Journal of Engineering Strategy and Innovation
Volume 1, Issue 1, July – September (2026) Arrived: 02/06/2026: Accepted: 26/06/2026

RESEARCH ARTICLE

Digital Twin Enabled Cognitive Id Using Hybrid CNN-BiLSTM For Autonomous Threat Prediction In Smart IoT Ecosystems

V. Hemamalini [1], S. Banupriya [2], A.Vijayasri [3]

[1] Department of Electronics and Communication Engineering, Assistant Professor, New Prince Shri Bhavani College of Engineering and Technology, Tamil Nadu, India
[2] Department of Electronics and Communication Engineering, New Prince Shri Bhavani College of Engineering and Technology, Tamil Nadu, India
[3] Department of Electronics and Communication Engineering, New Prince Shri Bhavani College of Engineering and Technology, Tamil Nadu, India

[1] hemamalini@newprinceshribhavani.com

***Abstract*- Smart IoT systems become susceptible to advanced attacks owing to their fast proliferation. Hence, intelligent and adaptive security measures are essential. Traditional intrusion detection systems often suffer from poor context awareness, inadequate attack response time, and lack of adaptation to dynamic IoT environment. In order to overcome these challenges, in this paper we propose a Hybrid Attention-Driven Deep Learning (DL) based Cognitive intrusion detection (ID) and Autonomous Threat Prediction scheme for Digital Twin (DT)-based IoT ecosystem. Our proposed approach generates a virtual representation of IoT systems and its behavior to continuously monitor the status of the system. In order to enhance intrusion detection efficiency and analyze spatial-temporal attack characteristics, a hybrid DL approach incorporates CNN, BiLSTM networks and attention mechanism. Also, in order to predict attacks beforehand using behavioral patterns, a Threat Prediction Module is designed.**

Keywords: *Internet of Things (IoT), Threat prediction, Intrusion detection, DL, behavioural pattern analysis.*

1. INTRODUCTION

People have become more dependent on the Internet as its significance and influence have increased over time. Because of its constantly growing user base, the Internet has become a significant conduit for cybercrime [1]. Advanced technologies are being used in the developing digital ecosystem to convert physical assets from the real world into networked smart objects or things. Among other things, this interconnection establishes the basis of the IoT [2], permitting machine-to-machine, or M2M, communication for objects within the network. The IoT is the new paradigm of our times, where distributed applications and services affect every aspect of human life and smart gadgets and sensors from all over the world are connected in a worldwide grid. IoT is a desirable target for thieves due to its enormous economic impact and extensive influence on our lives, making cybersecurity a primary issue for the IoT ecosystem [3]. Despite decades of research on cybersecurity, the large-scale IoT design and the emergence of new threats make traditional approaches essentially ineffective. One of the primary security attribute s of modern networks is IDSs which detect attacks, unauthorized invasions, and malicious activity in networks [4]. An IDS keeps an eye on network or host activity, identifying whether it is typical or abnormal and notifying the system administrator if it is. Since IDSs (IDSs) are a tried-and-true way to safeguard assets and resources from unwanted activity, they have been extensively studied [5].

Conventional cybersecurity techniques, like rule-based IDSs and supervised machine learning (ML) classifiers, are not very flexible and often have significant false positives, poor context awareness, and energy inefficiency [6]. These margins are expressly problematical in idealized environments, where real-time sensitivity and minimal computing overhead are crucial. Moreover, current strategies usually lack the necessary cognitive flexibility to recognize new threats or react adequately to them in distributed, dynamic situations [7].

The digital transformation of physical configuration has been followed by a new age of intellectual systems called DTs. The importance of DTs is growing in modelling, monitoring, and control of cyber-physical systems [8]. High-fidelity practical clones can be used for smart city applications, healthcare, transport, and industrial automation. This allows the synchronization of digital and physical entities in real time. DTs help in continuous monitoring, anomaly detection, and prediction-based security management by providing a virtual view of the IoT devices and the network operations. Nevertheless, with increased autonomy and connectivity of DTs, there is an increase in the attractiveness of DTs as targets of cyberattacks. Dynamic cyber threats include spoofing, manipulation of data, and sophisticated persistent attacks [9].

There has not been sufficient attention to the combination of DT approaches and the use of cognitive and attention-based DL techniques for predicting and identifying dangers autonomously. Moreover, in dynamic IoT environments, existing DL approaches usually fall short in considering the temporal and spatial aspects of attacks, which leads to a higher rate of false alarms [10]. Inspired As a result of these limitations, an intelligent IoT ecosystem framework is presented in this study. In order to predict autonomous threats using DTs and cognitive intrusion detection, a hybrid attention-based DL is used. In the case of next-generation smart IoT ecosystems, the proposed model aims at improving real-time cyberattack detection, enhancing predictive intelligence, reducing false alarms, and providing adaptive protection. The major contributions of the study are outlined below:

1. To propose, a novel cognitive ID architecture based on DT to enable real-time monitoring in cyber threat analysis.

2. To integrate CNNs with BiLSTM, and attention mechanism to advance ID accuracy.

3. Based on behavioral pattern analysis and dynamic network activity, an autonomous threat prediction system is presented to proactively predict possible cyberattacks.

4. To show the superiority of the suggested framework, a thorough experimental analysis and comparative evaluation are carried out utilizing benchmark IoT intrusion datasets.

This paper serves as a reminder in the following format: A brief review of the literature is done in section 2, and the system model and preparatory work are designed in section 3. The suggested algorithmic structure is outlined in Section 4, and the comprehensive simulation results are shown in Section 5. Section 6 concludes the proposed work by highlighting its significance and providing an essential avenue for further research.

2. LITERATURE REVIEW

2.1 ML based IDS

Isam Bahaa Aldallal et al. [11] suggested a hybrid IDS for Internet of Things networks that combines Support Vector Machine and Genetic Algorithm for attribute selection and parameter tuning. 98.79% of assaults are detected, and overhead is reduced by 30%. Abdulwahid Al Abdulwahid et al. [12] proposed an IDS to detect various IoT network attacks using the CIC-IoT-2023 dataset. To extract the most relevant IoT network attribute s, Particle Swarm Optimization and Improved Binary Grey Wolf Optimization are combined. The Random Forest (RF) method, which employs several decision trees to get an accurate outcome, is also used to assess the selected attributes. FlowSense, an interpreTABLE IDS created especially for heterogeneous IoT contexts, was presented by Mehdi Pourbasirat et al. [13]. FlowSense makes use of precisely constructed flow-based attribute s that are obtained from network data recorded on the backbone that links IoT gateways. We utilize the GR-DT classifier in order to ensure that we obtain meaningful security intelligence. This is due to the interpretability inherent in the algorithm, allowing the security analyst to associate the classification outcome with the actual network behavior. This is an important feature that some DL-based IDS systems may lack. Shayma Wail Nourildean et al. [14] have created DTXGRF, an ensemble-based lightweight IDS based on Decision Tree, Random Forest, and XGBoost by applying the soft voting technique to enhance the efficiency of attack detection in IoT. In Besides contributing to the design of cutting-edge ML-based IDS methods, Jyoti Prakash Sahoo et al. [15] offer useful information about the practical application of IDS using ensemble learning methods in edge networks and the Internet of Things. This study introduced Choir-IDS, an innovative IDS system designed specifically for the edge-IoT setting with explainability and fidelity being key concerns. Choir-IDS was developed based on the metaphor of a “choir,” which stands for the harmony of collaboration. They developed "Neural Boosting Ensembles," which leverage the synergy of several ML models through federated learning.

2.2 DL based IDS

Amit Sagu et al. introduced a new set of hybrid DL-based IDS models intended for extended IoT scenarios [16]. To address the issues of adaptive learning, computational limitations, and real-time threat detection, we specifically recommend and enhance three IDS models CNN-LSTM,

GRU-AE, and Bi-LSTM-CNN using hybrid designs. FA-CNN-RNN, a novel crossbreed DL-based ID framework, was proposed by Samar M. Zayed et al. [17]. It combines a hybrid CNN–Recurrent Neural Network (CNN–RNN) design for efficient spatial–temporal attributes, the Firefly Algorithm for optimized IoT-specific attribute selection, and the Synthetic Minority Oversampling Technique for class imbalance handling. A Deep Blockchain-based IDS was proposed by Swathi Darla et al. [18] to guarantee data security and privacy in cloud networks used by healthcare services. To detect threats during network data transfer in cloud systems a attribute vector selection technique based on Adaptive Gray Wolf Optimization produces a collection of attribute vectors, and a Hybrid Deep Neural Network with Optimized Bidirectional Long Short-Term Memory (uses the IDS) reduces the classification time. The Bi-LSTM classifier detection rate is then increased by using Golden Search Optimization to choose the ideal weights for the hidden layers.

Mirza Qais Baig, Ali Turab, and Farhan Ullah [19] designed a two-stage temporal DL system called TIDE-Net particularly for the attribute s of IDSIoT2024. Stage 1 of the system uses twofold classification to distinguish between benign and harmful communication, while Stage 2 contracts with malicious traffic that is further classified into three coarse-grained attack categories or twelve fine-grained attack types.

Tianhao Liu and Omar Dib introduced a federated learning-based ID solution that preserves data privacy while enabling cooperative model training among scattered IoT devices [20]. By sharing only model parameters for global aggregation and directly training local models on device data, their approach guarantees efficiency and anonymity. By managing both IID and non-IID data distributions, the system effectively decreased the heterogeneity found in IoT networks.

2.3 DT based IDS

Nida Nasir and Hussam Hamad originally introduced an architectural framework that enhances adaptive cyber protection by combining spiking neural networks and event-driven cognition [21]. The NCT converts telemetry data from the digital-twin layer into spike-based sensory inputs by using neuromorphic concepts like temporal encoding, sparse coding, and spike-timing-dependent plasticity. A multi-layered cognitive architecture keeps an eye out for irregularities in behavior and makes inferences about them.

A context-aware IDframework called CATwin-IDS was suggested by Chang Liu et al. [22]. It combines DT technology with a lightweight Distilled Bidirectional Encoder Representations from Transformers (DistilBERT) model. In our design, Temporal Self-Attention (TSA) improves the modeling of spatiotemporal dependencies across heterogeneous traffic, while Conditional Mutual Information (CMI) and Borderline Synthetic Minority Over-sampling Technique (Borderline-SMOTE) are used for attribute optimization and data balancing.

In order to provide low-latency inference appropriate for near-real-time IIoT monitoring, Shailendra Mishra et al. [23] proposed a Zero Trust-enhanced IDframework that integrates DL anomaly detection, differential privacy, lightweight blockchain-inspired hash-chained ledger, DT-based situational awareness, and visualization of device trust states.

A self-adaptive federated IDS for IoT environments enabled by DTs was presented by Sakthi Maheswari B and Deepa M. A DT employs a lightweight autoencoder that has been locally trained to detect abnormalities at resource levels that are fairly constrained. When the data distribution is non-IID and heterogeneous, the FedProx aggregation approach is utilized to ensure sTABLE convergence and differential privacy is used to protect the privacy of the data being used. Additionally, by regulating local learning behavior, a self-adaptive training mechanism reduces communication overheads.

In order to create a proactive, self-diagnostic, and tamper-resistant security framework for vital IoT infrastructure, Ashit Kumar Dutta et al. [25] introduce "Causio-TwinChain," a new security architecture that synergistically incorporates three cutting-edge technologies. A DT is a virtual duplicate that uses sandboxing to keep an eye on actual gadgets in real time. Data integrity and auditability are guaranteed via a permissioned blockchain, which offers an unchangeable, tamper-proof ledger for all device data and transactions.

3. IDS MODEL

3.1 Smart IoT

A smart IoT ecosystem consisting of cloud servers, gateways, edge nodes, heterogeneous IoT devices, and centralized security management units is taken into consideration by the proposed framework. Smart sensors, wearables, industrial controllers, healthcare monitoring devices, and intelligent home appliances are all part of the IoT environment. These gadgets constantly share data via wireless communication networks.

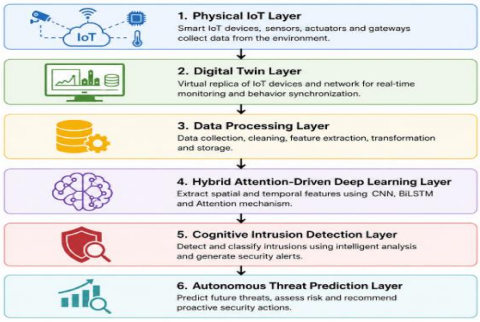

Figure 1. Smart IoT Architecture

The physical IoT ecosystem incorporates a DT layer to improve cybersecurity and intelligent monitoring. In order to continuously monitor system activity, communication patterns, and resource use, the DT builds virtual copies of IoT devices and network entities. The virtual environment allows for intelligent behavioral analysis for IDand autonomous threat prediction, and it synchronizes with the actual IoT network in real time.

3.2 DT Model

The DT framework replicates the real-time behavior of physical IoT devices and serves as a virtual cybersecurity monitoring platform. Every IoT device has a virtual duplicate that keeps track of operational data such as resource usage, communication history, traffic patterns, and device status. Each IoT device $X_i$comprises its own system state parameters S_i, traffic and communication behaviour T_i and device information D_i.the DT of the IoT device $X_i$is represented as XT_i Then the synchronization between the physical device and the DT can be represented as:

$$XT_i = f(D_i, S_i, T_i) \quad (1)$$

The DT detects departures from typical behavioral patterns and continuously modifies the virtual environment based on real-time network activity. Proactive threat monitoring and intelligent anomaly analysis are made possible by this synchronization.

3.3 Network Traffic Model

Large-scale heterogeneous traffic data with both benign and malevolent communication patterns is produced by the intelligent Internet of Things environment. Let t_n stand for network characteristics like packet size, transmission rate, protocol type, source address, destination address, and connection duration. Let the network traffic be written as $\{T = t_1, t_2, \dots t_n\}$

3.4 Threat Model

For intelligent intrusion detection, the suggested system uses a hybrid attention-driven DL model. To capture both spatial and temporal assault characteristics, the model integrates CNNs BiLSTM, and attention mechanisms. While the BiLSTM layer records temporal behavioral patterns and sequential dependencies, the CNN layer uses network traffic data to extract local spatial attribute s. By giving important attack-related attribute s more weights, the attention mechanism improves attribute learning even more. The BiLSTM model's hidden state is depicted as:

$$h_t = BiLSTM(I_t, h_{t-1}) \quad (2)$$

Where h_t is the hidden state and I_t is the input sequence.

The attention score is calculated as:

$$a_t = \frac{\exp(e_t)}{\sum_{k=1}^{T} \exp(e_k)} \quad (3)$$

Where a_t is the attention weight ande_t is the alignment score.

3.5 Problem Formulation

In dynamic IoT contexts, the core objective of the suggested framework is to optimize IDaccuracy while reducing false positive rates, detection delay, and computing overhead. The problem of multi-objective optimization is expressed as follows:

$$O(X) = \max [w_1 Acc - w_2 FPR - w_3 CO - w_4 DL] \quad (4)$$

Constrained to:

$$B_i \leq B_{max} \quad (5)$$

$$E_i \leq E_{max} \quad (6)$$

$$L_i \leq L_{threshold} \quad (7)$$

Where $w_1, w_2, w_3$and $w_4$are the weighting coeffiecnts.

4. PROPOSED DT ASSISITED COGNITIVE IDS

The suggested framework combines hybrid attention-driven DL with DT technology to provide autonomous threat prediction and intelligent ID in smart IoT ecosystems. The framework continuously keeps an eye on network activity, evaluates device behavior, finds cyberthreats, and makes real-time predictions about upcoming assaults. As seen in Figure 2, the suggested framework's workflow consists of six steps.

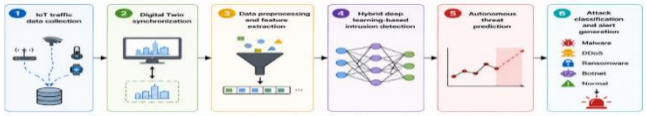

Figure 2. Proposed framework

4.1 Data Collection

Network traffic data is first gathered using the suggested framework from IoT devices, gateways, and communication routes. Both benign and malicious traffic examples can be found in the gathered data. Preprocessing the gathered data is required to improve the detection accuracy.

4.2 Preprocessing

As shown in Figure 3, the preprocessing is performed in four stages.

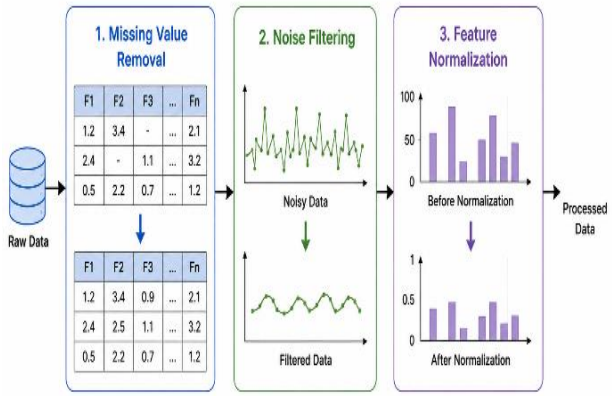

Figure 3. Preprocessing Steps

4.3 Missing value Removal

The missing value is substituted using mean-based imputation as follows:

$$x_j = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (8)$$

Where x_j is the replaced missing value, N is the total number of samples and x_i is the available attribute value.

4.4 Filtering

Noise filtering is executed to advance the reliability of extracted attributes. The filtered attribute vector X_{filter} is represented as:

$$X_{filter} = X + n \quad (9)$$

Where X is the original traffic data and n is the noise.

4.5 Normalization

To scale the attribute values between 0 and 1, min-max normalization is used. The normalized attribute vector X_{norm} is calculated as:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (10)$$

Where X_{max} is the highest attribute value and X_{min} is the lowest attribute value.

4.6 Hybrid Attention-Driven DL Model

The suggested ID model enhances cybersecurity intelligence by combining CNN, BiLSTM, and attention methods.

4.6.1. Extraction of Spatial Attribute s Using CNN

From IoT network traffic data, the CNN layer extracts spatial attack characteristics and local traffic patterns. The convolution process is shown as:

$$F(i,j) = (X * k)(i,j) \quad (11)$$

Where $F(i,j)$ is the extracted attribute map, X is the input attribute matrix and k is the convolution kernel,

4.6.2. BiLSTM-Based Temporal Learning

Sequential attack behaviors and long-term interdependence in IoT traffic sequences are captured by the BiLSTM layer. The representation of the forget gate operation is:

$$f_t = \sigma(W_t[h_{t-1}, x_t] + b_f \quad (12)$$

The cell state update is represented as:

$$C_t = f_t * C_{t-1} + i_t * C_t' \quad (13)$$

Attack sequence learning and anomaly detection capabilities are both improved by the BiLSTM design.

4.6.3. Attention Mechanism

By allocating adaptive importance weights, the attention mechanism allows the model to concentrate on important attack-related characteristics. This is how the attention function is expressed:

$$attention(Q,K,V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (14)$$

This method greatly increases classification accuracy while decreasing the influence of irrelevant attribute s..

4.6.4. Cognitive Intrusion Detection

The cognitive IDmodule uses intelligent traffic behavior analysis to categorize network activity as either malicious or legitimate. The classification function for Softmax is shown as:

$$P(y_i) = \frac{\exp(z_i)}{\sum_{k=1}^{T}\exp(z_k)} \quad (15)$$

Where $P(y_i)$ is the probability of attack class and $z_i$denotes classification score.

4.7 Autonomous Threat Prediction

Proactive cybersecurity defense is made possible by the prediction module before real attacks take place. The forecasting function is shown as:

$$T_p = f(X_t, H_t) \quad (16)$$

whereT_p denotes predicted threat, $X_t$denotes current traffic behaviour and $H_t$denotes historical attack patterns.

5 SIMULATION RESULTS AND ANALYSIS

A high-dimensional IoT network traffic dataset that included both benign and malevolent communication patterns was used to assess the suggested DT-Assisted Cognitive ID and Autonomous Threat Prediction architecture. Python with the TensorFlow and Keras DL packages was used to create the experimental environment. To increase the effectiveness of model training, the simulations were run on a system with an Intel Core i7 processor, 16 GB RAM, and NVIDIA GPU acceleration.

CNN, LSTM, CNN-LSTM Hybrid Model, and Attention-Based DL Model were among the baseline methods that were used to compare the performance of the suggested model.

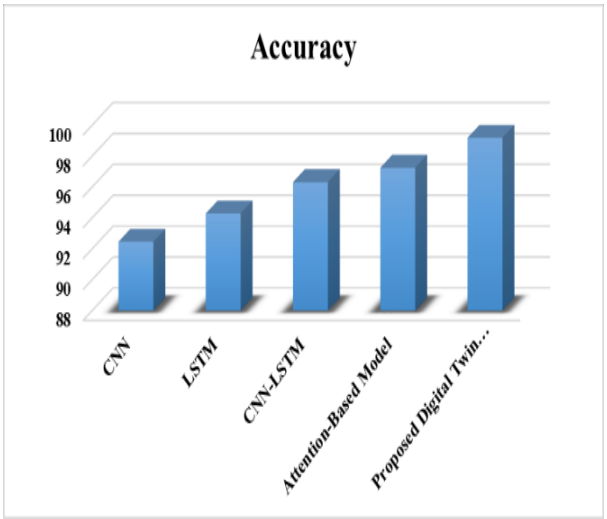

Figure 4. Performance in terms of Accuracy

The suggested DT-Assisted Hybrid Attention DL system attains the greatest classification accuracy of 99.18%, as shown in Figure 4.

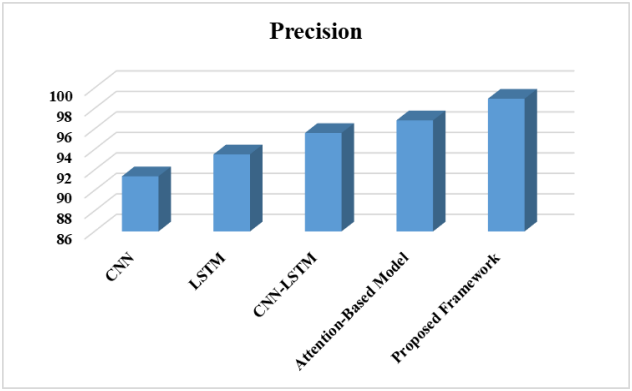

Figure 5. Performance in terms of Precision

Figure 5 illustrates how the attention mechanism's intelligent attribute prioritizing and the DT architecture's continuous behavioural synchronization allow the suggested framework to attain a superior precision value of 98.95%.

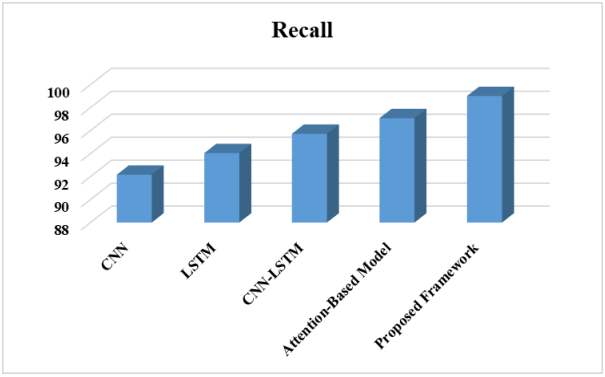

Figure 6. Performance in terms of Recall

The suggested model exhibits outstanding recall performance in Figure 6, demonstrating its capacity to identify even intricate and obscure assault activities in IoT environments.

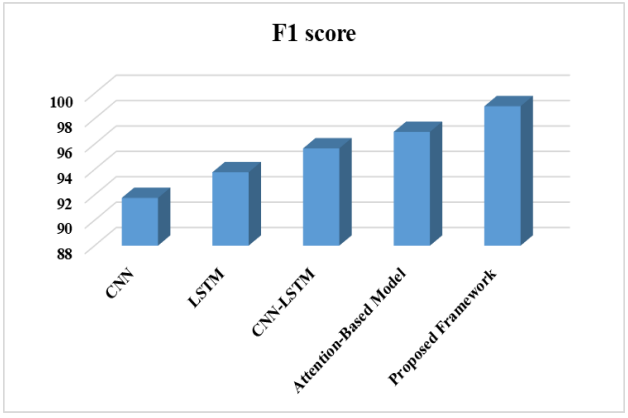

Figure 7. Performance in terms of F1 score

Figure 7 demonstrates how the framework's enhanced anomaly categorization and adaptive learning capabilities result in the greatest F1-score (98.98%).

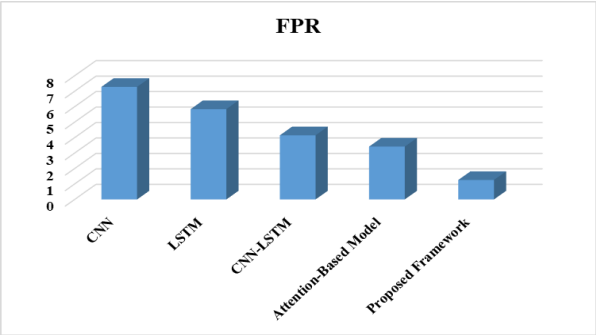

Figure 8. Performance in terms of FPR

Because the DT regularly updates traffic behavior profiles and increases attack classification accuracy, it is evident from Fig. 8 that the suggested framework obtains the lowest FPR. Prior to an actual breach, the autonomous threat prediction module forecasts potential cyberthreats. Table 1 displays the accuracy of threat prediction.

Table 1. Threat Prediction Accuracy

Model	Prediction Accuracy (%)
CNN-LSTM	92.14
Attention-Based Model	95.63
Proposed Framework	98.74

An essential component of IoT ecosystems with limited resources is computational efficiency. The computational efficiency of the suggested framework is displayed in Table 2.

Table 2. Performance in Terms Of Computational Efficiency

Model	Training Time (s)	Detection Latency (ms)
CNN	285	24
LSTM	321	28
CNN-LSTM	356	22
Attention-Based Model	374	19
Proposed Framework	338	14

The suggested approach maintains good detection performance while reducing detection latency. The DT minimizes needless computing overhead and improves network monitoring operations.

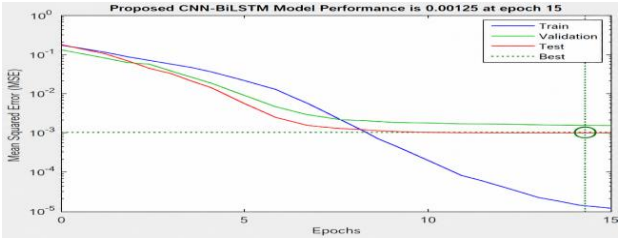

Figure 9. Performance of CNN-BiLSTM

While the BiLSTM layer captures long-term temporal relationships in IoT traffic sequences, the CNN layer effectively extracts spatial attack information, as demonstrated by the training curve in Figure 9. Strong generalization capacity and little overfitting are demonstrated by the testing and validation curves' continued stability and close alignment. With an MSE of around 0.00125, the best validation result is obtained at epoch 15, demonstrating the durability and dependability of the suggested framework for autonomous threat prediction and intelligent intrusion detection.

6 CONCLUSION

This work presented a hybrid attention-driven DL approach for DT-assisted cognitive ID and autonomous threat prediction in safe IoT ecosystems. The system utilizes the integration of DL approaches along with DT techniques to offer real-time monitoring and predictive analysis of network traffic data. The complex geographical and temporal characteristics of network traffic can be effectively captured due to the capability of the proposed model's hybrid attention-driven architecture that will ensure precise recognition of both known and unknown cyber threats. This approach will be especially useful in large IoT networks where high levels of accuracy are needed but computational cost must be reduced. Proactive cyber security defense becomes possible through predictive attack detection.

REFERENCES

[1] Afaq, Syed Adnan, Mohd Shahid Husain, Almustapha Bello, and Halima Sadia. "A critical analysis of cyber threats and their global impact." In Computational intelligent security in wireless communications, pp. 201-220. CRC Press, 2023.

[2] Serpanos, Dimitrios, and Marilyn Wolf. "Internet-of-Things (IoT) Systems." Architectures, Algorithms, Methodologies (2018).

[3] Chai, Yuqing. "Understanding the power of connection: An analysis of the Internet of Things." In 2025 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), pp. 1-5. IEEE, 2025.

[4] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29, no. 7 (2013): 1645-1660.

[5] Rakas, Slavica V. Boštjančič, Mirjana D. Stojanović, and Jasna D. Marković-Petrović. "A review of research work on network-based scada IDSs." IEEE Access 8 (2020): 93083-93108.

[6] Hozouri, Ali, Abbas Mirzaei, and Mehdi Effatparvar. "A comprehensive survey on IDSs with advances in machine learning, DL and emerging cybersecurity challenges." Discover Artificial Intelligence 5, no. 1 (2025): 314.

[7] Mohamed, Nachaat. "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms." Knowledge and Information Systems 67, no. 8 (2025): 6969-7055.

[8] Iranshahi, Kamran, Joshua Brun, Tim Arnold, Thomas Sergi, and Ulf Christian Müller. "DTs: Recent advances and future directions in engineering fields." Intelligent Systems with Applications 26 (2025): 200516.

[9] Maria Priska A, Dr.K.Madhan Kumar, Mrs.X.M.Binisha, & Ms.K.Sneha. (2025). Novel And Hybrid Frameworks for Attack Detection And Secure Transmission in Manet. International Journal of Advanced Engineering and Management System, 1(3), 204-213. https://doi.org/10.65379/tpsn2013/ijaemsv01i03p3

[10] Hassija, Vikas, Vinay Chamola, Rajdipta De, Soham Das, Arjab Chakrabarti, Kuldip Singh Sangwan, and Amit Pandey. "A survey on DTs: enabling technologies, use cases, application, open issues, and more." IEEE Journal of Selected Areas in Sensors 2 (2024): 84-107.

[11] Aldallal, Isam Bahaa, Abdullahi Abdu Ibrahim, and Saadaldeen Rashid Ahmed. "An Intelligent Multi-Stage GA–SVM Hybrid Optimization Framework for Attribute Engineering and IDin Internet of Things Networks." Computers, Materials, & Continua 87, no. 1 (2026).

[12] Al Abdulwahid, Abdulwahid, Saad Said Alqahtany, Darakhshan Syed, Mana Saleh Al Reshan, Khairan Rajab, and Asadullah Shaikh. "A hybrid improved binary GWO-PSO with random forest (IBGWO-PSO-RF) based IDmodel for large-scale attacks in IoT environment." Scientific Reports (2026).

[13] Pourbasirat, Mehdi, Majid IranPour Mobarakeh, and Behzad Soleimani Neysiani. "FlowSense: InterpreTABLE Micro-Temporal Flow-Based IDfor IoT Networks Using Gradient-Regularized Decision Trees on RT-IoT2022 Dataset." In 2026 12th International Conference on Web Research (ICWR), pp. 383-389. IEEE, 2026.

[14] Nourildean, Shayma Wail, Wafa Mefteh, and Ali Mohsen Frihida. "IDS-based ensemble machine learning to improve IoT network against cyber attacks." The Journal of Supercomputing 82, no. 6 (2026): 370.

[15] Sahoo, Jyoti Prakash, Binayak Kar, Ahmed M. Abdelmoniem, and Dimitris Chatzopoulos. "Choir-IDS: A federated learning framework for fidelity-calibrated explainable IDS for edge-IoT networks." Information Fusion 125 (2026): 103473.

[16] Sagu, Amit, Nasib Singh Gill, Preeti Gulia, Piyush Kumar Shukla, Ayman Sabry, and Mohamed M. Hassan. "Scalable and InterpreTABLE DL-Based IDFramework for Secure Internet of Things Networks." Security and Privacy 9, no. 1 (2026): e70179.

[17] Zayed, Samar M., Samah Alshathri, and Walid El-Shafai. "Firefly Algorithm Optimized Hybrid DL Framework for IDin IoT Environments." International Journal of Computational Intelligence Systems 19, no. 1 (2026): 158.

[18] Darla, Swathi, Naveena C, B. N. Ajay, and Muzameel Ahmed. "An optimized Bi-LSTM with DL-based IDS in healthcare using Blockchain." Information Security Journal: A Global Perspective 35, no. 1 (2026): 140-153.

[19] Qais Baig, Mirza, Ali Turab, and Farhan Ullah. "TIDE-Net: A Two-Stage Temporal DL Framework for Multi-Granular IoT Intrusion Detection." Concurrency and Computation: Practice and Experience 38, no. 4 (2026): e70604.

[20] Liu, Tianhao, and Omar Dib. "Advanced IDfor IoT devices using federated DL: T. Liu, O. Dib." International Journal of Information Security 25, no. 1 (2026): 19.

[21] Nasir N and Al Hamadi H (2025) Towards the neuromorphic Cyber-Twin: an architecture for cognitive defense in DT ecosystems. Front. Big Data 8:1659757. doi: 10.3389/fdata.2025.1659757

[22] Liu, Chang, Yurong Zhang, Zheng Xue, Zhengguo Sheng, Jiawen Kang, and Guojun Han. "CATwin-IDS: Context-Aware IDS for Both In-Vehicle and External-Vehicle Networks via DT." IEEE Transactions on Intelligent Transportation Systems (2026).

[23] Mishra, Shailendra, Tariq Saleh M. Aldafas, and Naif S. Alshammari. "A zero-trust DT framework for privacy-preserving multi-dataset IDin industrial IoT with lightweight blockchain auditing." Scientific Reports (2026).

[24] Deepa, M. "A Privacy-Preserving Self-Adaptive Federated IDFramework for DT Environments." In 2026 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), pp. 1-7. IEEE, 2026.

[25] Dutta, Ashit Kumar, Mohd Anjum, Hong Min, Yousef Ibrahim Daradkeh, Jung Taek Seo, and Sana Shahab. "DT-assisted blockchain IoT security model using contrastive and causal learning techniques." Scientific Reports (2026).