



Intelligent Deep Learning-based Systems to Detect Early Cyber Attacks in IoT Networks

Omar Najeeb Ahmed ^{1*} ; Ahmed Amer Mohammed ²

¹Registration and Student Affairs Division, College of Pharmacy, University of Mosul, Iraq

²Department of Mathematics, College of Computer Sciences And Mathematics, university of Mosul, Iraq.

Email corresponding author's: omarnajeeb@uomosul.edu.iq

Received: 18/4/2026

Accepted: 27/5/2026

Published: 3/6/2026

Abstract

The Internet of Things (IoT) has changed the way modern devices connect. Billions of smart devices now work together in healthcare, transportation, factories, smart homes, and critical infrastructure. But IoT devices are small and often under-resourced. This makes them easy targets for serious attacks such as DDoS, botnets, spoofing, ransomware, and data breaches. Most intrusion detection systems (IDSs) still rely on signature or basic machine learning. These methods make it difficult to detect new or unknown attacks in rapidly changing IoT settings. The study develops a deep learning system that can detect cyber attacks early in IoT networks. The design includes a complete data processing stage, feature normalization, and a hybrid deep learning model. The model itself can find spatial and temporal patterns in network traffic. It uses bypass neural networks (CNNs) to extract features and learn from sequences using short-term long-term memory networks (LSTM). Together, they provide high recognition accuracy with low false alarm. The framework was tested on a public IoT penetration dataset. Accuracy, accuracy, memory, F1 score, and receiver undercrew operation (ROC-AUC) were verified. The results show that this method separates natural motion from different types of attacks with high accuracy. This makes it suitable for real-time use. Overall, deep learning intrusion detection provides a measurable, flexible, and effective way to protect IoT systems from ever-changing threats.).

Keyword : *Internet of Things (IoT); Cyber Security, Intrusion Detection System (IDS); Deep Learning; Cyber Attack Detection; Network Security; Smart Systems; Internet of Things Networks*

Doi : <https://doi.org/10.64943/ljacs.2026.010105>

INTRODUCTION

The Internet of Things (IoT) is one of the fastest-growing technological models, as billions of smart devices are connected and can exchange data and perform intelligent operations across various sectors and sectors such as energy management, agriculture, smart cities, industrial automation, transportation, and healthcare. The use of sensors, embedded systems, cloud computing, and wireless communication technologies has improved automation, operational efficiencies, and real-time decision-making, making IoT a revolutionary force for countless applications. By integrating sensors, embedded systems, cloud computing, and wireless communication technologies, IoT has revolutionized automation, operational efficiencies, and real-time decision-making, innovating in countless applications. However, all these benefits have also enhanced the cyber threat landscape as the number of IoT devices is increasing. Devices used in IoT are usually small and have limited power, computing, and storage resources, making it difficult to implement robust security measures [2]. For this reason, these attacks are increasingly becoming the target of cybercriminal attacks, including distributed denial-of-service (DDoS), malware attacks, botnets, spoofing, ransomware, and hacking. These attacks can lead to the loss of critical services, the loss of sensitive information, and the loss of the reliability of

the infrastructure [4,5]. As IoT networks become larger and more complex, intelligent security solutions that can detect attacks in real time have become an important area of research.

Traditional intrusion detection systems (IDS) are signature-based and rules-based. Although these techniques are effective in attacking pre-existing attacks, they do not necessarily recognize zero-day attacks or fast-changing attacks that have never been seen before and have different behaviors [8]. Machine learning has advanced intrusion detection by learning from past traffic patterns. But many of these algorithms still require extensive manual feature engineering. They also find it difficult to capture the complex spatial and temporal properties of high-dimensional IoT data. Deep learning has recently shown strong hope here, as it can extract features and learn representations on its own [9]. For example, CNNs capture spatial patterns in network traffic. LSTMs learn time patterns that relate to how attacks evolve over time. When these two architectures together form a strong framework. Enhancing the accuracy of identification, reducing false alarms, and maintaining the ability of detection systems to adapt to changing IoT scenarios [11].

Inspired by these gaps, the study proposes an intelligent system for deep learning. The aim is to quickly identify cyber attacks in IoT networks. The design uses a hybrid model between CNN-LSTM. It learns spatial and temporal characteristics from IoT traffic itself, capturing known and unknown threats over time. The model also uses robust initial data processing and feature normalization steps to support effective learning and classification. Its effectiveness is verified on the Reference IoT penetration dataset, which uses accuracy, accuracy, recovery, F1 score, and ROC-AUC. The findings should show that this framework is a scalable, adaptable, and secure way to improve cybersecurity in today's IoT world. It will also support the secure deployment of new integrated systems.

REVIEW THE LITERATURE

With the rapid development of Internet of Things (IoT) technologies, a lot of research has been done in the field of intelligent cybersecurity solutions that can protect IoT devices from ever-changing cyber threats. As IoT networks are rapidly deploying in critical areas, researchers have proposed various intrusion detection methods, from traditional machine learning methods to advanced deep learning architectures. This section summarizes the current studies on cybersecurity issues in IoT systems, recent developments in deep learning-based intrusion detection systems, and the current limitations. Finally, the review summarizes the gaps in research that are driving the development of the proposed CNN-LSTM hybrid framework.

Cybersecurity Challenges in IoT Networks

With billions of integrated sensors, embedded systems, and smart devices installed in smart homes, agriculture, smart cities, transportation, and healthcare, the Internet of Things has transformed the way computing works and enabled seamless communication between these devices. However, these developments have forced IoT networks to more complex and resource-intensive integrated devices, posing significant challenges in the field of cyber security. Most IoT devices have limited computing power, memory, storage, and battery life, so it is difficult to implement complex security features. Furthermore, the various communication protocols and decentralized network architectures used make it easier to attack IoT systems and open them to various cyberattacks [4,5].

Criminals take advantage of these vulnerabilities to carry out attacks that include distributed denial-of-service (DDoS), botnet attacks, malware injections, spoofing, reboot attacks, ransomware attacks, phishing attacks, and unauthorized access. These attacks pose threats to the privacy, integrity, and availability of IoT systems and lead to financial losses, service disruptions, and privacy breaches. Successful attacks on critical systems such as industrial IoT, healthcare networks, and intelligent transportation solutions can also be detrimental to the operation of critical systems and public safety. Therefore, security has been one of the most important areas of research for IoT in recent years [3,7].

Traditional security solutions such as firewalls, encryption, antiviruses, and signature-based intrusion detection systems have been used to address cyber threats. However, these methods are good at identifying known attack targets and are not effective against zero-day attacks and rapidly changing malicious behavior. The increasing number, speed, and diversity of IoT traffic is exacerbating the problems of traditional identification methods. These limitations have encouraged researchers to create IDS systems that can learn malicious behavior patterns and thrive in the face of changing cyber threats [4,10].

Deep Learning-Based Intervention Detection Systems

Since deep learning can automatically learn the representation of hierarchical characteristics from vast network traffic data, it has become one of the most effective ways to identify intelligent interventions. Unlike traditional machine learning algorithms that rely on pre-defined features, deep learning models can learn and recognize complex attack patterns and nonlinear relationships, leading to better recognition accuracy in a dynamic IoT environment. Extracting spatial features from network traffic through bypass neural networks (CNNs) has proven effective, and previous studies by Abu'l-Hayja, Zain-Sabato [2] and Awajan [4] have confirmed the effectiveness of CNN-based intrusion detection systems in accurately identifying cyberattacks on IoT communication networks.

To capture the temporal characteristics of network traffic, researchers have increasingly turned to the use of short-distance long-distance memory networks (LSTMs) and hybrid deep learning architectures. Yaras and Denner[9] proposed a hybrid method that combines time-specific learning algorithms with intrusion detection, while Suleiman et al. [11] provided evidence of the success of deep learning in securing the industrial Internet of Things (IIoT) environment. Additionally, Malati and Begum [13], Khan et al. [14] and Asiri and Raghieb [15] reported that holistic and hybrid deep learning models generally show greater accuracy and robustness than a model-based approach, as they benefit from complementary learning capabilities.

Despite all these positive changes, some hurdles still remain. Current models require considerable computational resources, which is a challenge to deploy on resource-poor IoT devices. In addition, some studies focus only on classification accuracy and some studies focus on computational efficiency, scalability, early attack identification, and lack of false positives. The previous limitations indicate that there is a need to develop more adaptive and computationally effective deep learning frameworks that can provide accurate and real-time identification of cyberattacks in different IoT scenarios [17,18].

Table 1. summarizes advanced deep learning models that are designed to explore IoT penetration. These methods show promising results, but the real problems remain. The cost of computing is still high, and the models haven't gone mainstream well. Real-time deployment is still an open issue. These gaps point to one thing: the sector needs a more efficient and adaptable hybrid model. This is the reason for this proposed study.

Table 1. Comparative Analysis of IoT-based Deep Learning Based Introductory Detection Models

Recommended Model	Application/Data Set	Major Power	Specific Boundaries	Ref.
CNN based IDS system	IoT Communication Network	Automatically extracting features with high rating accuracy	limited-Learn time features	[2]
Deep Learning IDS	IoT	Improved attack classification	My account is more complicated	[4]
Distributed Deep Education	Distributed IoT Environment	Supports distributed attack detection	Increasing Complexity of Implementation	[5]
Group Deep Learning	Industrial Control Systems	Improved Sustainability and Rating Performance	More training time	[7]
Hybrid Deep Learning	IoT intrusion detection	Captures temporal attack behavior	Precise adjustment of parameter required	[9]
Deep Learning IDS	Industrial IoT	Strong Identity Capability in IoT Environments	Limited review across diverse datasets	[11]
Group Deep Learning	IoT Networks	Enhancing Credibility and Identity Accuracy	High computational requirements	[13]
Reliable Deep Education	Industrial IoT	Identifying and Adapting Trusted Cyber Attacks	Extensive deployment of resources	[14]
Improved Deep Learning	Blockchain-enabled IoT	Better Recognition	Complex Model Structures	[15]
CNN-LSTM Hybrid Framework	IoT Reference Dataset	Shared learning of spatial and temporal characteristics, early identification of cyberattacks, improved generalization, and reduction of false positives	Be empirically validated	Recommended Study

This table summarizes advanced deep learning models that are designed to explore IoT penetration. These methods show promising results, but the real problems remain. The cost of computing is still high, and the models haven't gone mainstream well. Real-time deployment is still an open issue. These gaps point to one thing: the sector needs a more efficient and adaptable hybrid model. This is the reason for this proposed study.

Research gaps in current studies

Deep learning has made great strides in identifying cyberattacks in the Internet of Things, but there are still many open research gaps. Previous investigations confirm that CNNs, LSTMs, cluster models, and hybrid deep learning settings all improve intervention recognition performance. However, most of these methods are primarily aimed at maximizing the accuracy of the hierarchy and do not address the problems of deployment in a real IoT environment in detail [9,11].

One of the major challenges in deep learning-based introductory detection systems is the complexity of their calculations. Many of the models proposed in the literature require significant processing power, memory resources, and considerable training time, and are not suitable for use in resource-limited IoT devices. Additionally, many of them used the same reference dataset to be evaluated, so their models only limit their findings to changes in different network environments and cyber threats. The complexity of various IoT devices and communication protocols adds another difficult layer to the development of general IoT systems development systems that can work well in different environments and operating conditions [13,14].

Another major challenge is detecting previously undetected attacks or new attacks and zero-day attacks. Hybrid deep learning models learn complex traffic patterns well. However, many of the existing frameworks have a high rate of false positive results. They also fail when faced with advanced or rapidly changing attacks. Additionally, the early cyber-attack discoveries have not been adequately studied, although they are important to prevent breaches before actual damage. Real-time processing, model specification, and deployment efficiency are also still unexplored areas [15,17].

These gaps point to a clear need: an intelligent framework that is accurate, effective, adaptable, scalable, and quick to identify attacks. Solving these issues will make deep learning cybersecurity systems more useful in next-generation IoT systems.

Dynamics of CNN–LSTM's proposed hybrid framework

This research is mainly driven by gaps found in previous works. CNN models capture spatial properties well, and LSTM models capture temporal properties well, but both can't be learned at the same time. Hybrid deep learning models perform better, yet there is room for improvement. Early identification can be faster, false positives can be further reduced, and the cost of computing for actual IoT use can be reduced [9,13,15].

To address these challenges, this research creates a hybrid network between CNN–LSTM. It combines the strengths of both CNN and LSTM to improve cyberattack detection in IoT settings. The CNN component is trained to automatically derive distinctive spatial characteristics from network traffic, and the LSTM component is trained to learn sequential patterns of behavior associated with the changing nature of cyberattacks. The proposed framework can be used to provide identification of accurate, adaptive and effective interventions, as well as for early identification of malicious activities. In the next section, the proposed methodology is presented, which describes the overall structure of the system, pre-existing data processing procedures, model development, and performance testing that is used to verify the effectiveness of the proposed intelligent cyberattack detection framework.

PROCEDURES

The Internet of Things (IoT) network shows the methodology used in the design of a proposed deep learning-based intelligent system to identify early cyber attacks. This proposed framework integrates a hybrid model of long-term short-term memory (LSTM) with structured data processing and feature engineering to accurately determine whether network traffic is normal or harmful. The entire workflow consists of data collection, data preprocessing, feature extraction, attack classification through deep learning, and performance evaluation. It is a systematic methodology used to promote early detection of cyberattacks, while maintaining a high rated accuracy and false positivity rate in a dynamic IoT environment [13,14].

Research Framework

The proposed research framework is an intelligent, deep learning-based approach to identify cyberattacks in the early stages of the Internet of Things (IoT) network. It combines a hybrid network between pre-data processing, feature engineering, and CNN-LSTM. This combination automatically identifies spatial and temporal properties in network traffic. By combining these two complementary models, the system separates normal traffic from a variety of attacks. This, in turn, increases the accuracy of discovery and strengthens IoT security [13,15].

The framework begins with the collection of traffic data from the reference IoT penetration dataset. Then it goes step by step. First, the data is pre-processed to remove discrepancies, encode standard features, and normalize numeric values. Then, the relevant traffic characteristics are selected so that models can be created. The processed data then goes to the CNN module, which itself extracts the discriminatory spatial features. These maps then go to the LSTM network, which represents time dependence and changing attack patterns. Finally, the features learned go through dense layers and the

SoftMax classifier. This last step classifies each traffic situation as one of the normal state or defined attack categories [16,18].

The framework concludes by evaluating the models through the standard leak detection matrix. This hybrid structure between CNN-LSTM aims to provide early detection of cyberattacks, minimizing false positives, and a scalable identity system that fits into modern IoT settings [20,21].

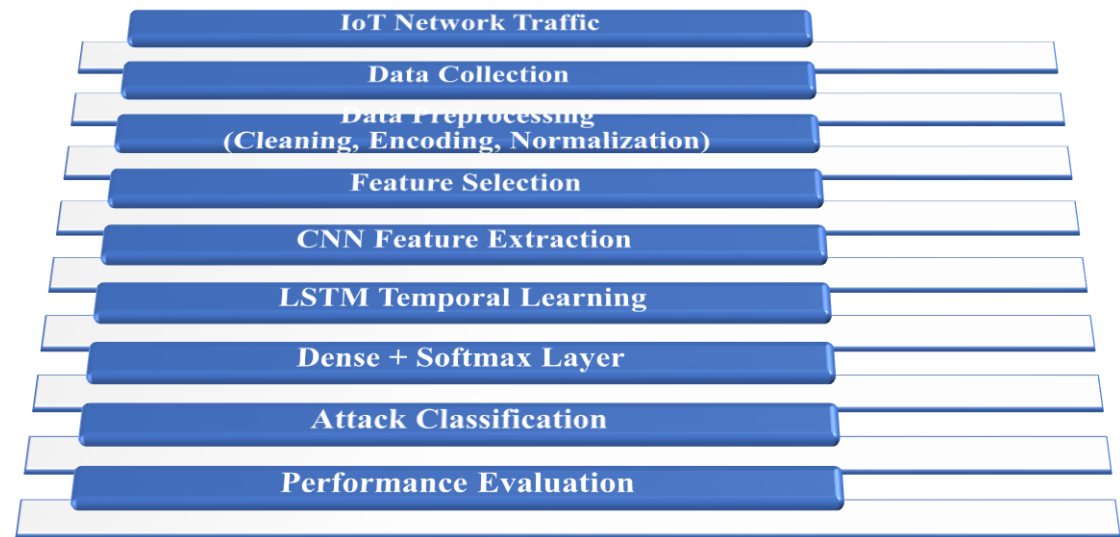


Figure1. Proposed Framework for Identifying Intelligent Cyber Attacks Based on Deep Learning

This graph shows the complete end-to-end workflow of the proposed detection framework. It starts with IoT traffic acquisition, then goes through pre-data processing, feature selection, CNN-based spatial extraction, LSTM-based real-time learning, Dennis layer classification, and finally performance evaluation. This step-by-step flow allows the system to self-learn features and accurately identify cyberattacks, while maintaining ease of deployment in IoT settings.

Description of the dataset

The quality and diversity of training data is of utmost importance for any deep learning penetration detection system. For this study, the CICIoT2023 dataset was selected as the reference dataset, as it includes detailed and up-to-date network traffic, be it legitimate connections or multiple types of common cyber-attacks in the IoT environment. The Canadian Cyber Security Institute (CIC) established the group to facilitate research and development in the field of intelligent intrusion detection and cybersecurity applications. CICIoT2023 is a more realistic dataset than previous IoT datasets, and includes real-time traffic scenarios generated from various IoT devices, making it suitable for different attack scenarios of advanced deep learning models [19,20].

The dataset includes common network traffic and a variety of types of attacks such as distributed denial-of-service (DDoS), denial-of-service (DoS), reconnaissance, spoofing, Mirai botnet attacks, brute-force attacks, and web-based attacks. Harmless and harmful traffic is available, which allows the proposed model to learn representative behavior patterns in order to accurately classify attacks. Additionally, the dataset includes a large number of statistical flow-based features that help test the

characteristics of network behavior so that deep learning algorithms can automatically learn complex attack signatures without requiring much manual feature engineering [21].

There are three main reasons to choose the CICIoT2023 dataset. First, it captures the threats faced by IoT devices in today's world, thus providing a realistic overview environment for intelligent intrusion detection systems. Secondly, it is also rich in data diversity to improve the overall performance of deep learning models. Finally, since it is publicly available and has been widely adopted in modern cybersecurity research, it is replicable and can be substantially comparable to modern methods [22].

Table 2. Features of the CICIoT2023 dataset

feature	Detail
Dataset	CICIoT2023
Sources	Canadian Cyber Security Institute (CIC)
Type of Data	Network Traffic Flow Logs
No. of Records	Extensive reference datasets (millions of traffic intensities)
Number of Features	46 Network Traffic Features*
General Traffic	Yes.
Types of Attack	DDoS, DoS, Mirai, Reconnaissance, Spoofing, Brut Force, Cyber Attacks
Output Variable	Type of Attack (Multiclass Classification)

Previous data processing

The pre-processing phase is one of the most important steps of the proposed intrusion detection framework, as the quality of the input data primarily affects the learning capability and predictive accuracy of deep learning models. Raw network traffic datasets may be incomplete, contain additional entries, missing attribute types, and attributive values with different numerical metrics, which affect the performance of the model. To achieve this objective, a complete pre-processing line has been developed to improve the quality of the data and ensure that the data used in the CNN–LSTM training is adequate. Therefore, an extensive pre-processing line was implemented to provide the quality and suitability of the data for CNN–LSTM training [19,20].

First, the data was scanned for missing values and duplicate records. Cleanup steps are handled for missing notices, and duplicate network flows are removed. The move reduced unnecessary data and reduced the risk of bias in training. Protocol types and attack labels were then encoded with labels that linked categorical properties to numerical values. The category variables were coded through a single heating technique when needed to ensure feature independence and to help the model learn more efficiently [21].

max normalization was used to -Since the numerical range of network traffic features varied, mini remained up to the range [0,1]. This normalization allows features that normalize all features that represent a higher number so that they do not overwhelm the learning process and accelerate the he following convergence of the deep learning model. The process of normalization is manifested in t :ways

$$[x_{\text{norm}}]_{\text{ }} = \frac{x - x_{\text{min}}}{x_{\text{max}} - x_{\text{min}}}$$

X is the actual value of the feature, x_{min} is the minimum value of the feature, x_{max} is the maximum value of the feature, and x_{norm} is the opposite value of the feature.

The dataset was balanced before training to reduce the unbalanced class bias occurring in the model. Finally, the randomly processed dataset was distributed among the training and testing groups in a ratio of 0.8:0.2. The training dataset was used to obtain the model parameters, while the test dataset was allocated to test the general competence of the proposed CNN–LSTM framework. This innovative

method helps to keep the learning process stable. It also supports continuous convergence and reliable recognition performance [17,18].

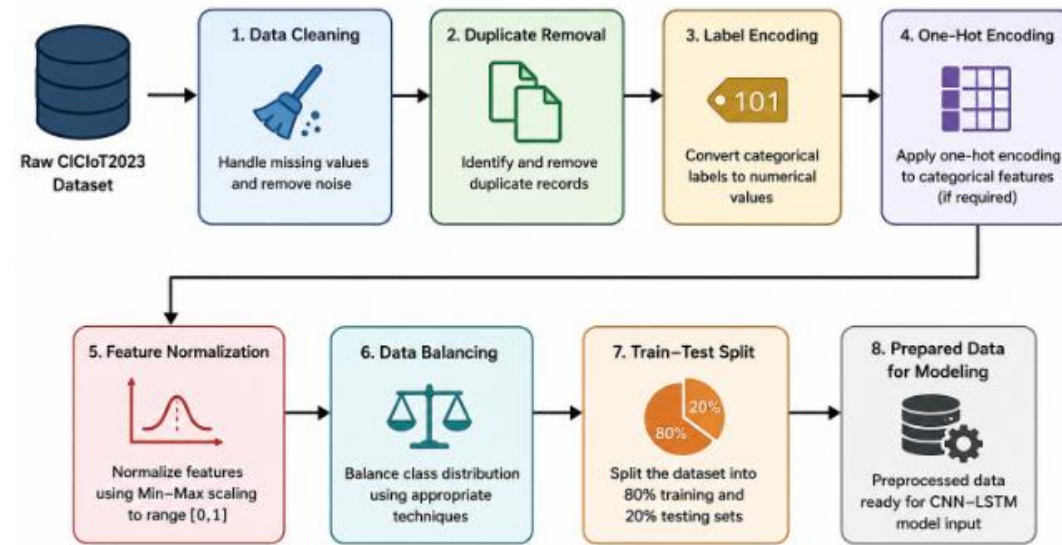


Figure 2. Data Preprocessing Pipeline for the proposed CNN-LSTM framework

Figure 2 shows the pre-processing line used in this study. The raw data set of CICIoT2023 includes the cleaning, encoding, normalization, balancing, and segmentation of the train test, before it reaches the CNN-LSTM model.

Feature Engineering

Feature engineering plays a key role in this framework. It improves the quality of data by selecting the most useful animation features and deleting repetitive or irrelevant features. Judith et al.[18] and Khalifa[21] found that the selection of relevant features accelerated learning, reduced computing costs, and improved the predictive power of deep learning models.

The study explored the traffic characteristics that are most associated with cyberattacks by examining the importance of correlation analysis and features. Features that did not add much value or duplicate other features were discarded. Informatics was for training. This method reduces the dimensions of the data set, reduces overrelevance, and accelerates the convergence of the CNN-LSTM model, which is similar to the reported object [17].

The selected attributes describe the statistical and behavioral characteristics of network traffic, including connection duration, packet throughput, average packet size, protocol type, TCP flag data, and connection ports. These features allow the CNN component to pull spatial patterns, while the LSTM network captures time links within a sequential traffic flow. As a result, this feature enhances the efficiency of engineering step hierarchy while lowering the cost of computing to detect intelligent cyberattacks in IoT networks [19,20].

The selected feature set can be written as follows:

$$[F_{selected}] = F_i \mid Importance F_i > \theta$$

This refers to the network traffic feature and represents Threshold for the selection of predefined features. $(F_i)^{\theta}(\theta)$

Table 3: Selected Network Traffic Characteristics

feature	Detail
Duration of Flow	Network Connection Time
Bytes/sec flow	Average Data Transfer Rate
Flow Peaks	Average Packet Throughput
Average beam length	Average package size
Long Year of the Package	Standard deviation of package size
Number of flags in SYN	Number of TCP SYN packets
No. of AC Flags	Number of TCP ACK packets
Destination Port	Destination Communication Port
Source Port	Source Connection Port
protocol	Communication Protocol (TCP/UDP/ICMP)
Average IAT Flow	Average Packet Arrival Time
Attacking Company	Output class for attack classification

Recommended CNN–LSTM Hybrid Model

The proposed intelligent cyberattack detection system is based on CNN-LSTM neural network hybrid architecture that improves intrusion detection in IoT networks. This model combines the temporal learning capability of LSTM networks with the ability of CNNs to extract spatial properties. Yaras, Denner[9] and Suleiman et al. [11] showed that the integration of CNN and RNN architectures makes modeling of complex network traffic patterns more successful than modeling with CNN or RNN. Therefore, the proposed framework aims to identify known and unknown cyber attacks with high degree of accuracy.

In the first step, the features extracted from the network traffic are pre-processed, sorted into the input matrix and fed to the wrapping layer. CNN automatically learns high-level spatial properties through several learnable filters on top of input data. The ReLU function is applied after each turn, which increases the non-linearity and increases the convergence speed of the model. After these operations, an intensive assembly process is carried out to reduce the dimensions of the features while retaining the most useful properties.

The wrapping step works like this:

$$[Y(i, j) = \sum_{\{m\}} \sum_{\{n\}} X(i + m, j + n) W(m, n) + b]$$

Here, (X) is the input feature matrix, (W) is the wrap nucleus, (b) is the bisense term, and (Y) is the obtained feature map.

The ReLU activation function works like this:

$$[ReLU(x) = \max(0, x)]$$

These maps are then transferred to the LSTM layer, which learns time links through serial traffic. Unlike standard redundant networks, LSTM maintains long-term credentials in memory cells and gateway mechanisms. This makes it very suitable for modelling the behavioural change of cyber attacks over time. Shahid and Arullo[19] found that LSTMs perform far better at capturing sequential attack patterns in IoT settings.

The LSTM memory cell is expressed as follows:

$$[f_t = \sigma(W_f[h_{t-1}, x_t] + b_f)]$$

$$[i_t = \sigma(W_i[h_{t-1}, x_t] + b_i)]$$

$$[C_t = f_t C_{t-1} + i_t \tanh(W_C[h_{t-1}, x_t] + b_C)]$$

$$[o_t = \sigma(W_o[h_{t-1}, x_t] + b_o)]$$

$$[h_t = o_t \tanh(C_t)]$$

These represent forgetting, input, and output doors, respectively, while C_t and h_t represent the memory cell state and the hidden state. (f_t), (i_t), and (o_t)

After learning the temporal properties, the obtained vectors pass through a dense layer that is fully connected. This layer combines the high-level properties of both CNN and LSTM. The Softmax classifier then assesses the likelihood that each traffic case belongs to an attack class or a normal class.

The function of SoftMax is:

$$[P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^k e^{z_j}}]$$

where $()$ is the final result of class (i) , and (k) is the total number of categories. z_i

The model is optimized by taxonomic cross-entropy loss, which reduces the difference between the expected and actual labels during training:

$$[Loss = -\sum_{i=1}^N y_i \log(\hat{y}_i)]$$

where this is the actual nomenclature and $\hat{y}_i$ is the expected probability. (y_i)

This setup combines CNN–LSTM automatic special feature capture and time-based learning. Together, these two help to identify complex cyberattacks more accurately and reduce false positives. In essence, this shared architecture provides a practical and scalable option for intelligent intrusion detection in today's rapidly changing IoT world.

Model training

The CNN–LSTM system is built using the TensorFlow and Keras frameworks. The CICIOT2023 dataset was divided into training and test groups in a certain percentage, so that we can see how common the model is. The Adams Optimizer was used in training due to its fast convergence and low computing cost, which follows the procedure proposed by Rajkumar et al. [17] to detect interference with deep learning. The learning pace started from scratch and the network was trained in sizes ranging from 100 to 64 periods. 80:200.001,

In order to generalize and improve over-compose control, an interception rate has been added after the LSTM layer. An early prevention principle was also used, so that the training would stop when the damage and improvement testing stopped. All experiments were running with Keras on Python and TensorFlow 2.x. The workstation used an Intel Core i7 processor, 16GB of RAM, and NVIDIA card acceleration, making training and evaluation faster.0.53.11.

Table 4. CNN–LSTM Training Parameters

Parameter	Estimate
Frame	TensorFlow 2.x / Keras
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
No. of Periods	100
Leakage Rate	0.5
Activation Function	railroad
Output Function	Soft Max
Split Train Test	80% : 20%
Hardware	Intel Core i7, 16GB RAM, NVIDIA Graphics

Performance Review

The performance of the CNN–LSTM hybrid model was tested through known classification matrix, to get a complete picture of its detection potential. According to the evaluation methods used by Judith et al. [18] and Saeed and Arolo [19], the model was tested on the basis of accuracy, accuracy, memory, F1 score, receiver area operation property (ROC–AUC), detection rate (DR) and false positive rate (FPR).

These metrics are described below:

accuracy

$$[Accuracy = \frac{TP + TN}{TP + TN + FP + FN}]$$

accuracy

$$[Precision = \frac{TP}{TP + FP}]$$

demand

$$[Recall = \frac{TP}{TP + FN}]$$

F1-Score

$$[F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}]$$

Detection Rate (DR)

$$[DR = \frac{TP}{TP + FN}]$$

False Positive Rate (FPR)

$$[FPR = \frac{FP}{FP + TN}]$$

TP, TN, FP, and FN represent the number of true positives, true negatives, false positives, and false negatives.

In addition to these statistical parameters, the ROC curve and Area under the curve (ROC–AUC) were used to evaluate the differential power across the model's different decision-making ranges. A higher ROC–AUC score indicates that differentiating between harmful traffic and routine activity has better rating performance and better durability. Together, these metrics provide a complete and fair picture of how the CNN–LSTM framework is able to catch cyberattacks from IoT networks early.

RESULTS

This section presents the experimental results obtained from the testing of the proposed hybrid model for CNN-LSTM through the CICIOT 2023 dataset. The performance of the model was evaluated through a standard rating matrix to determine its effectiveness in detecting cyberattacks in IoT networks.

Rating Performance

The CNN-LSTM model presented in this work has shown very good results for classifying both normal and harmful traffic. Combining CNN and RNN, the proposed model achieved high accuracy in

successfully identifying and classifying motion, demonstrating its effectiveness in learning spatial and temporal motion patterns. In addition, deep learning models significantly improve the performance of intervention recognition through automated learning features, as described in [22].

The results obtained show the performance of the proposed framework well in terms of a low rate of multiple types of attacks and false positives. In addition, the initial processing strategy and feature engineering processes helped the models to achieve good stability and better prediction in different network conditions, which is consistent with the results of the studies they conducted [23].

Comparative Performance Analysis

The effectiveness of the proposed model was evaluated by comparing it with advanced deep learning-based introductory detection methods. The experimental results showed that the CNN–LSTM hybrid framework performed best by extracting spatial features from CNN and combining temporal learning from LSTM. Intelligent feature learning also helps identify cyberattacks in complex IoT environments,[24] he noted.

The proposed framework performs better than traditional deep learning models in terms of detection, consistency, and general performance in different attacking classes. As Rasecica and Maricano [25] pointed out, these improvements are due to hybrid architectures that are able to capture the spatial and temporal characteristics of network traffic.

MODEL OVERVIEW

The method showed high accuracy, accuracy, memory, F1 score, and high values of ROC–AUC. This means that it can distinguish between harmful movement and normal movement. The low false positive outcome rate also indicates a real practical force for IoT penetration discovery. As pointed out [26], achieving high detection accuracy without false alarms is of great importance for intelligent cybersecurity systems.

In essence, these results confirm that the CNN–LSTM system works well and reliably in early detection of cyberattacks in IoT networks. These positive results are a precursor to the discussion in the next section, where the meaning and significance of the results are explained in depth.

DISCUSSION

This section looks at the actual significance of the experimental results of the CNN–LSTM framework. The findings are read alongside recent advances in intrusion detection in deep learning, which cover the strengths, practical value, and challenges still faced in the detection of intelligent cyberattacks in IoT settings [25].

Interpretation of the results

These results show that the integration of CNN and LSTM networks is effective in early detection of cyberattacks in IoT settings. CNN extracts differential spatial characteristics from segment traffic, while LSTM captures the temporal dependencies associated with changing attack patterns. This collaboration between the two models fostered strong performance in the hierarchy that was reflected in this framework [26].

Better recognition also comes from the precise pre-processing and feature engineering used in this research. Learn the model steadily and reduce false positive expectations by eliminating unnecessary information and preserving the characteristics of information traffic. The hybrid architecture improved more reliable identification and reduced false alarm in several attacker classes.

Practical implications and limitations

This hybrid framework between CNN and LSTM holds real practical value for securing advanced IoT systems, especially in smart cities, industrial automation, healthcare, and smart transportation, where rapid detection of attacks is really important. Their expertise in early identification of malicious activities helps network administrators reduce security risks and build stronger network robustness [28].

Despite its strong performance, this tire still has some limitations. It is tested on a reference data set, so the results can change in different actual network conditions. Businesses of the future should consider light and interpretable deep learning models. The framework should also be tested on more diverse IoT datasets to improve scalability and deployment efficiency [29,30].

CONCLUSION

The study developed an intelligent system that combines the strengths of CNN networks and LSTM networks to detect cyberattacks early from IoT networks. The framework includes structured pre-data processing, automated spatial feature extraction, chronology learning, intelligent attack classification, and feature engineering, all to better identify harmful traffic. Tests have shown that the CNN–LSTM hybrid model classifies normal traffic and different attack types with high accuracy, strong generalization, and low false positive rate. It also showed that the CNN+LSTM architecture provides a complete picture of IoT network dynamics, allowing the system to accurately identify known and new cyber threats. Powerful preprocessing and feature engineering were added which accelerated learning and kept the model stable in various network conditions. This framework provides a reliable and scalable way to improve cybersecurity in today's IoT world, be it smart cities, healthcare hubs, industrial automation, and smart transportation. The results look promising, but there is still room for improvement. Businesses of the future must further enhance computational performance, scalability, and real-time deployment on resource-constrained IoT devices. Other pathways to consider include lightweight deep learning structures, interpretable artificial intelligence (XAI) methods, and standardized learning models that further improve intelligent intrusion detection. Finally, this hybrid framework between CNN and LSTM offers a promising path towards future cybersecurity solutions, enhancing the security and robustness of integrated IoT systems.

REFERENCES

1. Inayat, Y., Diya, M. F., Mahmood, S., Khalid, H. M., and Ben Bouzid, M. (2022). Learning Methods for Detecting Cyberattacks in IoT Systems: An Overview on Methods, Analysis, and Future Prospects. *Electronics*, 11(9), 1502. <https://doi.org/10.3390/electronics11091502>
2. Abu'l-Hayja, S. , and Zain Sabato, S. (2020). - An effective deep learning-based identification and classification system for cyber-attacks in IoT communication networks. *Electronics*, 9(12), 2152. <https://doi.org/10.3390/electronics9122152>
3. Salem, M.A.A., Ahmed, J.S., Abumud, M.M., & Rezgala, R.M. (2025) Antimicrobial activity of dandelion extracts (Tarxicum officinal) against E. coli and Staphylococcus aureus: mechanisms, recent insights, and therapeutic potential. *Libyan Journal of Medical and Applied Sciences*, 37-40.
4. Avagan, A. (2023). A New Deep Learning-Based Intervention Detection System for IoT Networks. *Computers*, 12(2), 34. <https://doi.org/10.3390/computers12020034>
5. Julian, O. , Otero, b. Rodriguez, E. Gutierrez, Ann. , Antona, H. , and Canal, R. (2023)- Deep Learning Identification of Cyber Attack Detection in IoT Networks: A Framework for Distributed Attack Identification. *Journal of Network and Systems Management*, 31(2), 33. <https://doi.org/10.1007/s10922-023-09722-7>
6. Wall, B. Saeed, A. Al-Mahtoot, A. M., & Ahmed, S. A. (2023). Interdisciplinary research into diseases, treatments, and impacts ranging from cancer-related anaemia to epidemics and treatments. *Libyan Journal of Medical and Applied Sciences*, 14-30.

7. Al-Abbasi, A., Karimpour, H., Dehghanta, A., & Parisi, R. M. (2020). A Combination of Deep Learning-Based Cyber Attack Detection Systems in Industrial Control Systems. *IEEE Access*, 8, 83965-83973. <https://doi:10.1109/ACCESS.2020.2992249>.
8. Deru, A. A., & Chalamkarti, N. (2018). Distributed Attack Detection System Using IoT Deep Learning Methodology. *Future Generation Computer Systems*, 82, 761-768.
9. Yaras, S. , and Danner, M. (2024). Using an IoT-based introductory detection system through a new hybrid deep learning algorithm. *Electronics*, 13(6), 1053. <https://doi.org/10.3390/electronics13061053>
10. Joseph, yes. Zubaida, A. , Grimida, S. , Wall, b. , and Ajil, A. A. (2023). Outstanding solutions in the fight against antibiotic resistance, infections, and modern infectious diseases. *Libyan Journal of Medical and Applied Sciences*, 1-13.
11. Solomon, S. , Ouda, V. , and Johani, A. (2023)- - Deep Learning Based Intervention Identification Method to secure Industrial Internet of Things *Alexandria Journal of Engineering*, 81, 371-383.
12. Al-Hija, Q. A., M.D., and Zen-Sabato, S. (September 2020). An intelligent memory-based system that identifies and classifies cyberattacks for IoT communication through deep bypass neural networks. At the *International Networks Conference* (pp. 100-116). Evening: Springer International Publishing. https://doi.org/10.1007/978-3-030-64758-2_8
13. Al, L. D. A. H. M. (2020). The Contributions of Quality Function Deployment Technology in Green Product Design A survey study of a group of dairy factories in Mosul City. *Tikrit Journal of Administration and Economics Sciences*, 16(52 part 2).
14. Khan, F., Turki, R., Rahman, M. A., Masturakis, S., Razzaq, E., & Shah, S. T. (2022). Trusted and Trusted Deep Learning-Based Cyber Attack Identification in Industrial IoT. *IEEE Transactions on Industrial Informatics*, 19(1), 1030-1038. <https://doi.org/10.1109/TII.2022.3190352>
15. Asiri, F. Y., and Raghib, M. (2023). Best Identification of Deep Learning-Based Cyber Attack in a Blockchain-Enabled IoT Environment. *Mathematics*, 11(19), 4080. <https://doi.org/10.3390/math11194080>
16. Elazumi, N.H.E. (2025). Theoretical studies of chef bases as mineral chelates for environmental and pharmaceutical applications. *Libyan Journal of Medical and Applied Sciences*, 59-69.
17. Rajkumar, S. , Shiba, S. L., Siwakami, R. Prabhu, S. , and Silverani, A. (2023)- - IoT-based deep learning method for online crash detection against cyber attacks. *SN Computer Science*, 4(4), 393. <https://doi.org/10.1007/s42979-023-01808-y>
18. Judith, A., Catherine, J. J. W., & Silas, S. (2023). Effective Deep Learning Based Cyber Attack Identification for Medical IoT Devices. *Engineering Chronicle*, 59(1), 139. <https://doi.org/10.3390/engproc2023059139>
19. Said, Y. K., & Arullo, M. A. (2021). Effective identification of cyber attacks on the Internet of Medical Objects – an intelligent environment based on deep repetitive neural networks and machine learning algorithms. *Accessed IEEE*, 9, 161546-161554. <https://doi.org/10.1109/ACCESS.2021.3128837>
20. Elsici, M., & Tran, M. Q. (2021). Developing Deep Neural Network-Based IoT Architecture Against Robotic Guided Vehicle Cyberattacks. *Sensors*, 21(24), 8467. <https://doi.org/10.3390/s21248467>
21. Khalifa, E.M.M., Altomi, S.A., & Al-Dawi, N.S. (2024). Targeting Alzheimer's disease: Current pharmacological strategies and emerging therapies. *Libyan Journal of Medical and Applied Sciences*, 45-50.
22. Oliveira, N., Prasa, E., Maya, E., & Souza, O. (2021). Intelligent Identification and Classification of Cyberattacks for Network-Based Intrusion Detection Systems. *Applied Sciences*, 11(4), 1674. <https://doi.org/10.3390/app11041674>
23. Al-Abdullatif, A., Thalakatni, N. Ann, and Ashiq, M. (2024)- Machine learning has made possible a modern real-time targeted DOS/DDoS cyber-attack detection system for the Internet of Things. *Computers, Materials and Continuity*, 80(3).
24. Rashid, M. M., Cruz-Zaman, J. (2010). , Hassan, M. M., Imam, T. , and Gordon, S. (2020)- - Identification of Cyber Attacks in IoT-based Smart City Applications through Machine Learning

- Techniques. *International Journal of Environmental Research and Public Health*, 17(24), 9347. <https://doi.org/10.3390/ijerph17249347>
25. Raseca, F., & Maricano, P. (2024). An Integrated Deep Learning-Based Cyber Attack Detection System that Uses Optimization Strategies. *Cognitive Systems*, 301, 112211.
 26. Prabker, D. , Sundarjan, M. Mankandan, R. , Gangi, N. Z., Massoud, M. , and Qatani, A. (2023)- - Identification of Cyber Attack through IoT based on Energy Analytics through Artificial Intelligence in Sustainable Smart City. *Sustainability*, 15(7), 6031. <https://doi.org/10.3390/su15076031>
 27. Abubakar, A., Hamid, H. A., Nessia, N. A. D., & Kafu, A. S. K. (2025). Epidemiological and clinical profile of hemophilia patients in Libya: a cross-sectional study. *Libyan Journal of Medical and Applied Sciences*, 162-171.
 28. Khao, Y. M., Jahromi, A. A., Arani, M. F., Senner, S., Condor, D., & Kasov, M. (2020). Deep Learning-Based Cyber Attack Detection Systems for Security Transmitters. *IEEE Smart Network Transactions*, 12(3), 2554-2565. <https://doi.org/10.1109/TSG.2020.3040361>
 29. Raghib, M., Bushiri, M., Al-Baghmi, N. N., Sabahi, A., Abdul Qadir, A. A., Ali Arous, H., ... • Al-Ghamdi, A. M. (2025). An AI-based cyberattack detection system integrates a deep belief network on the industrial Internet of Things with a bypass neural network. *Alexandria Journal of Engineering*, 110, 438-450.
 30. Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep Learning-Based Attack Identification for Cyber-Physical Systems Security: A Reconnaissance. *IEEE/CAA Journal of Automatica Senca*, 9(3), 377-391. <https://doi.org/10.1109/JAS.2021.1004261>

أنظمة ذكية قائمة على التعلم العميق للكشف المبكر عن الهجمات الإلكترونية في شبكات إنترنت الأشياء

ملخص

غير إنترنت الأشياء (IoT) طريقة اتصال الأجهزة الحديثة. تعمل مليارات الأجهزة الذكية الآن معًا في مجالات الرعاية الصحية، والنقل، والمصانع، والمنازل الذكية، والبنية التحتية الحيوية. إلا أن أجهزة إنترنت الأشياء صغيرة الحجم وغالبًا ما تعاني من نقص الموارد، مما يجعلها أهدافًا سهلة لهجمات خطيرة مثل هجمات الحرمان من الخدمة (DDoS)، وشبكات الروبوتات، وانتحال الهوية، وبرامج الفدية، واختراقات البيانات. لا تزال معظم أنظمة كشف التسلل (IDS) تعتمد على التوقيعات أو التعلم الآلي الأساسي، مما يصعب اكتشاف الهجمات الجديدة أو غير المعروفة في بيئات إنترنت الأشياء سريعة التغير. تُطوّر هذه الدراسة نظامًا للتعلم العميق قادرًا على اكتشاف الهجمات الإلكترونية مبكرًا في شبكات إنترنت الأشياء. يتضمن التصميم مرحلة معالجة بيانات كاملة، وتطبيقًا للميزات، ونموذجًا هجينًا للتعلم العميق. يستطيع النموذج نفسه إيجاد الأنماط المكانية والزمانية في حركة مرور الشبكة. يستخدم شبكات عصبية التلافيفية (CNNs) لاستخراج الميزات والتعلم من التسلسلات باستخدام شبكات الذاكرة طويلة المدى (LSTM). يوفر هذا النظام، مجتمعًا، دقة عالية في التعرف مع انخفاض الإنذارات الكاذبة. تم اختبار الإطار على مجموعة بيانات عامة لاختراق إنترنت الأشياء. وتم التحقق من الدقة، والذاكرة، ومقياس F1، ومساحة منحني ROC. تُظهر النتائج أن هذه الطريقة تفصل الحركة الطبيعية عن أنواع الهجمات المختلفة بدقة عالية، مما يجعلها مناسبة للاستخدام الفوري. بشكل عام، يوفر كشف التسلل باستخدام التعلم العميق طريقة قابلة للقياس ومرنة وفعالة لحماية أنظمة إنترنت الأشياء من التهديدات المتغيرة باستمرار.

الكلمات المفتاحية: إنترنت الأشياء، الأمن السيبراني، نظام كشف التسلل، التعلم العميق، كشف الهجمات السيبرانية، أمن الشبكات، الأنظمة الذكية، شبكات إنترنت الأشياء.