CNN and RNN-LSTM Algorithms for the Detection Threats in IoT

Nouf Bader Aljabri and Omar H Alhazmi

College of Computer Sciences and Engineering .Taibah University, MEDINA , SAUDI ARABIA
College of Computer Sciences and Engineering.Taibah University, MEDINA , SAUDI ARABIA

Abstract
Recently, the Internet of Things (IoT) had significant influence and much interest in many industrial sectors, including smart cities, healthcare fields, and automobiles. IoT devices generate a huge amount of data that gets transmitted across public networks. However, these devices are susceptible to various cyber threats due to their physical diversity and lack of security mechanisms. This research presents an IoT cyber threats detection system based on the Deep Learning (DL) model. DL has proven to be a powerful approach for effectively addressing and preventing cyberattacks on IoT infrastructure. The proposed system serves a critical role in protecting sensitive information by identifying and mitigating malicious activities. This paper focuses on the proposed detection system carrying out RNNs with LSTM and CNNs using the UNSW-NB15 dataset and the results show that the proposed system based on CNN and RNN-LSTM algorithms when including HashFeature significantly outperformed when including Principal Component Analysis (PCA) in all evaluation metrics.

Keywords
Internet of Things, Cyber Threats, CNN, RNN, LSTM, Attack detectio

1. Introduction

An IoT is a pivotal force in modern technology, transforming various aspects of daily life by facilitating effective interaction between individuals and devices everywhere, all the time. IoT is a wireless technology that integrates various objects over a network to send and receive. These physical objects are embedded in sensors, and actuators interconnected through wired and wireless networks. Each object acts as a sensor, produces output, collects data from its environment, and transfers them to other objects without human intervention.

An IoT operates through a multi-layered architecture that consists of perception, network, and application layers. At every layer, security principles need to be implemented to guarantee the steadiness and integrity of the IoT [1]. While the IoT offers various services and applications, it confronts security challenges, particularly attacks. Despite the security measures employed between users and IoT devices, concerns persist. Moreover, IoT security devices and networks must be continuously monitored and analyzed to mitigate potential risks and prevent damage to system components, which could result in unacceptable threats.

IoT cybersecurity threats are defined as cybercriminal activities targeting the IoT infrastructure. IoT cyberattacks, especially those involving hackers and security breaches, have gained increased visibility. Privacy concerns emerge when sensitive information is lost or intercepted, regardless of whether it occurs through legal ac-cess or not. An IoT attack is an activity done by an attacker to exploit vulnerabilities in the hardware, software, or communication protocols of IoT devices.

In recent years, Machine Learning (ML) and DL have made significant progress in IoT cyber threats. Leveraging these intelligent systems, organizations can detect threats in real time and enhance accuracy in identifying vulnerabilities. Moreover, ML and DL models can learn and adapt to emerging attack vectors, making them highly effective in tackling the evolving and complex landscape of IoT cybersecurity. This advancement in threat detection significantly helps in better safeguarding IoT networks from potential breaches, ensuring a more secure and resilient infra-structure.

This paper aims to detect cybersecurity threats in recent technology and identify vulnerabilities within organizations by utilizing intelligent systems and DL techniques that cannot be addressed effectively by traditional techniques.

1.1 Background

The area of computer science has seen significant growth in the realm of interconnected systems and devices, especially with the emergence of IoT. IoT is a rapidly advancing technology with diverse applications across numerous fields. It integrates various objects over a network for the purpose of sending and receiving information. These objects, which are physical devices embedded with sensors and actuators, are interconnected through both wired and wireless networks. Each object functions as a sensor, gathering data from its environment, making decisions, and transmitting the collected information to other devices within the network. However, this interconnected nature presents considerable security challenges, which makes IoT systems highly vulnerable to cyber threats.

Manuscript received April 5, 2026
Manuscript revised April 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.4.13

Recent improvements in artificial intelligence (AI) encompasses DL which has emerged as a promising in enhancing cybersecurity measures, particularly in the context of identifying and addressing cyber threats within IoT environments. In contrast to conventional rule-based approaches, DL algorithms can analyze large datasets and identify anomalies that could indicate potential security breaches. Importantly, these models can adapt to new and evolving threats, thereby offering a more resilient defense against advanced cyber-attacks that frequently bypass traditional security techniques.

The significance of IoT cybersecurity is highlighted by its practical applications and real-world impact. As IoT devices become increasingly common in essential infrastructure and personal environments, securing these systems to protect privacy and data is essential. Cyber-attacks targeting IoT networks can result in data leaks, financial damage, and even potential physical risks. Consequently, deploying DL-based threat detection in IoT networks is a vital research focus in computer science and crucial for safeguarding sensitive data and maintaining the integrity of essential systems in our connected world.

Real Word Applications of Cyber Threats Detection Based DL Model

- Smart Healthcare Systems

IoT technologies was widely integrated into health sector, such as medical records, and ,wearable health trackers collects, store , and transmit sensitive patient data. However, Cyber threats aimed at these systems may lead to unauthorized access to medical records or even malicious manipulation of device functions. DL-based security resolutions can analyze network behavior and identify anomalies, such as unauthorized access attempts or abnormal device activity, guaranteeing patient data protection and medical devices' integrity.

- Industrial IoT (IIoT) and Smart Manufacturing

In industrial environments, sensors and connected devices enable predictive maintenance, process automation, and remote monitoring. Cyber-threats on these systems Poses significant security challenges that require advanced solutions such as DL-driven intelligence-based approaches for detecting and preventing cyber threats.

- Smart Home and Consumer IoT

IoT plays a crucial role smart home such as, Smart locks, and Smart Thermostats. Cyber-attacks on these systems can results in unauthorized surveillance, data breaches, or even home intrusions. DL-based security frameworks can monitor abnormal user behavior to protect household privacy and security.

- Smart Cities and Public Infrastructure

The growing adoption of IoT devices smart cities for applications like traffic monitoring, smart transportation, and smart waste management. Cyber threats against these systems can disrupt essential services, such as emergency response systems, and smart traffic control systems. DL-based intrusion detection systems can detect cyber threats in real time and guarantee security of smart city infrastructure.

Security has always been an essential aspect of humanity, leading to the creation of laws and regulations to ensure the well-being and comfort of individuals. With the rise of technology, security has become a top priority in designing various technologies, such as smart devices, tracking systems, and control systems, all aimed at improving human life. The IoT has further underscored the significance of security, especially with the sensitive information exchanged in areas like banking and healthcare. Despite this technology's benefits, there is a growing concern about cyber threats exploiting vulnerabilities. International organizations are working on protocols to enhance security, considering challenges like hardware limitations and network infrastructure. Extensive research is being conducted to improve efficient security protocols and algorithms, emphasizing the ongoing significance of advancing security measures in the digital era.

IoT layered architecture

IoT and its inherent heterogeneity demand a layered architecture. IoT architectures refer to the structure and design of IoT systems, where various tasks and processes are structured into unique layers. Each layer serves a distinctive purpose and is com-posed of particular components that contribute to the overall functionality and effectiveness of the IoT system. While different models exist, the most common IoT architecture frameworks are mainly based on a five-layer approach [2].

Five-layer architecture

Is a widely recognized framework that organizes the components and processes in-volved in IoT systems into five distinct layers.

•**Perception layer:** This is the physical layer that has sensors for sensing and collecting data about an environment. This layer acts as the foundation for IoT systems by identifying other smart objects.

•**Network layer:** This layer is responsible for distributing the data obtained by the perception layer to other systems or devices for processing. Additionally, it ensures that all data is transmitted securely and reliably across the network.

•**Processing Layer:** This layer is responsible for storage, processing, and analysis of Responsible for analyzing, processing, and storing the data received from the network layer.

•**Application layer:** This layer provides application-specific services to the user.it converts the processed data into practical insights, enabling real-time monitoring, control, and decision-making.

•**Business layer:** This layer defines the business logic and rules that guide the operation of the IoT system. It includes business processes, rule engines, and analytical tools used

to interpret data generated by IoT devices and enable informed decision-making.

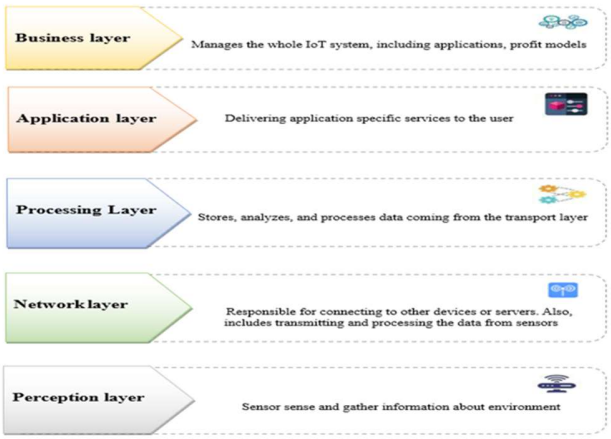

Figure 1. Five IoT Layer architecture

1.2 Problem Statement

The increasing adoption of IoT devices Varying from intelligent home appliances to industrial sensors generates enormous amounts of data that can be hard to analyze in real-time, which greatly raises the risk of cyber threats targeting these devices. Conventional cybersecurity techniques frequently face challenges safeguarding IoT ecosystems because of their distinct features such as decentralized structures, limited resources, and various protocols. These restrictions make IoT networks vulnerable to various cyberattacks like DDoS attacks, malware infections, and phishing, which led to significant operational disruptions and data breaches [3]. The primary concern revolves around developing real-time, scalable, effective detection systems that can identify and mitigate threats on IoT devices without overwhelming their limited computing and power resources [4]. This research contributes to investigating DL algorithms for addressing and mitigating cyber threats in IoT networks, focusing on accuracy, scalability efficiency, and real-time response, while applying the models to real-world datasets to enhance the security of IoT systems.

1.3 Research Questions

- What methodologies can be used to enhance IoT cyber threat detection?
- How can DL techniques be continuously updated to detect new and emerging cyber threats in IoT environments?
- How can IoT real-time datasets be efficiently utilized to train and assess the performance of cyber threats detection systems?
- What evaluation metrics are most suited for assessing the performance of DL models in IoT cyber threats detection, and how do these metrics accurately capture the effectiveness and reliability of these models in real-time scenarios?

1.4 Research Objectives

- To identify and develop methodologies that can enhance IoT cyber threat detection models.
- To investigate how DL techniques can be continuously updated to detect new and emerging cyber threats in IoT environments.
- To explore the efficient utilization of real-time IoT datasets for training and assessing the performance of cyber threat detection models.
- To determine the most suitable evaluation metrics for assessing the performance of DL models in IoT cyber threat detection and analyze how these metrics accurately capture the models' effectiveness and reliability in real-time scenarios.

1.5 Contribution

- Developing cyber-attacks detection in IoT network by developing DL models on recent IoT datasets.
- Enhancing the accuracy and performance of DL model by optimizing model configurations and training methods to effectively identify and mitigate cyber threats.
- Comparative analysis of the proposed model against existing models focusing on cyber threats detection IoT environment, demonstrating the proposed model's enhancement over current solutions.
- Utilizing a hashing algorithm to significantly reduce the large data generated by the sensors in IoT environments. By reducing this data, the system's efficiency in storage and transmission is improved, resulting in better performance and scalability for IoT applications.

1.6 Scope and limitations

- Scope

This research focuses on the development and evaluation of DL models tailored for IoT cyber threats detection. These models evaluate on recent IoT datasets.

- Limitations
  - Testing the proposed model on diverse IoT-specific datasets, where variations in attack types, sophisticated attacks, and the presence of missing data.
  - Semi-supervised machine learning and federated learning approaches remain underexplored for detecting malicious attacks

in IoT environment. Furthermore, there is a significant lack of a comprehensive cyber-detection system that provides the necessary scalability, accuracy, and protection to defend against a wide range of malicious threats.

Our paper is structured as follows:

- The first section provides a brief introduction that includes the study's background, problem statement, research questions, research objectives, and contribution.
- The second section presents the project literature of several recent articles where background and related work of similar studies are discussed.
- The third section presents the research methodology as a sequence of phases and discusses each phase.
- The fourth section presents the results and discussions.

2. Literature Review

In this Section, we provide a literature review of recent studies on IOT cyber threat detection. We discuss each study's objectives and the problem to be solved. We also present the datasets and methods used in the study and their performance. We high-light the study's limitations and suggest directions for future studies.

[5] combine the Mayfly optimization (MFO) with regularized extreme learning machine (RELM) to produce a new model called the MFO-RELM model to identify the concern of identifying and categorizing cybersecurity threat in an IoT environment. The MFO-RELM approach shows significant effectiveness in detecting and evaluating cybersecurity vulnerabilities. The N-BaIoT dataset was utilized with MFO-RELM model to address cyber threats within the IoT infrastructure. The results show that the proposed model is better than other methods. However, the dataset is limited. The researchers also suggest could include using different clustering and outlier removal techniques to further enhance the performance of the MFO-RELM model.

[3] addressed the growing security concerns associated with the IoT, emphasizing the need for ML-based security measures to counter various cyber-attacks, such as denial-of-service, malware, and phishing. They employ a Ridge Classifier as the primary model for addressing anomalies within IoT systems on the ability to identify and detect attacks in real-time accurately. The publicly available dataset UNSW-NB15, showcases its ability to identify and predict attacks in real time accurately. By utilizing this approach, the system demonstrates a high detection accuracy of 97%. However, they rely on a single dataset, which is smaller compared to real-world scenarios, and focus solely on network traffic data without incorporating other sources like system logs or user behaviour. They also plan on expanding the data scope and applying more advanced techniques to further strengthen IoT network defenses. Similarly, [6] proposes an ML-based approach to identify security threats in IoT networks by leveraging the large volumes of data generated by IoT devices. By evaluating models on labelled datasets containing both normal and attack pat-terns, the system is designed to recognize potential security threats and respond promptly. The authors evaluate multiple machine learning models using binary and multiclass classification techniques to capture the variety of attacks in IoT environments. A dataset from Wheelus and Zhu, reflecting real-world conditions, was created for identifying and classifying IoT network assaults. Key feature selection and normalization methods, such as correlation and information gain, were employed. The models tested included Bagging, KNN, J48, Random Forest (RF), Logistic Regression (LR), and Multilayer Perceptron (MLP). The RF model accomplished the highest performance with a 99.9% ROC score, particularly excelling in binary classification tasks. However, they should focus on real-time attack detection and expanding datasets to cover a wider range of attack types, further improving the resilience of IoT security systems. In addition,[7] introduce an innovative method combining machine learning and neural network algorithms, such as gradient boosting, CNNs, LSTMs, and RNNs, trained on the Edge-IIoTset dataset. These models were evaluated using accuracy, precision, recall, and F1-score, with gradient boosting achieving the highest accuracy of 93%. Findings highlight the effectiveness of ML and DL for detecting and preventing cyber threats in IoT environments, emphasizing their ability to understand complex data patterns. Future research will focus on im-proving cyber threat detection through ensemble learning, anomaly detection, and explainable AI. It will address challenges like class imbalance and data scarcity. This aims to enhance the resilience and reliability of IoT cybersecurity when the model's performance is tested in a dynamic setting. Similarly,[8] presents a frame-work for detecting malicious traffic using three machine learning models: SVM, Gradient Boosted Decision Trees (GBDT), and RF. The NSL KDD dataset was used to evaluate the models, with RF achieving the highest accuracy at 85.34%. In future, they plan to focus on testing different IoT devices and expanding dataset use for cyber-attack detection. Same as, [9] evaluate several ML algorithms for detecting IoT network attacks using the Bot-IoT dataset. They applied seven machine learning algorithms, including KNN, ID3 (Iterative Dichotomiser 3), RF, AdaBoost, Quadratic discriminant analysis (QDA), Multilayer perceptron (MLP), and Naïve Bayes (NB), achieving high performance with F-measure scores ranging from 0.77 to 0.99. Feature extraction was performed using CICFlowMeter, and feature importance was calculated using the Random Forest Regressor. The performance metrics, measured by F-measure, varied across algorithms, with K-Nearest

Neighbors achieving the highest score of 0.99. At the same time, Random Forest, ID3, and AdaBoost also demonstrated strong performance with scores of 0.97. They will explore unsupervised learning algorithms and investigate multi-layered models to enhance detection capabilities.

[10] explore the use of machine and deep learning algorithms to detect security threats in IoT networks using the BoT-IoT dataset. They assessed ten ML models, including two single classifiers (KNN and SVM) and eight ensemble classifiers (e.g., RF, Extra Trees, AdaBoost, LGBM), as well as four DL models (LSTM, GRU, RNN). To detect the challenge of imbalanced network traffic data, the SMOTE (Syn-thetic Minority Over-sampling Technique) algorithm is applied. Notably, the Cat-Boost and XGBoost classifiers achieved high accuracy rates of 98.19% and 98.50%, respectively, outperforming deep learning models. However, they require to com-pare distributed DL models with numerous datasets. In the future, they also plan to focus on addressing mobile network intrusions, employing ensemble learning, feature engineering, and optimization techniques to enhance detection capabilities.

[4] address the need for improved cyber-attack detection in IoT-based Cyber-Physical Systems (CPS). However, the SVM model's reliance on past data limits its ability to handle evolving cyber threats. To address this, the study proposes a new DL-based Convolutional Neural Network (CNN) model using the UNSW-NB15 dataset in Python. The CNN model enhances cyber-attack detection, outperforming the SVM model in terms of accuracy, precision, recall, and F1-score. This approach offers better adaptability and effectiveness in responding to dynamic cyber-attacks, making it a promising advancement for securing IoT-based CPS.

[11] address the growing cybersecurity challenges in IoT networks, particularly against Distributed Denial of Service (DDoS) attacks. Using the CIC-IoT2023 dataset, they evaluate four machine learning models (LR, KNN, DT, RF) for detecting IoT cyber threats. Results show that DT and RF are the most effective, achieving high accuracy rates of 0.9919 and 0.9916, with excellent precision, recall, and F1-scores, making them reliable for distinguishing between benign and malicious traffic. KNN also performed well, while LR showed the lowest accuracy at 0.8275. They highlight future recommendations for integrating unsupervised learning, deep learning models, and federated learning techniques to improve scalability and adaptability in addressing evolving cyber threats.

[12] introduce a combined DL approach to address software piracy and malware attacks in IoT networks. It uses TensorFlow deep neural networks to detect software piracy by identifying source code plagiarism, employing tokenization, and weighting methods to filter noise and highlight key tokens. The dataset for piracy detection is sourced from Google Code Jam (GCJ). Additionally, the approach uses CNNs to detect malware by visualizing malware files as color images. These malware samples are taken from the Maling dataset, which is processed using a CNN to identify malicious infections in IoT networks. The results show that the proposed approach exceeds existing methods regarding classification accuracy for both piracy and mal-ware detection. They suggest utilizing abstract syntax trees and control flow graphs to enhance the detection of pirated software and focus on developing algorithms to identify malware from previously unknown families.

[13] presented a comparative analysis of cyber-attack detection methodologies employing machine learning and deep learning algorithms. They evaluate six models: RF, LR, SVM, NB, KNN, and MLP across various datasets, including Power System and BotNet attack datasets. They used three datasets from the ICS Cyber-attack Dataset collection for the Power System dataset. Each model's performance was assessed using precision, recall, F-score, and ROC metrics. Results indicate that Random Forest outperformed the other models regarding accuracy and efficiency, while KNN exhibited higher computational demands and lower accuracy. They will focus on enhancing real-time attack detection through ensemble techniques.

[14] present an advanced approach utilizing RNNs to improve the detection of these attacks. By training the RNN model on the UNSW-NB15 dataset, the proposed method achieves a remarkable 99.99% accuracy in addressing DoS and DDoS at-tacks and 98% accuracy in identifying various attack patterns. Performance evaluation using metrics such as precision, recall, accuracy, and F1-measure shows the RNN model's effectiveness, with a high accuracy rate and a minimal loss rate of 0.003, underscoring its effectiveness in multi-class classification for IoT network security.

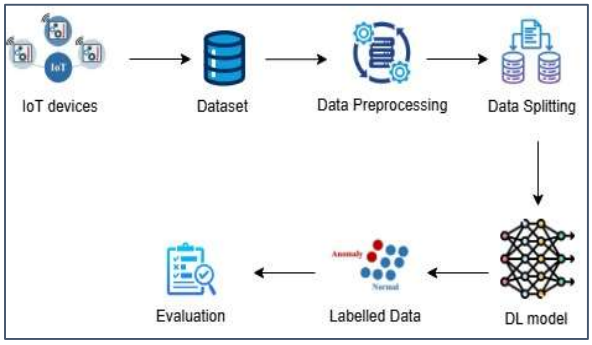

Figure 2. Proposed Approach Overview

[15] introduces a diverse range of interconnected devices, increasing vulnerability to various risks, including insider attacks. They propose an advanced IoT attack detection model utilizing an optimized RNN enhanced by the Self-Improved Whale Optimization Algorithm (SI-WOA). The SI-WOA improves the RNN's weight optimization, leading to superior attack detection accuracy. The model was assessed using the KDD Cup 1999 dataset and compared against various existing methods, including NB, ANN, DBN, LSTM, SVM, RF, and several RNN variants. The SI-WOA-enhanced RNN demonstrated the highest accuracy in

detecting attacks, at-tributed to its optimized features such as statistical metrics, Relief, mutual information, and improved correlation. This approach outperforms existing models, underscoring its effectiveness in enhancing IoT network security.

The rapid expansion of the IoT raises significant security challenges, such as managing individual device security and updating defenses against evolving threats becoming increasingly complex. Traditional security measures often fail due to their reliance on outdated datasets and limited attack coverage. [16] Address these limitations by introducing a novel security framework utilizing DL to detect IoT attacks effectively. The proposed framework employs CNN to extract features from data and an LSTM model for classification. Evaluated on an IoT-23 dataset from twenty Raspberry Pi-infected IoT devices, the framework achieved an impressive 96% accuracy. They demonstrate that the proposed model outperforms existing DL-based detection mechanisms and can efficiently scale with additional IoT sub-networks. It also avoids common issues like underfitting and overfitting, making it a robust solution for identifying and mitigating various IoT attacks and their variants.

3. Research Methodology

If

The system design for IoT cyber threat detection utilizing a DL approach consists of multiple connected components to ensure effectiveness and scalability. This design concentrates on analyzing IoT data in real-time, identifying possible cyber threats, and addressing risks through automated responses. The figure below illustrates the system design

- **IoT devices:** These devices generate substantial amounts of data and serve as the primary source of datasets for analysis.
- **Dataset:** in this stage, the publicly available dataset UNSW-NB15 is used to assess the proposed model. This dataset is widely used for developing anomaly detection methods, measuring intrusion detection systems, and training ML and DL models. It contains nine distinct attack categories: Fuzzers, Analysis, Backdoor, Denial of Service (DoS), Exploits, Generic, Reconnaissance, Shellcode, and

Figure 3. Proposed Approach Overview

Worms. It also includes non-anomalous packets, with over 87% of the packets classified as non-anomalous, making the dataset significantly imbalanced. This dataset contains 49 features that include six groups called the Basic Features, Flow Features, Time Features, Content Features, Labelled Features and Additional Generated Features.

- **Data pre-processing:** Is the critical step in preparing the UNSW-NB15 dataset for DL-based IoT cyber threat detection. The raw dataset which contains a mixture of normal and malicious network traffic, requiring to be cleaned and transformed in order to make sure it is appropriate for training a model. This step includes:
  - Data Cleaning: is the process of removing inconsistent, duplicate, errors entries and handling the missing values to guarantee the integrity of the dataset which is crucial for training deep learning models effectively.
  - Normalization: is applied to scale numeric feature to fall within a consistent range, typically [0, 1] to guarantee that all features participate equally to the learning process in DL model.
  - Encoding: this step converts the categorical features into numerical representations through encoding techniques.
  - Features Selection: this step involves identifying the most relevant features to reduce noise and eliminating irrelevant or redundant features. This step guarantees improving model performance by focusing on most critical features.
- **Data Splitting:** is a critical step of building a DL model for IoT cyber threats detection. The pre-processed dataset is divided into three subsets:
  - Training set: used to train the DL model, making it to learn patterns from the labelled data.
  - Validation set: is a subset of the training data to assess the performance of DL through hyperparameter tuning and model selection.
  - Test set: This is used to estimate the model's performance on unknown data, simulating its ability to detect threats in an operational IoT environment.
- **DL model:** the DL model analyzes the UNSW-NB15 dataset to address the cyber threats. Different methods are used for identifying various IoT threats to ensure
- **Labelled Data:** is essential for supervised learning, where the output DL model is labelled as either normal or malicious activity.
- **Evaluation:** This step assesses the model's performance using various metrics and ensures it

achieves the desired accuracy, and performance before deployment.

Effectively detecting IoT cyber threats using DL requires the integration of various algorithms, methods, and tools. These components are carefully selected to adapt to evolving cyber threats in IoT environments.

- **Convolutional Neural Network (CNN)**

It is one of the most important networks and widely used in the DL field. It is designed to extract the features from a large dataset automatically. CNN in IoT cybersecurity plays a vital role in addressing anomalies and classifying malicious behaviors. The network utilizes convolutional layers to identify key features, such as anomalies in traffic patterns or unauthorized access attempts, while pooling layers minimize the size of the data, preserving critical indicators of threats. At the final stage, fully connected layers categorize the input data into classes such as normal or malicious activities. By utilizing CNNs, IoT cybersecurity systems achieve high accuracy, adaptability, and efficiency, ensuring robust protection against advanced threats while maintaining the integrity of connected devices.

- **Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM)**

RNNs are neural networks that processes sequence data by storing information from previous inputs using a recurrent architecture. They are particularly effective for tasks involving time-series data, such as detecting behavioural anomalies in IoT over time. However, traditional RNNs suffer from challenges such as vanishing gradients, which limit their ability to learn long-term dependencies.

To address these limitations, LSTM networks were developed as an advanced extension of RNNs. LSTM utilize memory cells which is controlled by input, forget, and output gates. These gates enable them to selectively retain or discard information over extended periods. This ability allows LSTMs particularly useful for analyzing IoT data, where addressing anomalies requires an in-depth understanding of sequential dependencies. The combination of RNNs and LSTMs enables IoT cybersecurity systems to efficiently detect sequential anomalies and adapt to emerging threat patterns, ensuring reliable and real-time threat mitigation.

- **TensorFlow**

is a machine-learning framework designed for advanced computations in a complex environment. It supports the implementation of various DL algorithms in IoT cyber and threat detection through its specific application programming interfaces (APIs). TensorFlow facilitates the development of modern architectures such as CNNs, RNNs, and LSTM networks, which are essential for analyzing complex IoT data, identifying anomalies, and classifying cyber threats. TensorFlow offers tools for data preprocessing, including normalization and feature extraction, which are essential for transforming raw IoT data into a format suitable for analysis. Moreover, TensorFlow facilitates transfer learning and retraining, enabling models to adapt and effectively respond to emerging cyber threats.

The implementation of the IoT cyber threat detection system using deep learning will involve a strategic integration of technologies, platforms, and programming languages. This plan provides a detailed framework of the structured steps necessary for development and testing.

- **Python:** is a core programming language well-suited for developing IoT cyber threat detection systems. It provides a wide range of libraries specifically designed to optimize processes such as data preprocessing and deployment, establishing it as an essential tool for modern application development.
  - **Keras:** is a high-level DL API built on top of TensorFlow. Its Focus on simplicity makes it ideal for quick experimentation. It can also support a multi-layer perceptron (MLP).
  - **Scikit-learn:** An open-source Python library that crucial in preparing raw IoT data for analysis. Its tools for normalization, dimensionality reduction, and feature selection help to clean and structure the data, making it suitable for deep learning models.
  - **TensorFlow:** is a more complex library for advanced computations in a complex environment. It supports the implementation of various DL algorithms in IoT cyber threats detection. TensorFlow facilitates transfer learning and retraining, enabling models to adapt and effectively respond to emerging cyber threats.
- **Visual Studio code (VS code):** is one of the most popular and powerful lightweight code editors that is well-suited for developing IoT cyber threat detection systems. VS Code supports a wide range of languages, including Python. It offers powerful tools for coding, debugging, and deploying applications. Moreover, VS code provides functionality and facilitates the combination of frameworks such as TensorFlow, and Keras, supporting the implementation of advanced IoT cyber threat detection.

3. results and disccusion

The implementation of the proposed IoT cyber threat detection system was performed by using python language because of its robust support for data analysis and ML libraries. The DL models were developed using TensorFlow 2.x and the Keras API, which provided a high-level interface for constructing and training neural networks.

Additional libraries such as Pandas and NumPy were employed for data loading and manipulation, Matplotlib for effectiveness visualization, and Scikit-learn for tasks including label encoding, feature hashing, dimensionality reduction, and model evaluation. The system architecture was designed into modular components consisting of data preprocessing, feature transformation, model building training, and evaluation. The preprocessing module handled data cleaning, conversion of categorical variables using Feature Hashing, and normalization using StandardScaler. A flexible model pipeline was created using the Sequential class from Keras, supporting both a CNN and a hybrid RNN-LSTM architecture. The CNN model used stacked Conv1D, MaxPooling1D, Flatten, and Dense layers to extract certain features, while the RNN-LSTM model combined SimpleRNN and LSTM layers to capture temporal dependencies in the sequence data. A unique evaluation function was implemented to compute and present performance metrics including accuracy, precision, recall, F1-score, confusion matrix, classification report, and ROC curve, guaranteeing comprehensive model evaluation. The figure 3 shows the workflow of our system.

The implementation and evaluation of the proposed IoT cyber threat detection model were deployed on a local computing environment prepared with an Intel Core i7 11th generation processor 2.80 GHz, 8 cores, 16 GB of RAM, and an NVIDIA GeForce RTX 3050 GPU with 4 GB of dedicated memory. This hardware configuration provided appropriate computational capacity for training and testing

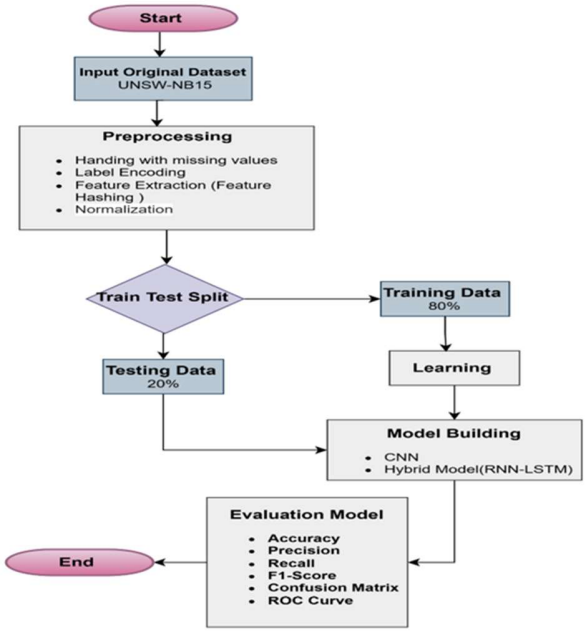

Figure 4 Flow diagram for IoT Cyber Threats Detection System

DL models including CNN and RNN with LSTM. The software environment was based on the Windows 10 (64-bit) operating system, with Python 3.10 used as the primary programming language. The DL models were developed using TensorFlow 2.x and the Keras API. The software environment was built around the Windows 10 (64-bit) operating system, with Python 3.10 serving as the major programming language. The deep learning models were built with TensorFlow 2.x and the Keras API. NumPy and Pandas were used to manipulate data, Scikit-learn for preprocessing and metric evaluation, Matplotlib for display, and OS for system configuration. Conv1D, LSTM, SimpleRNN, Dense, Dropout, and Sequential were imported from keras._tf_keras.keras.layers, and to_categorical was used to generate multi-class target labels. In addition, the TensorFlow environment variable TF_ENABLE_ONEDNN_OPTS was set to '0' to ensure stable and consistent functioning during training. This constant hardware and software configuration ensured the dependability, and efficiency of all experiments.

To assess the effectiveness of proposed IoT cyber threats detection system, a sequence of experimental procedures was implemented on the UNSW-NB15 dataset. The dataset was preprocessed and then partitioned into training and testing sets (80% training, 20% testing) This partition ensured that the model was properly trained, and evaluated on unseen data to prevent overfitting and measure generalization capability. CNN and ensemble model combine RNN with LSTM, were implemented using the Keras API on TensorFlow. Key hyperparameters were empirically tuned and carefully chosen: the model was trained for 10 epochs, the batch size was fixed at 32, and the learning rate was set to 0.001. Adam was employed as an optimizer due to its efficiency and adaptive learning capabilities. Dropout layers were used to minimize overfitting. For control conditions, a baseline model was created and trained using a simple feedforward neural network in identical situations. This enabled a direct performance comparison of traditional and sequential DL algorithms. Evaluation metrics such as accuracy, precision, recall, F1-score, and latency were recorded for both the proposed and baseline models to guarantee a fair and comprehensive assessment.

To measure the effectiveness of the IoT cyber threats detection system, evaluation metrics and datasets will be employed. This provides a comprehensive understanding in detecting and mitigating IoT cyber threats. Let TP, TN, FP, and FN denote true positive, true negative, false positive, and false negative. These metrics are defined as follows:

- **Accuracy:** assess the proportion of correctly predicted instances (normal or malicious) out of a total number of instances.

$$Accuracy = \frac{TP+T}{TP+TN+FP+F} \quad (1)$$

- **Precision:** measure the proportion of correctly detected threats over the total instance labelled as malicious.

$$Precision = \frac{TP}{TP+F} \quad (2)$$

- **Recall:** represents the ratio of actual threats correctly addressed by the model.

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

- **F1-score:** Assess the harmonic mean of precision and recall; it is a single balanced measure of model performance.

$$F1-score = 2 * \frac{Precision*Recall}{Precision+Recall} \quad (4)$$

- **Confusion matrix:** a tabular summary that allows visualization of the performance of a classification algorithm.

We evaluated the proposed research in two experiments:

Experiment 1: CNN and RNN-LSTM with using HashFeature. The performance of the proposed CNN and RNN-LSTM with HashFeature has been analyzed using Comparison illustrated in table 1

Model	Accuracy	Precision	Recall	F1 Score
CNN	0.991943	0.536813	0.439053	0.415525
RNN+LSTM	0.989129	0.364195	0.350130	0.324914

Table 1 Comparison of models with using HashFeatures

The CNN model achieved the highest test accuracy at 99.19%, outperformed RNN-LSTM in all evaluation metrics. The outcomes of these experiment are visualized through figure 4.

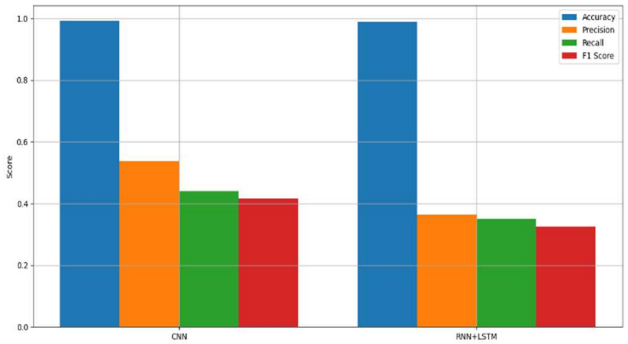

Figure 5 Performance metrics comparison of CNN and RNN-LSTM models with HashFeature

Model	Accuracy	Precision	Recall	F1 Score
CNN	0.990207	0.380211	0.396026	0.382283
RNN+LSTM	0.989136	0.354596	0.395594	0.372218

Table 2 Comparison of models with using PCA

Experiment 2: CNN and RNN-LSTM with using Principal Component Analysis (PCA). The performance of the proposed CNN and RNN-LSTM with PCA has been analyzed using Comparison illustrated in table 2

The CNN model achieved the highest test accuracy at 99.02%, outperformed RNN-LSTM in all evaluation metrics. The outcomes of these experiment are visualized through figure 5.

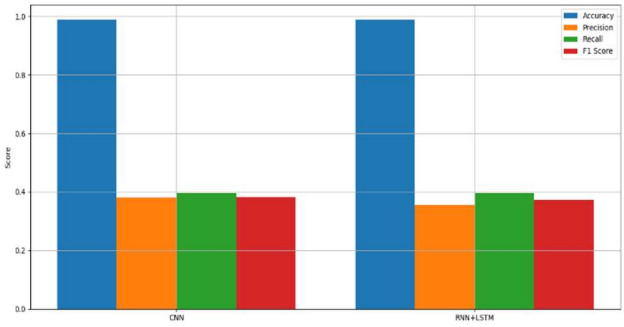

Figure 6 Performance metrics comparison of CNN and RNN-LSTM models with PCA

In conclusion, the findings that When using the **hash feature**, the CNN model achieved an accuracy of **0.990207**,

slightly higher than the RNN+LSTM model (**0.989136**). Additionally, CNN outperformed RNN+LSTM in all other metrics: **precision (0.380211 vs. 0.354596)**, **recall (0.396026 vs. 0.395594)**, and **F1-score (0.382283 vs. 0.372218)**. In contrast, when applying PCA, CNN again demonstrated superior performance with an increased accuracy of 0.991943, and significant improvements in precision (0.536813), recall (0.439053), and F1-score (0.415525). The RNN+LSTM model with PCA performed less favorably, showing reduced scores across all metrics, particularly precision (0.364195) and F1-score (0.324914).

5. Conclusion

In conclusion, this paper proposes an IoT cyber threats detection system-based DL model, specifically RNNs with LSTM and CNNs, to effectively identify and mitigate malicious activities. By integrating advanced DL techniques with robust tools and frameworks, the system achieves high accuracy and adaptability in identifying and mitigating malicious activities. The model is evaluated using the UNSW-NB15 dataset combined with comprehensive evaluation metrics. The findings highlight the significance of integrating advanced DL techniques into IoT security systems and establish a foundation for future improvement in safe-guarding connected devices and networks. Our future work will focus on optimizing the accuracy of the proposed system and assessing its performance on diverse datasets to identify different attack types.

References

[1] G. Fersi, 'Fog computing and Internet of Things in one building block: a survey and anoverview of interacting technologies', *Cluster Comput*, vol. 24, no. 4, pp. 2757–2787, Dec. 2021, doi: 10.1007/s10586-021-03286-4.

[2] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, 'A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis', *Sensors*, vol. 20, no. 13, p. 3625, Jun. 2020, doi: 10.3390/s20133625.

[3] A. Alomiri, S. Mishra, and M. AlShehri, 'Machine Learning-Based Security Mechanism to Detect and Prevent Cyber-Attack in IoT Networks', *IJCDS*, vol. 15, no. 1, pp. 645–659, Aug. 2024, doi: 10.12785/ijcds/160148.

[4] G. Anusha, G. Baigmohammad, and U. Mageswari, 'Detection of cyber attacks on IoT based cyber physical systems', *MATEC Web Conf.*, vol. 392, p. 01166, 2024, doi: 10.1051/matecconf/202439201166.

[5] F. Alrowais, S. Althahabi, S. S. Alotaibi, A. Mohamed, M. Ahmed Hamza, and R. Marzouk, 'Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment', *Computer Systems Science and Engineering*, vol. 45, no. 1, pp. 687–700, 2023, doi: 10.32604/csse.2023.030188.

[6] Satish S. Banait, 'An Approach for Detecting Security Attacks using Machine Learning in IoT Environment', *jes*, vol. 20, no. 1s, pp. 103–113, Mar. 2024, doi: 10.52783/jes.756.

[7] A. Alaa Hammad, M. Adnan Falih, S. Ali Abd, and A. Rashid Ahmed, 'Detecting Cyber Threats in IoT Networks: A Machine Learning Approach', *IJCDS*, vol. 17, no. 1, pp. 1–25, Jan. 2025, doi: 10.12785/ijcds/1571020041.

[8] M. Anwer, S. M. Khan, M. U. Farooq, and . Waseemullah, 'Attack Detection in IoT using Machine Learning', *Eng. Technol. Appl. Sci. Res.*, vol. 11, no. 3, pp. 7273–7278, Jun. 2021, doi: 10.48084/etasr.4202.

[9] J. Alsamiri and K. Alsubhi, 'Internet of Things Cyber Attacks Detection using Machine Learning', *IJACSA*, vol. 10, no. 12, 2019, doi: 10.14569/IJACSA.2019.0101280.

[10] O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, 'A Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things', *Information*, vol. 14, no. 10, p. 550, Oct. 2023, doi: 10.3390/info14100550.

[11] A. I. Jony and A. K. B. Arnob, 'Securing the Internet of Things: Evaluating Machine Learning Algorithms for Detecting IoT Cyberattacks Using CIC-IoT2023 Dataset', *IJITCS*, vol. 16, no. 4, pp. 56–65, Aug. 2024, doi: 10.5815/ijitcs.2024.04.04.

[12] F. Ullah *et al.*, 'Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach', *IEEE Access*, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/ACCESS.2019.2937347.

[13] A. H. K. Mohammed, H. Jebamikyous, D. Nawara, and R. Kashef, 'IoT Cyber-Attack Detection: A Comparative Analysis', in *International Conference on Data Science, E-learning and Information Systems 2021*, Ma'an Jordan: ACM, Apr. 2021, pp. 117–123. doi: 10.1145/3460620.3460742.

[14] E. Shaoul and S. Sonare, 'IoT Network attack detection and Classification using Standardized Recurrent Neural Network model', vol. 5, no. 5, 2023.

[15] Z. Jie, 'IoT-Network Attack Detection with Optimized Recurrent Neural Network and Optimal Feature Selection', in *2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA)*, Dalian, China: IEEE, Oct. 2022, pp. 951–957. doi: 10.1109/ICDSCA56264.2022.9987890.

[16] A. K. Sahu, S. Sharma, M. Tanveer, and R. Raja, 'Internet of Things attack detection using hybrid Deep Learning Model', *Computer Communications*, vol. 176, pp. 146–154, Aug. 2021, doi: 10.1016/j.comcom.2021.05.024.