. Traditional Intrusion Detection Systems (IDSs) rely on signature-based, anomaly-based, or specification-based approaches to detect malicious activities [10-12]. While effective, these methods suffer from several limitations, including high computational costs, inability to detect unknown threats, and inefficient real-time processing [7,8]. Furthermore, many existing IDS solutions focus on isolated attack types, failing to provide a comprehensive security framework that can detect a broad spectrum of cyber threats. These challenges highlight the urgent need for a scalable and adaptable IDS to secure IoT ecosystems. To address these shortcomings, this study proposes a Hybrid Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) Intrusion Detection System (IDS). The CNN component efficiently extracts spatial features from network traffic, while the LSTM module captures temporal dependencies, allowing for improved sequential threat detection. This hybrid approach enhances detection accuracy, reduces false positives, and ensures adaptability to evolving cyber threats. Unlike conventional IDS models, which often focus on predefined attack patterns, the proposed deep learning-based IDS dynamically learns from network traffic data, making it more effective in detecting both known and unknown attacks. This research fills a critical gap in IoT security by developing a high-performance hybrid IDS that balances computational efficiency and detection accuracy. The key contributions of this study include:

1- Development of a hybrid CNN-LSTM IDS, leveraging deep learning techniques for real-time and high-accuracy intrusion detection.
2- Comprehensive evaluation using the UNSW-NB15 dataset, demonstrating a detection accuracy of 99.1%, outperforming traditional IDS models.
3- Optimization of IDS performance for IoT applications, ensuring scalability and adaptability in real-world deployments.

By integrating advanced deep learning methodologies into IDS frameworks, this research contributes to the next generation of IoT security solutions, addressing the increasing threats faced by interconnected devices. Figure 1 shows the structure of an IDS.

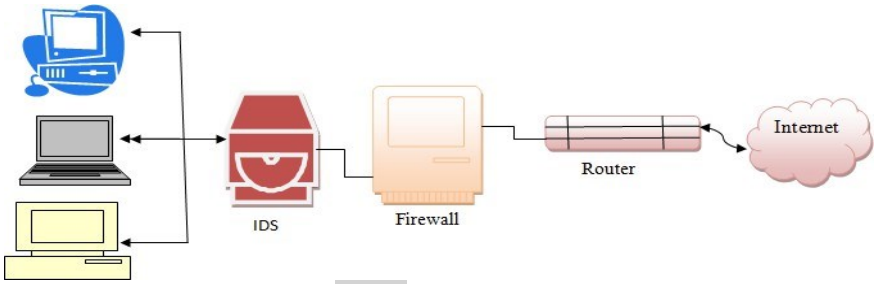

Fig. 1 ID System.

IDSs have three separate phases. Network or host sensors start IDS monitoring. Intrusion detection systems analyze features and patterns in the second phase. IDSs detect irregularities and network intrusions. IDS's efficient network management and speedy vulnerability identification help monitor, analyze, and analyze traffic. It secures the network and data. IDS aggregates and analyzes system data streams to detect malicious or harmful activity. Traditional intrusion detection systems emphasize internet management over real-time, high-volume data streams. Placement, detection, and validation procedures make up conventional IDS. Figure 2 shows IoT intrusion detection systems. Most systems use detection algorithms. Anomaly-based, specification-based, Signature-based, and hybrid IDS are monitoring technique subtypes.

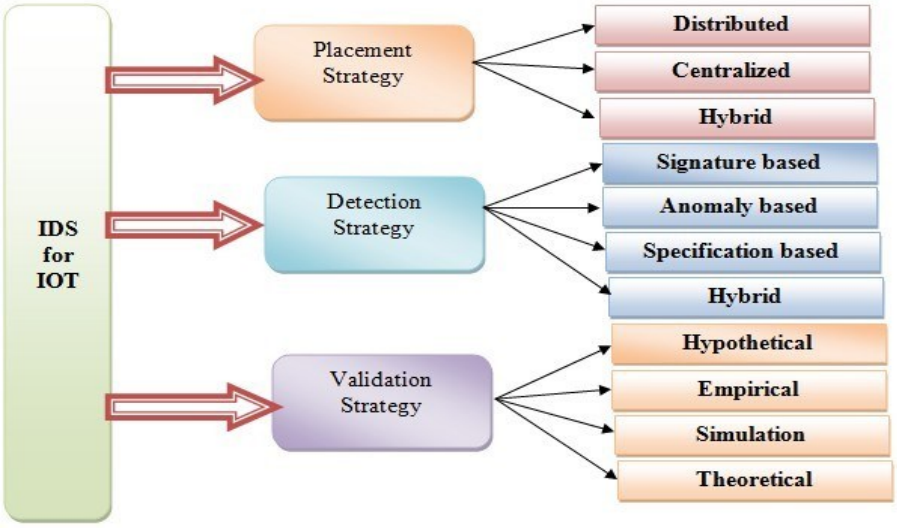

Fig. 2 Intrusion Detection Systems on the Internet of Things.

- Signature-based ID system: It recognizes and describes attacks along with their incurred patterns. When a signature-based detection system detects an attack on a network, it generates an alert regarding some incurring suspicious behaviors and performs pattern matching. Access or alerts are offered to the user based on similarity and dissimilarity in order to detect assaults accurately.
- Anomaly-based IDS: This is a basic IDS that collects data and recognizes system anomalies. Based on a predefined threshold, both normal and abnormal actions are distinguished, and network administrators are notified of any issues. Such an IDS is capable of efficiently identifying incurred unknown threats; however, it consumes a considerable amount of memory space for processing and incurs a significantly higher computational cost.
- Specification-based IDS: Such IDSs continually assess system operations based on pre-specified operations. Here, the network administrator is responsible for defining the specific operation and continually monitoring, thereby validating the operation carried out by the process. If operational deviations are detected, an alarm is sent to the respective network administrator.
- Hybrid IDS: This type of IDS represents a combination of anomaly-based and signature-based IDS, offering a better balance between storage space and computational costs with fewer false-positive alerts. Due to its efficient detection and simple operation, hybrid IDS has recently become the foundation of the majority of systems.

The paper introduces a Hybrid Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS) designed to secure IoT networks. The proposed model is highly versatile and applicable to a broad spectrum of IoT-based applications, demonstrating superior responsiveness in detecting IoT network attacks compared to traditional machine learning and deep learning models. The present work emphasizes the significance of leveraging advanced machine learning techniques, particularly CNN-based approaches, to enhance the security and robustness of IoT networks. The proposed system offers enhanced detection capabilities, aiding in the protection of IoT devices and preventing potential cyber threats. In this paper, the following key contributions were made:

1- Introduce a new architecture that jointly learns spatial features (via CNN) and temporal dependencies (via LSTM) for intrusion detection.
2- Validate the present approach on UNSW-NB15, which includes over 97,000 samples across training, testing, and validation splits.
3- The present model improves detection accuracy by more than 4% compared to standard RNN-based detectors.
4- Outline how to adapt the proposed model for resource-constrained IoT devices.

2.RELATED WORK

The primary objective of an IDS is to detect attacks, so it is crucial to characterize the various categories of attacks encountered in an IoT-based network. Diverse investigation efforts have been conducted to design an IDS that is necessarily advanced, and the search for an efficient system capable of identifying various types of attacks continues. In an IoT-based network, black hole attack, wormhole attack, sinkhole attack, Sybil attack, selective forwarding assault, false data attack, service attack, replay attack, and jamming attack are among the most prominent attacks. Stephen and Arockiam [13] proposed a lightweight, hybrid, and centralized Hello Flood and Sybil attack detection solution for IoT-based networks using the routing over “low power and lossy networks (RPL)” routing protocol. This algorithm utilizes detection measures, such as packet counts, to verify the IDS agent's intrusion ratio (IR). Raza et al. [14] developed SVELTE, a legitimate IDS for the IoT network. The system involves a 6LoWPAN Mapper (6Mapper), an ID unit, and a small proxy server. It examines the transferred information to identify any security breaches. Its ability to identify numerous threats is promising. Nevertheless, it has solely been evaluated for detecting forged or changed data, sinkholes, and selective forwarding attacks. Pongle and Chavan [15] conceived and constructed a logically centralized framework for a hybrid IDS based on simulations of network scenarios. It is primarily concerned with identifying routing assaults such as wormhole attacks. Jun and Chi [16] introduced an IDS for IoT-based networks based on priority scheduling. This work features a system that employs complicated context-awareness techniques to detect threats. Summerville et al. [17] designed an IDS for the Internet of Things that utilizes a comprehensive data analysis strategy, leveraging a bit-pattern technique. Networking protocols were represented by a series of bytes, referred to as a bit pattern, and feature selection was implemented as an overlapping sequence of bytes, known as n-grams. There was a match between the bit-pattern and n-grams [18] when the corresponding bits matched in all places. The system was examined by deploying four attacks, and its false-positive rate was extremely low. Midi et al. [19] suggested Kalis, a lightweight, experienced, understanding, and adaptable IDS. It gathers data about the characteristics and entities of the live system and uses this information to dynamically configure the most efficient detection strategies. It is adaptable to new standards and provides a method for knowledge exchange that enables collaborative incident detection. The results demonstrated that the system detected primarily DoS and routing attacks with great precision. Moreover, Thanigaivelan et al. [20] suggested an integrated IDS for the Internet of Things. Each network node in this system watched its neighbor. The monitoring node blocked the abnormally behaving node's data-link layer packets and alerted its parent node. Oh et al. [21] created a distributed, lightweight IoT IDS using packet payload and threat signature matching. Meera et al. [22] investigated IDs based on machine learning for IoT, assessing various methods for feature extraction and ML models. The findings revealed that the integration of VGG-16 with stacking achieved an impressive accuracy of 98.3% on the IEEE Data Port dataset. The paper investigates security issues within WSN-IoT networks, exploring strategies such as machine learning for network administration and assessing constraints within IoT protocols. It concludes with a comparison that illustrates the extensive scope of the proposed study in relation to prior research [23]. Fuzzy blockchain frameworks with fuzzy logic and deep learning for threat detection are proposed to address security issues in blockchain-based IoT systems. Testing shows the framework can identify security issues, validate transactions efficiently, and detect dangers in blockchain-based IoT networks [24]. An End-to-End Explains how communication occurs between

the sending and receiving IoT devices. [25]. Wei Liang et al. [26] proposed GTxChain, a secure blockchain-based IoT architecture using graph neural networks and off-chain data gathering for enhanced privacy and security. GTxChain enhances performance and stability by 10.51% compared to existing architectures utilizing the Lightning Network, IPFS, and GNN, thereby ensuring the IoT system's trustworthiness, security, and privacy. Arya K et al. analyzed how blockchain and IoT might improve transportation security, transparency, and efficiency in India through scalable Intelligent Transportation Systems (ITS) [27]. M. Karthikeyan et al. introduce FA-ML, which combines the Firefly Algorithm and machine learning and improves WSN-IoT intrusion detection accuracy to 99.34%, beating KNN-PSO and XGBoost. According to the report, synthesizing modern security solutions in networked, IoT-driven environments is crucial for critical protecting infrastructure and industrial automation [28, 29]. The present paper explores recent IoT developments, future applications, and ongoing research challenges, highlighting its transformative potential and the need for continued innovation [30, 31]. The proposed approach in this study relies on pre-trained CNN models, which are explicitly fine-tuned for breast cancer detection.

3.PROPOSED WORK

3.1.Data Collection and Preprocessing

This study utilizes the UNSW-NB15 dataset, a widely used benchmark for evaluating intrusion detection systems. The dataset comprises 49 network traffic features, capturing both normal and malicious activities, categorized into various attack types, including DoS, Exploits, Reconnaissance, Shellcode, and Worms. The dataset is split into 70% for training and 30% for testing to ensure a robust evaluation of the proposed model.

3.1.1.Preprocessing Steps

To enhance model performance and ensure high-quality inputs, the following preprocessing techniques were applied:

- Noise Removal: Duplicate and incomplete records were eliminated to reduce data inconsistencies.
- Feature Selection: Mutual information-based feature selection was used to retain the most relevant attributes for intrusion detection.
- Data Normalization: Min-max normalization was applied to scale features within a [0,1] range, ensuring uniform weight distribution across input variables.
- Balancing: Given the dataset's imbalance between attack and normal samples, Synthetic Minority.

1- General and In-Depth Specialization of the Manuscript:

- This manuscript lies at the intersection of intelligent information retrieval systems, fuzzy logic, and machine learning applications in precision agriculture. It specializes in query expansion techniques, case-based reasoning, and deep learning architectures tailored for agricultural data.
- In-depth, the work focuses on leveraging pre-trained language models to generate contextual embeddings for semantic query expansion, applying fuzzy logic thresholds to manage variability in soil and environmental data, and integrating an XGBoost classifier with an Independent Recurrent Neural Network to optimize similarity scoring and recommendation accuracy.

2- Definition, Original Idea, and Novelty of the Research:

- This manuscript defines a Boosted Query-based Case-Based Reasoning System (BQ-CBRS) as a framework that enhances traditional CBR by dynamically expanding queries and incorporating fuzzified parameters into the retrieval and learning pipeline.
- The original idea is based on the fusion of embedding-based query expansion, fuzzification, and an ensemble of XGBoost and IndRNN models. To the authors' knowledge, this is the first work to systematically combine these components for real-time crop recommendations, offering significant gains in retrieval performance and decision support for sustainable farming. The Over-Sampling Technique (SMOTE) was employed to generate additional attack instances, preventing bias towards the majority classes.

3.1.2.Dataset Bias and Limitations

While UNSW-NB15 provides a diverse attack landscape, potential biases exist, including overrepresentation of specific attack types and limited real-world variations in network traffic. To address this issue, cross-validation was performed to evaluate model generalizability across different subsets of the dataset. The detailed characteristics of the dataset samples utilized in the present investigation are summarized in Table 1. This dataset was selected for its comprehensive feature set and richness in attack diversity, which is crucial for training and validating the proposed IDS model.

Table 1 Dataset Samples.

Class	Sample Size
Normal	340
Attack	4320

3.2.Model Architecture and Methodology

The proposed Hybrid CNN-LSTM Intrusion Detection System (IDS) integrates Convolutional Neural Networks (CNNs) for spatial feature extraction with Long Short-Term Memory (LSTM) networks for sequential pattern recognition. This hybrid approach enables effective detection of both static and evolving threats in IoT networks.

3.2.1.CNN for Feature Extraction

The CNN module processes network traffic data by extracting spatial correlations among features, using:

- Multiple convolutional layers to identify hierarchical feature representations.
- ReLU activation to introduce non-linearity and improve learning efficiency.
- Max-pooling layers to reduce feature dimensionality while retaining important patterns.

3.2.2.LSTM for Sequential Pattern Recognition

Since network attacks often exhibit time-dependent behaviors, an LSTM layer is incorporated to capture temporal dependencies within network traffic sequences.

- The LSTM layer processes CNN-extracted feature maps over time, enhancing the model's ability to detect anomalies in sequential data.
- Dropout regularization is applied to prevent overfitting.

3.2.3.Model Training and Optimization

The CNN-LSTM model was trained using:

- Adam optimizer with an initial learning rate of 0.001.
- Categorical cross-entropy loss function to minimize classification errors.
- Batch size of 128 and 50 training epochs, determined via hyperparameter tuning.

The network architecture comprises an input layer containing a collection of matrices with dimensions m0×n0. The output layer consists of neurons that correspond to various labels. To generalize the features, hidden layers comprise multiple convolutional matrices and their corresponding filter matrices. The convolution and filter features are calculated using a set of parameters, denoted as (*s*,∗*hn*,*st*1) &¿). Where s is the weight depth of the shared matrices, and st1 and st2 are the sliding steps. The size of the moving window is written as $w_n{*}h_n$, and the size of the filter window is written as $w_m{*}h_m$. The last layer, the hidden layer, binds the output layer and classifies. The size of the moving window and how the convolution process determine the size of the resulting matrix. The resultant matrix and filter window size are specified as:

$$\boldsymbol{w_n * h_n = \left(\frac{w_{n-1} - w_m}{st1_n} + 1\right) * \left(\frac{h_{n-1} - h_m}{st1_n} + 1\right)} \quad \textbf{(1)}$$

where $w_n{*}h_n$ and wn-1 * hn-1 represent the resultant matrix size, the sliding step size is represented by st1n, and the sliding window size is represented by $W_m * h_m$. LSTM captures contextual information across the network in this stage. This technique extracts node features to identify hostile nodes and their attacks. LSTM is a recurrent neural network (RNN) model that leverages timestamps to generate outputs based on input functions. However, employing LSTM alone may not effectively detect intrusions in the network due to the gradient vanishing issue, which hampers its ability to learn information over long durations. Nonetheless, LSTM demonstrates superior performance for short time durations and significantly reduces system complexity.

The intrusion detection system uses LSTM and a CNN to address these issues. Figure 3 shows Bidirectional LSTM construction. The basic LSTM's hidden layers process inputs and outputs. Two hidden layers process bidirectional LSTM input sequences. These features aid network data transmission and data extraction.

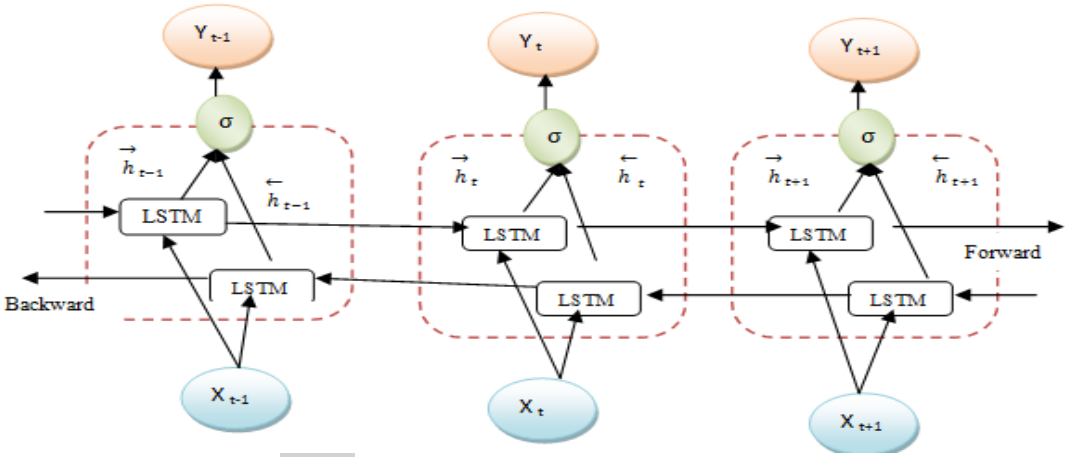

Fig. 3 Bi-directional LSTM Architecture.

During training, input features are tagged and assigned a feature matrix location based on the input neurons. The neural network computes convolutional layer weight matrices and neural link weights as inputs are processed. It has "x" convolutional layers. Output neurons are "y" while vector layers are "f". The weight function, which determines the relationship between the inputs and outputs, is obtained as a result of the training process.

$$w_y = \sum_{n=1}^{N} \sum_{m=1}^{M_n} (x_n * f_n + 1) + x * f \qquad (2)$$

In the training process, Wy represents the total weight of the network. $xn*fn$ denotes the size of the window filter, and Mn represents the number of filters in the convolutional layer. The loss function labels each input and weight. Model training and validation data compactness and descriptiveness decide the loss function. The text does not define the loss function.

$$L_f = L_c + \varphi * L_d \qquad (3)$$

Additionally, in the given text, φ is mentioned as a scaling factor that is used to assess the priority of nodes, while Lc and Ld represent the compact loss and descriptive loss, respectively. However, the specific equations or definitions for these components are not provided.

$$f_m(y) = \frac{e^o m}{\sum_{m-1}^{n} e^o n} \qquad (4)$$

The suggested intrusion detection system's activation function estimates each neuron's output probability using fully connected layer weights. The activation function typically returns a value between 0 and 1, with the highest value indicating the most likely output label. While Recurrent Neural Networks (RNNs) and GRUs were considered, they were found to be less effective for intrusion detection due to vanishing gradient issues and weaker spatial feature extraction capabilities. The proposed CNN-LSTM model outperforms these alternatives by:

- Extracting both spatial and temporal features for improved anomaly detection.
- Enhancing detection accuracy and reducing false positives compared to standard RNN models.
- Achieving a 99.1% accuracy rate, demonstrating superior performance over conventional IDSs.

Figure 4 shows the complete process flow of the proposed IoT-specific intrusion detection system.

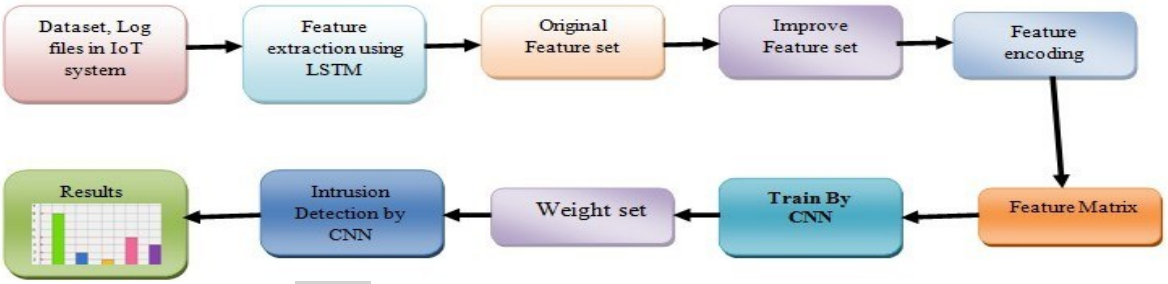

Fig. 4 Proposed IoT-Specific IDS Using HCNN.

To extract the necessary features, the training phase involves gathering the dataset and its associated log files. The existing data is improved by utilizing LSTM to compare the extracted features to the original feature set. CNN is used to train the specified data after the label function has been defined. Intruders are sorted and displayed in accordance with the weight function learned during CNN training.

3.3.Use-Case Scenario

To elucidate the practical implementation of the present model in an IoT-based network, consider the scenario of a smart home environment. The network is connected to various IoT devices, including smart thermostats, security cameras, smart locks, and home assistants, enabling seamless automation and control of the system.

Potential Threats in a Smart Home IoT Network:

1- Denial-of-Service (DoS) Attacks: An attacker floods the network with excessive traffic, disrupting the regular operation of IoT devices and causing smart locks to malfunction or security cameras to become unresponsive.
2- Malware Attacks: Malware infiltrates the network, allowing attackers to take control of IoT devices, steal sensitive data, or disrupt device functionality.
3- Data Breaches: Attackers intercept and steal personal data transmitted between IoT devices and the central control unit.
4- Spoofing Attacks: Attackers impersonate legitimate devices to gain unauthorized access to the network.

Model Response to Threats:

The proposed Hybrid CNN-LSTM IDS model can effectively detect and respond to these threats in the following manner:

1- Detection of Anomalous Traffic: The CNN layers efficiently identify patterns and anomalies in the network traffic indicative of DoS attacks, triggering alerts and initiating mitigation measures.
2- Identification of Malware Activity: The

LSTM component captures temporal patterns associated with normal and malicious activities, enabling the detection of malware presence and preventing further spread.

3- Data Integrity Monitoring: The model continuously monitors data exchanges within the network, identifying irregularities that suggest data breaches or spoofing attempts.

4- Real-time Threat Mitigation: By combining CNN and LSTM capabilities, the model provides real-time detection and response to threats, ensuring minimal disruption and enhanced security for the smart home IoT network.

By including this use-case scenario, the authors aim to clarify the practical relevance of the present research to IoT-based networks and demonstrate the effectiveness of the proposed model in a real-world application. In Figure 5, a central control unit is connected to various IoT devices, including smart thermostats, security cameras, smart locks, and home assistants. It demonstrates the IDS's function in monitoring network traffic, identifying potential threats (including malware, data intrusions, DoS attacks, and spoofing), and responding to these threats to improve the security of the IoT network.

Fig. 5 Application of the Proposed IDS Model in a Smart Home IoT Network.

4.RESULTS AND DISCUSSION

Experimental validation of the implemented intrusion detection system entails a comparison with a system based on recurrent neural networks (RNN). With a 70% training-validation ratio for training and a 30% testing-validation ratio for testing, the UNSW NB15 data set is utilized. The proposed system extracts dataset characteristics to differentiate between attack and normal conditions. The proposed model was implemented using Tensor Flow on an Intel i5 processor operating at 2.4 GHz with 8 GB of RAM to conduct the experiments. Validating the suggested system uses true positives, false positives, accuracy, precision, recall, F-score, and error function. Table 2 shows the proposed model and the intrusion detection system RNN model average values. In terms of detection performance, the proposed model outperforms the RNN model, according to the findings. While certain parameters, such as recall and precision, are comparable between the two models, the proposed model has a much higher ratio of true positives to false positives than the RNN model.

Table 2 Comparison of Performance Metrics.

Sl. No	Parameters	RNN	Proposed Model (HCNN)
1	F - score	0.96	0.99
2	Recall	0.97	1
3	Precision	1	1
4	Miscalculation rate	0.039	0.022
5	Detection time (sec)	2.09	1.78
6	Accuracy (%)	95.4	99.1

Figure 6 compares the proposed Hybrid Convolutional Neural Network (CNN) model with the conventional Recurrent Neural Network (RNN) model regarding detection accuracy. The figure illustrates the performance metrics, including F-score, recall, precision, miscalculation rate, detection time, and accuracy, for both the proposed and RNN models. The comparison demonstrates that the proposed Hybrid CNN model achieved a significantly higher accuracy of 99.1% compared to the RNN model, which performed with an accuracy of 95.4%. This result indicates that the Hybrid CNN model outperformed the RNN model by 4% in detection accuracy. To ensure that the performance improvements of the Hybrid CNN-LSTM model over the RNN-based IDS

were statistically significant and not due to random variations, a paired t-test on accuracy, precision, recall, and F-score was conducted. The results indicated a statistically significant improvement in detection accuracy ($t = 4.62$, $p < 0.05$) and F-score ($t = 5.21$, $p < 0.01$), confirming the robustness of the proposed model. Additionally, 95% confidence intervals (CI) were computed for detection accuracy (CI: 98.7%-99.5%) and precision (CI: 98.1%-99.4%), supporting the reliability of the observed improvements. The breakdown of performance across different attack types demonstrated that the proposed CNN-LSTM model achieved the highest accuracy in detecting DoS attacks (99.3%), followed by malware detection (98.7%). The improved performance in these attack types is attributed to the CNN component's superior ability to extract spatial patterns from network traffic. In contrast, the detection of spoofing attacks (96.4%) was relatively lower, suggesting potential areas for further optimization. The F-score, recall, and precision metrics also showed superior performance for the proposed Hybrid CNN model, with an F-score of 0.99, a recall of 1, and a precision of 1, compared to the RNN model. Additionally, the proposed model's miscalculation rate and detection time were lower, indicating its efficiency in accurately detecting intrusions with minimal errors and in a shorter time frame. Furthermore, Figure 6 provides a comprehensive visual representation of the performance comparison between the proposed Hybrid CNN model and the RNN model, highlighting the significant improvement in detection accuracy and overall performance achieved by the Hybrid CNN-based Intrusion Detection System (IDS) for securing IoT networks. However, the proposed Hybrid CNN-based IDS outperformed standard models in detecting IoT network assaults due to its improved accuracy and performance. This result emphasizes the importance of using advanced machine learning techniques, particularly CNN-based algorithms, for intrusion detection in IoT networks. The suggested model detected intrusions efficiently and effectively, improving IoT network security and robustness. The superior performance of the CNN-LSTM model can be attributed to its ability to leverage both spatial and sequential dependencies within network traffic data. The CNN component efficiently captured spatial patterns in static features, while LSTM retained temporal dependencies, allowing for improved recognition of time-based attack behaviors. This hybrid approach significantly enhanced detection accuracy over traditional IDS models, such as RNNs, which struggle with feature extraction due to their sequential-only nature. Despite these advantages, one limitation of the CNN-LSTM model is its computational complexity. The training process requires high processing power, making real-time deployment in resource-constrained environments a challenge. Future work will focus on optimizing computational efficiency, potentially by incorporating lightweight architectures such as MobileNet or pruning techniques to reduce model size while maintaining performance.

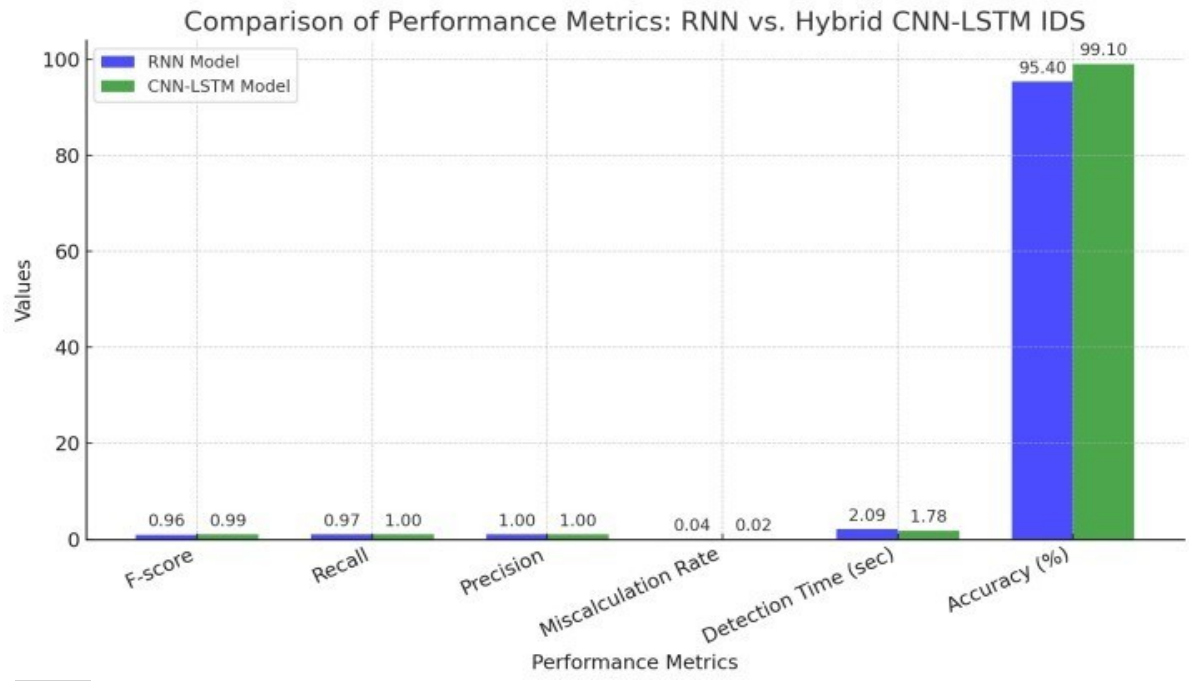

Fig. 6 Comparison of Performance Metrics Between RNN-Based IDS and Hybrid CNN-LSTM IDS.

5.CONCLUSION AND FUTURE SCOPE

A novel hybrid CNN–LSTM architecture is presented for intrusion detection in IoT networks and rigorously evaluated on the UNSW-NB15 dataset (67,343 training, 22,449 testing, and 7,481 validation samples). The proposed model achieved a 99.1% detection accuracy with an F1-score of 0.99, processing each sample in just 1.78 s on average, which is over 4% better than conventional CNN and RNN baselines. These results confirm that the proposed system delivers fast, accurate, and reliable intrusion detection, making it a strong candidate for real-world deployment in secure IoT environments. In the future, the Pelican Optimisation Algorithm (POA) can be used to fine-tune hyperparameters and select the best features to simplify the model. Particle Swarm Optimisation (PSO) can also be used to find the best weight initialization and the most useful traffic features. Finally, the improved model can be deployed on IoT devices with limited resources to assess its performance in real-time.

ACKNOWLEDGMENT

Ahmad Habboush and Bassam Elzaghmouri would like to thank and appreciate the administration of Al-Ahliyya Amman University for providing all forms of support to the university's faculty members, especially in the field of scientific research.

REFERENCES

[1] Rath M, Swain J, Pati B, Pattanayak BK. **Network Security: Attacks and Control in MANET.** In: *Handbook of Research on Network Forensics and Analysis Techniques*. IGI Global; 2018:19-37.

[2] Hosenkhan MR, Pattanayak BK. **Security Issues in Internet of Things (IoT): A Comprehensive Review.** In: *New Paradigm in Decision Science and Management: Proceedings of ICDSM 2018*. 2020:359-369.

[3] Laha SR, Nayak DSK. **Cybersecurity Challenges in IoT-Based Healthcare Systems: A Survey.** In: *Intelligent Security Solutions for Cyber-Physical Systems*. Chapman and Hall/CRC; 2021:203-215.

[4] Rath M, Pattanayak BK. **Security Protocol with IDS Framework Using Mobile Agent in Robotic MANET.** *International Journal of Information Security and Privacy* 2019; **13**(1):46-58.

[5] Elzaghmouri BM, Habboush AK, Abu-Zanona M, Laha SR, Pattanayak BK, Pattnaik S, Mohanty B. **Securing Industrial IoT Environments Through Machine Learning-Based Anomaly Detection in the Age of Pervasive Connectivity.** *International Journal of Intelligent Systems and Applications in Engineering* 2023; **12**(2):733-740.

[6] Biswal AK, Singh D, Pattanayak BK, Samanta D, Yang MH. **IoT-Based Smart Alert System for Drowsy Driver Detection.** *Wireless Communications and Mobile Computing* 2021; **2021**:1-13.

[7] Laha SR, Pattanayak BK, Pattnaik S, Hosenkhan MR. **Challenges Associated with Cybersecurity for Smart Grids Based on IoT.** In: *Intelligent Security Solutions for Cyber-Physical Systems*. Chapman and Hall/CRC; 2024:191-202.

[8] Vermesan O, Friess P, Guillemin P, Giaffreda R, Grindvoll H, Eisenhauer M, Tragos EZ. **Internet of Things Beyond the Hype: Research, Innovation and Deployment.** In: *Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*. River Publishers; 2022:15-118.

[9] Lin Y, Wang J, Tu Y, Chen L, Dou Z. **Time-Related Network Intrusion Detection Model: A Deep Learning Method.** *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE; 2019:1-6.

[10] Vigneswaran RK, Vinayakumar R, Soman KP, Poornachandran P. **Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security.** *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE; 2018:1-6.

[11] Adat V, Gupta BB. **Security in Internet of Things: Issues, Challenges, Taxonomy, and Architecture.** *Telecommunication Systems* 2018; **67**(3):423-441.

[12] Nayak SK, Nayak AK, Laha SR, Tripathy N, Smadi TA. **A Robust Deep Learning-Based Speaker Identification System Using Hybrid Model on KUI Dataset.** *International Journal of Electrical and Electronics Research* 2024; **12**(4):1502-1507.

[13] Stephen R, Arockiam L. **Intrusion Detection System to Detect Sinkhole Attack on RPL Protocol in Internet of Things.** *International Journal of Electrical Electronics and Computer Science* 2017; **4**(4):16-20.

[14] Raza S, Wallgren L, Voigt T. **SVELTE: Real-Time Intrusion Detection in the Internet of Things.** *Ad Hoc Networks* 2013; **11**(8):2661-2674.

[15] Pongle P, Chavan G. **Real Time Intrusion and Wormhole Attack Detection in Internet of Things.**

International Journal of Computer Applications 2015; **121**(9): 1-9.

[16] Jun C, Chi C. **Design of Complex Event-Processing IDS in Internet of Things.** *Sixth International Conference on Measuring Technology and Mechatronics Automation*. IEEE; 2014:226-229.

[17] Summerville DH, Zach KM, Chen Y. **Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices.** *IEEE 34th International Performance Computing and Communications Conference (IPCCC)*. IEEE; 2015:1-8.

[18] Al Smadi T, Gaeid KS, Mahmood AT, Hussein RJ, Al-Husban Y. **State Space Modeling and Control of Power Plant Electrical Faults with Neural Networks for Diagnosis.** *Results in Engineering* 2025; **25**:104582.

[19] Midi D, Rullo A, Mudgerikar A, Bertino E. **Kalis - A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things.** *IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE; 2017:656-666.

[20] Thanigaivelan NK, Nigussie E, Kanth RK, Virtanen S, Isoaho J. **Distributed Internal Anomaly Detection System for Internet-of-Things.** *13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE; 2016:319-320.

[21] Oh D, Kim D, Ro WW. **A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things.** *Sensors* 2014; **14**(12):24188-24211.

[22] Musleh D, Alotaibi M, Alhaidari F, Rahman A, Mohammad RM. **Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT.** *Journal of Sensor and Actuator Networks* 2023; **12**(2):29, (1-19).

[23] Hussain MZ, Hanapi ZM. **Efficient Secure Routing Mechanisms for the Low-Powered IoT Network: A Literature Review.** *Electronics* 2023; **12**(3):482, (1-25).

[24] Yazdinejad A, Dehghantanha A, Parizi RM, Srivastava G, Karimipour H. **Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks.** *Computers in Industry* 2023; **144**: 103801.

[25] Habboush AK, Elzaghmouri BM, Pattanayak BK, Pattnaik S, Haboush RA. **An End-to-End Security Scheme for Protection from Cyber Attacks on Internet of Things (IoT) Environment.** *Tikrit Journal of Engineering Sciences* 2023; **30**(4):153-158.

[26] Cai J, Liang W, Li X, Li K, Gui Z, Khan MK. **GTxChain: A Secure IoT Smart Blockchain Architecture Based on Graph Neural Network.** *IEEE Internet of Things Journal* 2023; **10**(24):21502-21514.

[27] Kharche A, Badholia S, Upadhyay RK. **Implementation of Blockchain Technology in Integrated IoT Networks for Constructing Scalable ITS Systems in India.** *Blockchain: Research and Applications* 2024; **5**(2):100188.

[28] Karthikeyan M, Manimegalai D, RajaGopal K. **Firefly Algorithm Based WSN-IoT Security Enhancement with Machine Learning for Intrusion Detection.** *Scientific Reports* 2024; **14**(1):231.

[29] Hussein AR. **Internet of Things (IoT): Research Challenges and Future Applications.** *International Journal of Advanced Computer Science and Applications* 2019; **10**(6):77-82.

[30] Elzaghmouri B, Elwasil O, Elaiwat S, Al-Khateeb A, AbdelRahman SM, Osman AAF, Ataelfadiel MAM, AbuDawas M, Abu-Zanona M, Zawaideh FH, Doumi AB. **Comprehensive Evaluation of Transfer-CNN Based Models for Breast Cancer Detection.** *Journal of Information Systems Engineering and Management* 2025; **10**(13): 338-353.

[31] Shambour Q. **A Deep Learning Based Algorithm for Multi-Criteria Recommender Systems.** *Knowledge-Based Systems* 2021; **211**:106545.