KINGDOM OF SAUDI ARABIA
Northern Border University (NBU)
Journal of the North for Basic & Applied Sciences(JNBAS)
p - ISSN : 1658 -7022 / **e-ISSN:** 1658 - 7014
www.nbu.edu.sa
s.journal@nbu.edu.sa

Blockchain-Driven Privacy Preservation for Robust IoT Security with an Attribute-Reduced Hybrid Deep Representation Learning Approach

Sultan Alkhliwi
Associate Professor, Department of Computer Science, Faculty of Science, Northern Border University, Saudi Arabia-Arar

(**Received:** 13th September 2025; **Accepted:** 9th November 2025)

Abstract

The Internet of Things (IoT) is highly vulnerable to cyberattacks, such as denial-of-service attacks. An intrusion detection system (IDS) is an effective cybersecurity device mainly used to detect malicious behaviours. Recently, blockchain technology has emerged as a secure framework for the IoT by ensuring privacy and reliability. This study introduces a model in an IoT environment called Blockchain-based Attack Detection using Dimensionality Reduction and Hybrid Deep Learning Model (BCAD-DRHDLM) to enhance cybersecurity in the IoT. The model integrates several advanced techniques for the process of attack classification: Z-score standardisation system for the data pre-processing step to scale and standardise data for improved model performance, sparrow search algorithm for model of feature selection to recognise and retain pertinent features from input data and a hybrid convolutional neural network and bi-directional gated recurrent unit with additive attention mechanism (Conv-BiGRU-AA) technique. In addition, the farmer ants optimisation algorithm technique is used in the parameter refinement procedure to enhance the classification performance of the Conv-BiGRU-AA method. The BCAD-DRHDLM is validated in terms of the Edge-IIoT and ToN-IoT datasets. In comparison studies, the BCAD-DRHDLM achieves significantly higher precision values than other existing models in both datasets.

Keywords: blockchain, IoT, Farmer Ants Optimisation Algorithm, cybersecurity, DDoS, deep learning, Dimensionality

1658-7022© JNBAS. (1447 H/2026). Published by Northern Border University (NBU). All Rights Reserved.

(*) **Corresponding Author**:
Sultan Alkhliwi
Associate Professor, Department of Computer Science, Faculty of Science, Northern Border University, Saudi Arabia-Arar
Email: salkhliwi@nbu.edu.sa
Orcid: https://orcid.org/0000-0002-3481-549X

DOI: 10.12816/0062490

1. Introduction

Currently, internet connectivity is provided in a growing number of places. The prevalent use of connected gadgets and cloud technologies has allowed novel kinds of computation outsourcing and data, along with the emergence of the Internet of Things (IoT) [1]. The upsurge in IoT gadgets and network technologies is also rapidly developing. Either the development of gadgets or technology has inspired the advancement of decentralisation methods for different scenarios [2]. Consequently, it relies on an entity or a single gadget to present resources and services due to the collaboration between many communication nodes [3]. The cybersecurity of computer systems is a significant issue. If a given application necessitates handling sensitive data, it is typically resolved by safeguarding a given device or node. Even though this solution is cost-effective, it also contains one point of failure risk [4]. Various cyber threats comprise distributed denial-of-service (DDoS), and denial-of-service (DoS) attacks are generally performed by humanly instructed methods, such as bots or botnets, which contain many gadgets with internet access [5]. Bots can exist when a computer is infected with malware through particular software. These bots carry out multiple threats, such as data stealing, ransomware or DDoS. DoS attacks are a type of menacing, intrusive and aggressive behaviour on online servers [6]. They seriously reduce the accessibility of the victim, router, host or overall network, causing severe harm to services [7]. Thus, effective recognition of DoS attacks is vital to security. Improving attack recognition is generally aimed at the progression of network-based recognition mechanisms. Fig. 1 presents the general architecture of blockchain (BC)–IoT in cybersecurity.

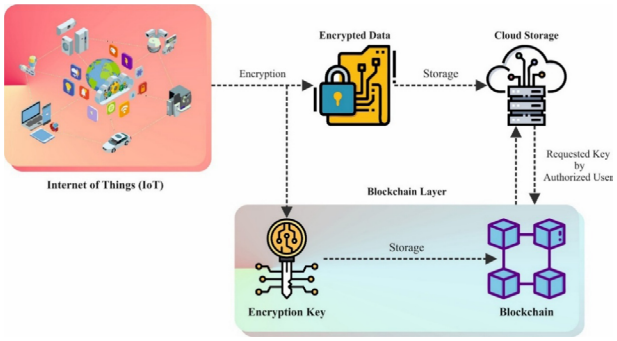

Fig. 1. General architecture of BC-IoT in cybersecurity

BC technology provides decentralised storage in which data are securely stored without requiring a single trusted party. It has previously been implemented in multiple diverse scenarios [8]. In the previous year, BC technology was accepted in various application fields to increase security concerns in a decentralised manner. Owing to its nature, this technology can be directly applied to IoT smart home settings, as it can aid security-related use cases [9]. Recently, the utilisation of BC technology has attracted interest in the field of cybersecurity. Specifically, the use of smart contracts (SC) was combined with implementing and designing the DoS defence mechanism. An intrusion detection system (IDS) is a cybersecurity system feature that identifies systems and networks from policy breaches or malicious activities. IDS has recently attracted much attention and popularity from security experts for safeguarding IoT gadgets, and it is a hybrid method that integrates more IDS approaches [10]. Investigators are motivated to use decentralised IDS, which incorporates several deep learning (DL) and machine learning (ML) methodologies in analysing the existing progression in intelligent machines. The application of multiple DL techniques identifies risks using two classifications to categorise different threats with multi-class classification into a determined investigation field.

This study presents the Blockchain-based Attack Detection using Dimensionality Reduction and Hybrid Deep Learning Model (BCAD-DRHDLM) for IoT environments. The BCAD-DRHDLM is an effective model for enhancing cybersecurity in IoT networks by developing robust threat detection mechanisms to mitigate evolving security risks. The Z-score system is used in the data pre-processing phase to scale and standardise data for improved model performance. The sparrow search algorithm (SSA) is used in the FS procedure to detect and retain related features from the input data. Moreover, the hybrid convolutional neural network and bi-directional gated recurrent unit with additive attention mechanism (Conv-BiGRU-AA) technique is implemented for attack classification purposes. The parameter fine-tuning model is executed using the farmer ants optimisation algorithm (FAOA) technique. The efficacy of the BCAD-DRHDLM is validated using the Edge-IIoT and ToN-IoT datasets. The major contributions of the BCAD-DRHDLM are summarised as follows:

The BCAD-DRHDLM uses the Z-score to convert input features into a common scale without changing variances in the value ranges. This standardisation improves training consistency and accelerates model convergence. It improves the learning stability of the attack classification framework.

The BCAD-DRHDLM implements the SSA method to select related features from higher-dimensional input data, effectively eliminating redundancy and noise. This optimisation mitigates computational load and improves detection precision. It also significantly enhances the complete efficiency of the attack classification model.

The BCAD-DRHDLM applies the hybrid Conv-BiGRU-AA model, integrating convolutional layers

for the spatial extraction of the features, BiGRU for capturing the temporal dependencies, and an additive attention mechanism for focusing on critical patterns. This integration improves classification precision by learning intrinsic representations. It assists in the robust detection of various attack types in IoT data.

The BCAD-DRHDLM utilises the FAOA technique for hyperparameter tuning, which improves the convergence rate and effectively fine-tunes critical parameters. This strategic tuning process significantly enhances model performance by optimising learning dynamics. It also assists in achieving stable and efficient training outcomes.

The integration of SSA-based feature selection with the Conv-BiGRU-AA classifier and FAOA tuning introduces a novel and cohesive framework that effectively balances high accuracy, computational efficiency and adaptive optimisation. This unique integration enhances attack detection by mitigating irrelevant data while capturing complex spatial-temporal patterns. Adaptive tuning additionally refines the model parameters for robust and reliable performance in dynamic environments.

2. Literature Review

Selvarajan et al. [11] advanced a decentralised identifiable distributed ledger technology-BC (DIDLT-BC) structure in which private and public keys are generated to prove the transaction. The block employs DIDLT and contains the timestamp, block header information, transaction list and hash code. The main objective is to find numerous untrustworthy nodes with differing hash values. In [12], the authors examined BC and federated learning (FL) for IoT. The projected approach gathers real-world data, namely environmental conditions and traffic flow, and then encrypts, normalises and strongly keeps them on a BC to guarantee tamper-proof data management. The DAC employs progressive cryptographic models for secure data access in another stage. Ponnuru et al. [13] projected a BC-aided authentication protocol built particularly for fog-enabled IoT settings to examine the identity of users before accessing IoT gadgets. The proposed protocol applies sophisticated crypto primitives, such as hash functions, elliptic curve cryptography and BC, to determine protected communication among IoT gadgets and users. Alamri et al. [14] developed an assessment of cybersecurity threat management and a structure for BC-based identity management systems (BC-IdM) in the medical IoT. In this study, a Delphi approach is employed to examine the architecture that contains the features, which is leveraged to assess any HIoT BC-IdM methods and the cybersecurity risk management activities and processes that might be implemented. Kumar and Das [15] advanced an improved radio frequency identification authentication protocol that combines BC and edge computing. This method also uses the real-world processing capability of edge computing, immutability of BC and decentralisation. Makhahlela et al. [16] developed a lightweight BC-based secure communication protocol that combines BC technology and lightweight encryption to generate a robust and comprehensive security solution for IoT networks. By using this technology, the proposed approach safeguards data privacy, authenticity and integrity while reducing resource utilisation in IoT gadgets, therefore addressing the unique constraints of IoT gadgets.

Pokharel et al. [17] introduced the blockHealthSecure structure that combines BC technology with cutting-edge cybersecurity procedures. The BC's immutable and decentralised framework improves the transparency, accuracy and security of electronic medical records and sensitive medical care data. Ismail et al. [18] presented a combined security architecture utilising ML and BC methods. The structure contains dual modules: ML detection and BC prevention modules. The BC prevention component has two mechanisms, trust and identity management, which use a lightweight SC to control authentication and node registration. The ML recognition component leverages the light gradient boosting machine model for classifying mischievous nodes and notifying the BC network. Kuru and Kuru [19] developed a BC-based decentralised privacy-preserving ML (DPPML) method that integrates FL to enhance identity protection and cybersecurity. The approach aims to prevent identity impersonation, credential and avatar theft and unreal transactions by removing single points of failure and detecting malicious nodes, including generative adversarial network (GAN) attacks. In [20], the authors examined a lightweight and privacy-preserving vehicular task offloading strategy utilising an attention-based heterogeneous GNN (HetGNN) within a space–air–ground integrated vehicular network, optimising latency and scalability in the Internet of Vehicles (IoV) environment. In [21], the authors developed a protected attack detection method for vehicular ad hoc networks (VANETs) by utilising the modernised random parameter-based green anaconda optimisation technique for feature selection and an ensemble machine learning model by integrating MLP, SVM, AdaBoost and Bayesian networks for accurate detection and classification of attacks. Andrei et al. [22] proposed a privacy-preserving synthetic data generation model using deep convolutional generative adversarial network (DCGAN) methodology for histopathology images of colorectal cancer, improving classification accuracy while protecting sensitive medical data. Danquah et al. [23] presented a low-complexity FL model using differentially private MLP (DP-MLP) and principal component analysis (PCA) techniques for the accurate detection of IoT botnet attacks on resource-constrained edge devices.

Kathole et al. [24] developed an ensemble DL method for IDS in IoT networks by effectively detecting and preventing unauthorised access. Nazir et al. [25] compared ensemble ML and hybrid NN techniques for precise and efficient IoT threat detection using key datasets to enhance IoT safety. A secure federated cloud storage system was developed for the Internet of Medical Things (IoMT) by applying hybrid heuristic attribute-based encryption with the permitted BC and FL using multiscale bi-long short-term memory (Bi-LSTM) [26]. The gated recurrent unit (GRU) technique ensures data confidentiality, privacy preservation and accurate disease prediction. An SC-aided BC framework integrated with ML was proposed for protected and privacy-preserving authentication in IoV using a hybrid adaptive network with MLP and ridge classifiers, optimised through the opposition beluga whale optimisation technique for effective malware detection [27]. Nazir et al. [28] systematically reviewed ML and DL models to identify IoT botnet assaults. Ganesh et al. [29] presented a BC-integrated secure data storage and task offloading framework using adaptive multiscale dilated BiLTM for user authentication and improved nuclear reaction optimisation for tuning and key generation. Hybrid attribute-based encryption with an elliptical curve cryptography model was applied to secure low-power data encryption and transmission. In [30], the authors improved IoT safety by integrating cooperative threat intelligence, BC technology and ML methods into the IoT23 dataset to increase threat recognition accuracy and reduce false negatives. Kadiyala et al. [31] developed a decentralised IDS for IoT using BC, homomorphic encryption and DL methods such as convolutional LSTM and GRU, incorporating secure hash algorithm (SHA-256), L-Diversity and digital signatures for improved privacy, anomaly detection and system integrity. Nazir et al. [32] improved IoT security by integrating FL with BC technology, using DNNs and LR in the N-BaIoT dataset to achieve high accuracy and secure decentralised model training. Slama et al. [33] presented an ML model BC-based privacy-preserving technique utilising BC and cryptographic hash functions for secure storage, integrity and reliable misbehaviour detection in VANETs.

Despite crucial improvements in integrating BC, FL, ML and DL for securing IoT, IoV and VANET environments, a key research gap exists in the unified deployment of lightweight, real-time and privacy-preserving mechanisms under constrained computational resources. Most techniques emphasise either detection accuracy or data privacy but not both simultaneously with lesser latency. Various studies lack robustness against adversarial threats, such as GAN-based attacks and do not adequately address scalability in decentralised frameworks. Moreover, the integration clarity between BC and IDS or ML models remains limited in many models. The absence of standardised evaluation metrics and real-time interaction among SCs, encryption modules and detection systems also marks a critical research gap.

3. Methodological Frameworks

This study proposes the BCAD-DRHDLM for IoT environments. It is an effective model for enhancing cybersecurity in IoT networks by developing robust threat detection mechanisms to mitigate evolving security risks. The BCAD-DRHDLM involves different levels, such as data pre-processing, feature selection, classification and parameter tuning. Fig. 2 illustrates the overall process of the BCAD-DRHDLM.

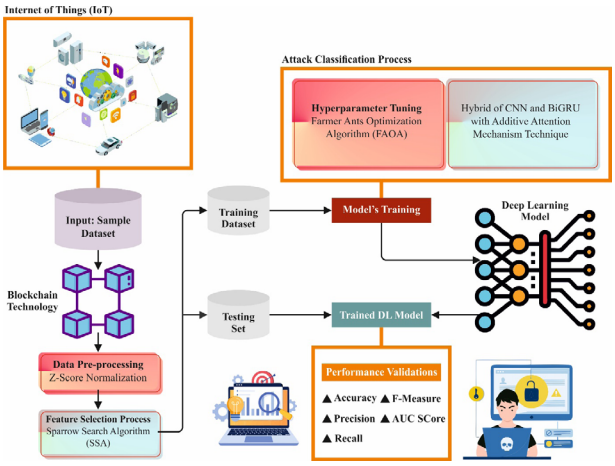

Fig. 2. Overall working process of the BCAD-DRHDLM

3.1 Data Pre-Processing Model

Initially, the Z-score model is used in the data pre-processing phase to measure and normalise data for enhanced model performance [34]. This model is chosen because it standardises data by transforming features to have a standard deviation of 1 and a mean of 0, making diverse features comparable regardless of their original scales. It is useful for algorithms sensitive to feature scales. Unlike min-max scaling, which compresses data into a fixed range and can be affected by outliers, this model is stronger, as it corresponds to data distribution. It preserves the shape of the original distribution and is effective when data follow a Gaussian distribution. Overall, it enhances convergence speed and model performance by ensuring that features contribute equally during training.

The Z-score model is a statistical method applied to standardise data by translating them into a general measure. In the cybersecurity framework, this method aids in noticing anomalies by emphasising deviances from usual behaviour in device activities, network traffic or transaction designs. This model guarantees that dissimilar features donate similarly to security models, thereby averting bias from main features. This increases the correctness of ML techniques for intrusion detection

and fraud recognition in IoT networks. By standardising data, BC-based security structures can handle transactions more effectively and precisely recognise latent attacks. This method reinforces the trustworthiness and reliability of IoT methods by enhancing real-time attack detection.

3.2 SSA-Based Feature Selection Process

The SSA identifies and retains the most related features from input data for feature selection [35]. This approach is selected for its efficiency in discovering larger composite searching regions and avoiding local best through its swarm intelligence-inspired mechanism. Compared with conventional methods, such as particle swarm optimisation, SSA provides faster convergence and a better balance between exploration and exploitation. It is simple to implement and requires fewer parameters, thus mitigating computational overhead. SSA effectively detects the most relevant features, improves model accuracy, reduces dimensionality and improves training speed and generalisation performance. This makes it appropriate for handling high-dimensional datasets in ML tasks.

The SSA is a population-based intelligence optimiser model stimulated by a sparrow's antipredator and foraging behaviours that constantly upgrade the population location over iterations until the best solution is gained. The model considers the sparrow's searching behaviour as the 'leader–follower' method that focuses on separating the population's individuals into followers and leaders. It is stimulated by the sparrow's anti-predation and foraging behaviours. As a result, the sparrow optimiser model is applied to improve the levels of decomposition and penalty features. The position of the leader equation is upgraded to the following: X_{ij}^{τ}

$$\sum_k \frac{\|\hat{u}_k^{n+1}-\hat{u}_k^n\|_2^2}{\|\hat{u}_k^n\|_2^2} < \varepsilon$$

where X_{ij}^{τ} denotes the location data of the j^{th} size of the i^{th} individual, j=1,2,3,…,d, R_2 denotes the alerted value, ST is a pre-defined constant representing the security value, Q is a randomly generated number whose value follows the standard distribution, L is an ith-ordered-dimensional matrix, and $\alpha \in (0,1)$ is an arbitrary number.

$$X_{ij}^{\tau+1} = \begin{cases} Q * exp\left[\frac{X_{wj}^{\tau}-X_{ij}^{\tau}}{i^2}\right], & i > \frac{N}{2} \\ X_{bj}^{\tau+1} + \left|X_{ij}^{\tau} - X_{bj}^{\tau+1}\right| * A^{+} * L, i \le \frac{N}{2} \end{cases}$$

$X_{ij}^{\tau+1}$ denotes the poor individual location of the individual of the population in the jth size at τ iterations, A is the first-order d^{th}-dimension matrix with components 1 or *-1*, and $A^{+} = A^{\tau max}(AA^{\tau})^{-1}$.

To prevent the model from dropping into the local best, part of the individual of the population should be placed under the vigilance mechanism.

$$X_{ij}^{\tau+1} = \begin{cases} X_{ij}^{\tau} * \sigma\left[X_{ij}^{\tau} - X_{gj}^{\tau}\right], & f_i \neq f_g \\ X_{ij}^{\tau} + \mu * \left[\frac{X_{ij}^{\tau}-X_{\omega j}^{\tau}}{|f_i-f_\omega|+\delta}\right], & otherwise \end{cases}$$

where X_{gj}^{τ} is the global best individual location of the individual of the population at iterations, is the step controller parameter that randomly generates numbers following a standard distribution, f_i is the population's fitness value, f_ω is the best and poor fitness values between the individuals of the population, $\mu \in (0,1)$ is a set arbitrary number, and δ is a parameter set to prevent the denominator from becoming zero.

In the SSA model, the fitness function (FF) applied is expected to achieve a balance among the chosen feature counts in each solution (minimum) and the classifier precision (maximum) obtained using these chosen

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|}$$

where γ_R *(D)* is the classifier rate of error of a presumed classifier, $|R|$ is the chosen subset cardinality, $|C|$ is the total feature counts, and are dual parameters that correspond to a position of classifier excellence and subset length.

3.3 Conv-BiGRU-AA-Based Classification Method

The hybrid Conv-BiGRU-AA technique is used for attack classification [36]. It is capable of capturing spatial and temporal features in sequential data. Unlike conventional models, convolutional layers efficiently extract local patterns, while BiGRU processes the context from past and future time steps, improving sequence understanding. The attention mechanism (AAM) enhances performance by focusing on the most relevant features, resulting in better discrimination and interpretability. This hybrid approach provides higher accuracy and robustness than standalone CNN or RNN models, making it ideal for complex classification tasks.

A 1D-CNN is an NN structure that performs better in removing characteristics from shorter fixed-length inputs through a complete dataset. It is typically applied to handle one-dimensional textual data or time series data. Initially, convolutional processes are implemented to remove the main characteristics inside the sequence; then, a convolution filter (or kernel) is applied. Given W and the input sequence X, the output ξ is calculated in every position as follows:

$$\xi[j] = (X \cdot W)[j] = f(\sum_{k=0}^{K=1} X\,[j \times T_s + k] \cdot W[k] + b_{cnn})$$

where $\xi[j]$ is the component of the sequence of output originating from the convolutional process. In Eq. (5), $X[j+k]$ is $j+kth$ the component of the sequence of input, j is the present location of the convolutional process, k is the offset and multiplied element by element and added to give the jth component of the sequence of output, T_s is the time step, $W[k]$ refers to k convolution kernel's weight, k is the convolution kernel size, b_{cnn} is the term of bias, and f is the function of the activation that presents nonlinear properties. The standard activation functions include ReLU and parametric ReLU, among others.

$$x[j] = \max(X[j \times T_s : (j+1) \times T_s])$$

where $x[j]$ stands for the initial jth component. In Eq. (6), $X\,[j \times T_s : (j+1) \times T_s]$ specifies that a sub-sequence is designated in a sequence of input.

LSTM and GRU preserve significant historical characteristics by using a 'gate' structure. A combination of input and forgetting gates in LSTM is compressed into the update gate, including an update gate z and a reset r. x_t signifies the present input moment of the GRU component, $h_{(t-1)}$ refers to the preceding moment state, r_t is the reset gate that originates depending on Eq. (7) and is applied to establish the dependence grade of candidate state $\tilde{h}_t$ on $h_{(t-1)}$, z_t is the gate of update that can arise from Eq. (8), and h_t is the value of the output candidate after the gate of the reset process. h_t is attained by relating Eqs. (7)–(10).

$$r_t = sigmoid(U_r h_{t-1} + W_r x_t + b_r)$$

$$z_t = sigmoid(U_z h_{t-1} + W_z x_t + b_z)$$

$$h_t = \tanh(U_c(r_t h_{t-1}) + W_c x_t + b_c)$$

$$h_t = z_t h_{t-1} + (1 - z_t)\tilde{h}_t$$

In Eq. (7), U_r and W_r are the weighted matrices of the gate of reset, and b_r is the bias gate of reset. In Eq. (8), U_z and W_z are the weighted matrices of the update gate, and b_z is the bias of the update gate. In Eq. (9), b_c is the candidate hidden state's (HL) bias, and U_c and W_c are the weighted matrices of candidate HL.

Although the unidirectional GRU architecture can gather historical data from a particular point during his time, it cannot gather the before- and after-associated data. The backward, forward and particular computing operations are expressed in Eqs. (11)–(13), respectively.

$$\vec{h}_t = GRU_f(x_t, \vec{h}_{t-1})$$

$$\overleftarrow{h}_t = GRU_b(x_t, \overleftarrow{h}_{t-1})$$

$$h_t = \vec{h}_t \oplus \overleftarrow{h}_t$$

where $\vec{h}_t$ and $\vec{h}_t$ are the backward and forward GRU passes, respectively, GRU_f and GRU_b are the tandem combinations of forward and backward GRU functions, respectively, and $\oplus$ denotes the vector splice process.

The initial use of the AAM was for sentence translation, and recently, its use extended to the image processing field. It allows the method to adaptably assign changing weights to different portions inside the sequence of input, thus enabling a concentrated study of the essential components in the sequence data processing and the implementation of the converted characteristics by the sigmoid function to illustrate the similarity connection among the dual features that may successfully address nonlinear relationships. The equation for AA is expressed as follows:

$$y_i = DecoderOutput(s_t, c_t)$$

where y_i signifies the output at time step i. In Eq. (14), s_t is the HL at time step t, and y_i is the result. In Eq. (15), c_t is obtained by decoding at time step t.

$$c_t = \sum_{i=1}^{T} a_{t,i}\, h_i$$

The weights are computed as follows:

$$a_{ti} = \frac{\exp(e_{t,i})}{\Sigma_{j=1}^{T} \exp(e_{t,j})}$$

Here, the attentional weight is obtained from the score of attention standardised by Softmax and embodies the attention weight of the decoder from the to the time step. The score of attention is measured as follows:

$$e_{t,i} = v_a^T \tanh(W_a h_i + U_a s_{t-1})$$

In AA, the score of attention is computed through the linear transformation of the decoders and the HL encoder. In Eq. (17), is the score attention from decoding at the time step to the time step is the learned weighted vector, and and are the learned parameter matrices. Fig. 3 presents the framework of the Conv-BiGRU-AA method.

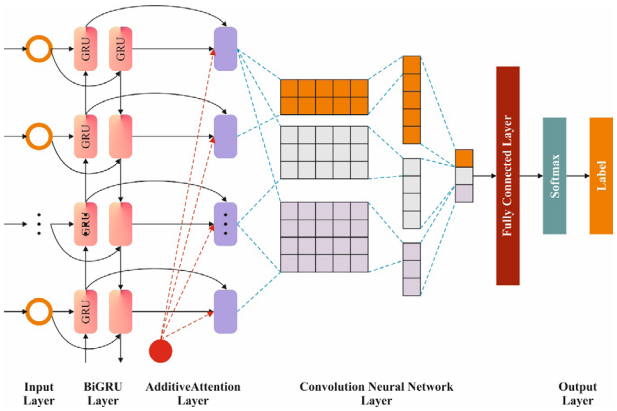

Fig. 3. Framework of the Conv-BiGRU-AA system

3.4 FAOA-Based Hyperparameter Tuning Model

Parameter fine-tuning is executed by utilising the FAOA to enhance the classifier efficiency of the Conv-BiGRU-AA classifier [37]. This model is selected for its simplicity, fast convergence and strong global search capability. It effectively explores the hyperparameter space by replicating the food-seeking behaviour of fruit flies, mitigating computational costs and avoiding the local minima. Furthermore, FAOA requires fewer iterations to find optimal solutions, resulting in enhanced model performance and faster training times than other metaheuristic algorithms.

The FAOA model, which is stimulated by the life of farmer ants, is described as follows: At the start of the model, the ant counts (n), which are in charge of finding nutrition and are responsible for the mushrooms (), are established. The ants should process every mushroom. The ant counts are higher than or equivalent to the mushroom counts. Occasionally, the mushroom counts within the nests may be equivalent to the ant counts. Near the nest, the ants have additional nutrition, and all mushrooms are allocated to the ants to deliver their preferred food. The growth rate of the mushrooms relies on the form of the food they nourish. This dependence is uncertain at the start of the model. Changing this feature may limit the exploration behaviour of the method, which is fine-tuned based on all problems.

As the growth rate of mushrooms relies on the appropriate food they nourish, it corresponds to the form of bacteria made by the assumed ant. Therefore, this feature can be more efficient in growing the mushrooms. The pest factor (PF) is measured as a parameter that uses negative effects on mushroom growth, but its effect decreases when the correct bacteria for the mushroom are selected. The efficiency of PF is further established by the coefficient C_3.

$$W_k = \sum_{for\ all\ ants\ and\ mushrooms} W_0 + (C_1 \times f_m + C_2 \times B_i) \times W_0 - C_3 \times PP \times W_0$$

where W_0 is the mushroom's first weight; C_1, C_2 and C_3 are the learning parameters; f_m is the food quality value for diet m, and B_j is the ant bacteria i. PF is also established by Eq. (19).

$$PF = Is^{\alpha}$$

where I represent the pest's negative influence value, s denotes pest capacity, and α is the pest's spreading parameter on the mushrooms, which is fine-tuned based on the issue.

PF plays an integral part in representing the negative effects that compromise the optimiser procedure. It presents an accurate problem, avoids overfitting to best states and creates a FAOA that is efficient for composite, *NP*-hard difficulties with natural tradeoffs. The bacteria's influence on the growth of mushrooms is further measured by Eq. (20), where e is the positive efficacy parameter, and t denotes the bacteria lifetime. β is a changeable parameter that adjusts the bacterial influence, approximating a dial to fine-tune its power according to the problem's requirements.

$$B_i = e \times v \times t^{\beta}$$

Various arbitrary solutions are measured to improve the model's exploration ability. In doing so, a greater selection of solutions can result from discovering improved solutions and preventing dropping into local bests. In such a case, a few ants lose their way and immigrate to another nest. This problem is expressed by Eq. (21).

$$p_j^{ik} = \frac{SP_k \times SP_j \times W_j}{(1-SP_k) \times \Sigma_{M=1}^{K} W_M} \; where\; 0 < SP_j \; and \; SP_k \leq 1$$

Eq. (22) illustrates the global stages in discovering the solution. The 1-*FP* ant percentage behaves arbitrarily and carries the ants to another nest to handle the mushrooms. These ant counts or n_L should be described while in progress, which could differ based on the problem.

$$W_L = (1 - FP) * p_j^{ik} * \sum_{I=1} [W_0 + (r_1 \times f_m + r_2 \times B_i) \times W_0 - r_3 \times PF \times W_0] + FP * \sum_{L+1}^{k} W_k$$

W_L comprises dual portions: The initial portion is associated with the performance of L ants, while the nest portion is associated with the leftover ants.

In this context, the coefficients r_1,r_2, and r_3, which are arbitrary numbers among (0,1), substitute for the coefficients C_1, C_2 and C_3, respectively. In this case, the model behaviour is more arbitrary, and a global search is carried out. The mushroom weight formed in all nests *k* is measured. M,B,W and F denote the mushrooms, bacteria, weight and food, respectively. Eq. (23) is expressed as follows:

$$W = \max\{(\sum_{i=1}^{K} w_k), (\sum_{i=1}^{L} w_L + \sum_{L+1}^{K} w_k)\}$$

W denotes the complete weight of the mushrooms. In this context, similar local and global processes must be performed. In the FAOA, fitness selection is an extensive factor that manipulates performance. The hyperparameter range process comprises a solution-encoding model for evaluating the proficiency of the candidate solution. To design the FF, the FAOA imitates precision as the foremost criterion, which is expressed as follows:

$$Fitness = \max(P)$$

$$P = \frac{TP}{TP + FP}$$

where FP and TP are the false and true positive rates, respectively.

4. Results Analysis and Discussion

The performance assessment of the BCAD-DRHDLM is examined using the Edge-IIoT [38] and ToN-IoT databases [39]. The Edge-IIoT database holds 36,000 records under 12 kinds of events, as shown in Table 1. It has 63 features, but only 45 features are selected.

Table 1. Details of the Edge-IIoT database

"Edge-IIoT Database"	
"Type of Event"	**"Data Record"**
"Normal"	3,000
"DDoS-UDP"	3,000
"DDoS-ICMP"	3,000
"SQL injection"	3,000
"DDoS-TCP"	3,000
"Password"	3,000
"DDoS-HTTP"	3,000
"Uploading"	3,000
"Backdoor"	3,000
"XSS"	3,000
"Ransomware"	3,000
"Fingerprinting"	3,000
Total Record	**36,000**

Fig. 4 illustrates the classifier outcomes of the BCAD-DRHDLM in the Edge-IIoT database. Figs. 4a–4b show the confusion matrix by identifying each class based on 70%

TRAPHA and 30% TESPHA. Fig. 4c presents the PR inspection, with higher performance shown through each class label. Fig. 4d shows the outcome of the ROC and expert solutions through higher ROC values for diverse classes.

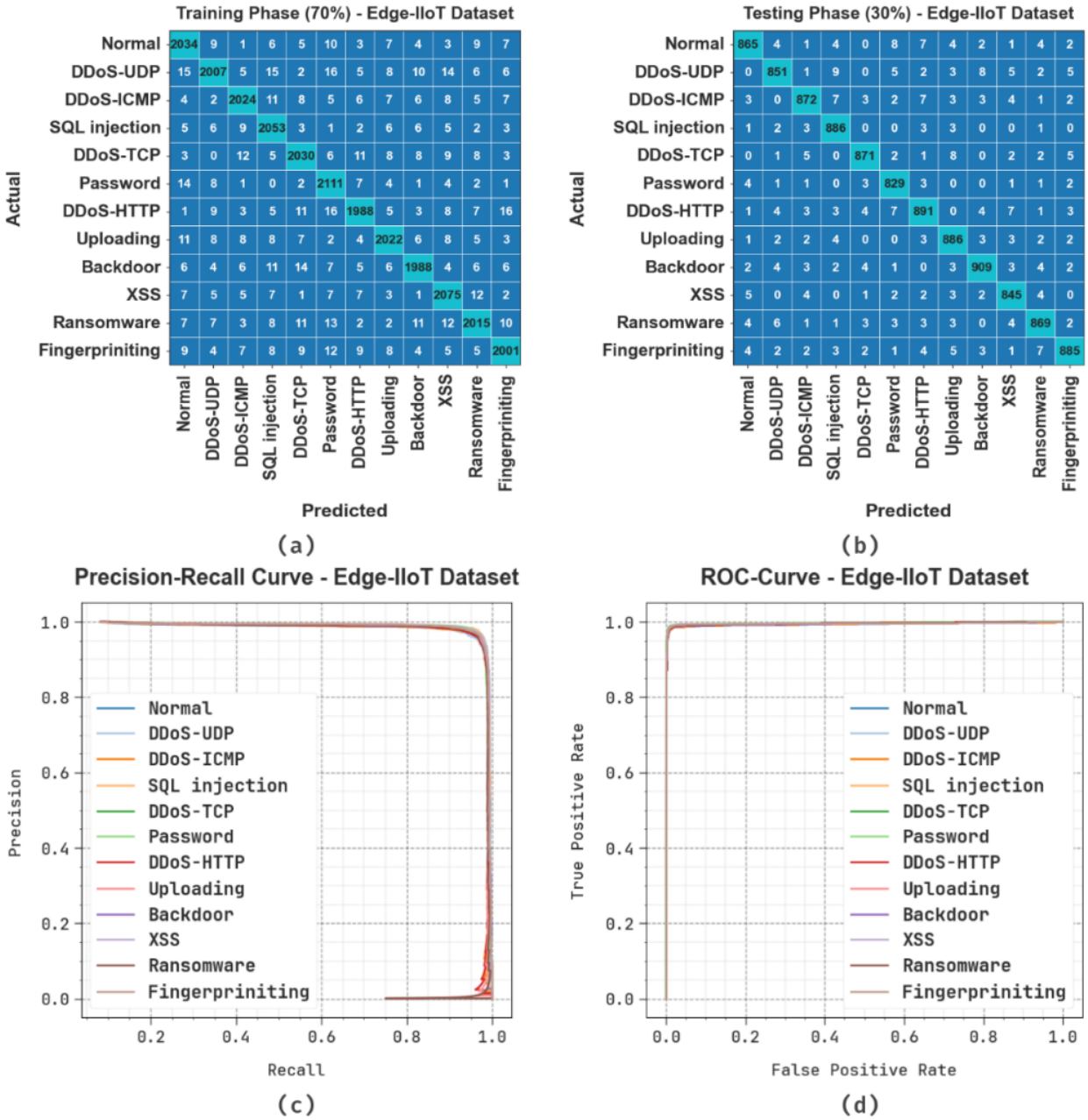

Fig. 4. Edge-IIoT database: (a–b) 70% TRAPHA and 30% TESPHA and (c–d) PR and ROC curves

Table 2 and Fig. 5 depict the attack detection of the BCAD-DRHDLM in the Edge-IIoT database. Based on 70% TRAPHA, the proposed BCAD-DRHDLM reaches a typical of 99.44%, of 96.63%, of 96.61%, of 96.62% and of 98.15%. Based on 30% TESPHA, the proposed BCAD-DRHDLM achieves an average of 99.47%, of 96.84%, of 96.85%, of 96.84% and of 98.28%.

Table 2. Attack detection of the BCAD-DRHDLM in the Edge-IIoT database

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$	AUC_{Score}
TRAPHA (70%)					
Normal	99.42	96.12	96.95	96.54	98.30
DDoS-UDP	99.35	97.00	95.16	96.07	97.45
DDoS-ICMP	99.49	97.12	96.70	96.91	98.22
SQL injection	99.48	96.07	97.72	96.89	98.68
DDoS-TCP	99.42	96.53	96.53	96.53	98.11
Password	99.45	95.69	97.96	96.81	98.77
DDoS-HTTP	99.42	97.02	95.95	96.48	97.84
Uploading	99.47	96.93	96.65	96.79	98.19
Backdoor	99.46	97.07	96.36	96.72	98.05
XSS	99.46	96.29	97.33	96.80	98.49
Ransomware	99.39	96.78	95.91	96.34	97.81
Fingerprinting	99.43	96.90	96.16	96.53	97.94
Average	**99.44**	**96.63**	**96.61**	**96.62**	**98.15**
TESPHA (30%)					
Normal	99.43	97.19	95.90	96.54	97.82
DDoS-UDP	99.39	97.04	95.51	96.27	97.62
DDoS-ICMP	99.44	97.10	96.14	96.62	97.94
SQL injection	99.57	96.41	98.55	97.47	99.11
DDoS-TCP	99.57	97.76	97.10	97.43	98.45
Password	99.56	96.40	98.11	97.24	98.90
DDoS-HTTP	99.33	96.22	96.01	96.12	97.83
Uploading	99.47	96.20	97.58	96.88	98.61
Backdoor	99.51	97.32	97.01	97.17	98.38
XSS	99.50	96.46	97.35	96.90	98.52
Ransomware	99.45	96.77	96.66	96.72	98.19
Fingerprinting	99.45	97.25	96.30	96.77	98.02
Average	99.47	96.84	96.85	96.84	98.28

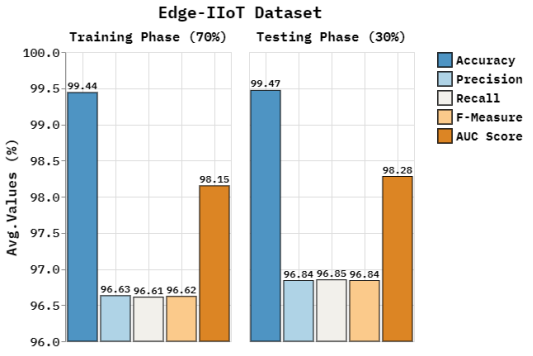

Fig. 5. Average of the BCAD-DRHDLM in the Edge-IIoT database

Fig. 6 reveals the training (TRAN) accu_y and validation (VALN) $accu_y$ outcomes of the BCAD-DRHDLM based on the Edge-IIoT database. For 0–25 epochs, the values of $accu_y$ are computed. The figure highlights that either $accu_y$ value expresses cumulative tendencies, indicating the proficiency of the BCAD-DRHDLM over the maximum outcome through multiple iterations. Likewise, both $accu_y$ values are closer in the epochs, specifying lowered overfitting and an increased outcome of the BCAD-DRHDLM and assuring balanced computation in undetected instances.

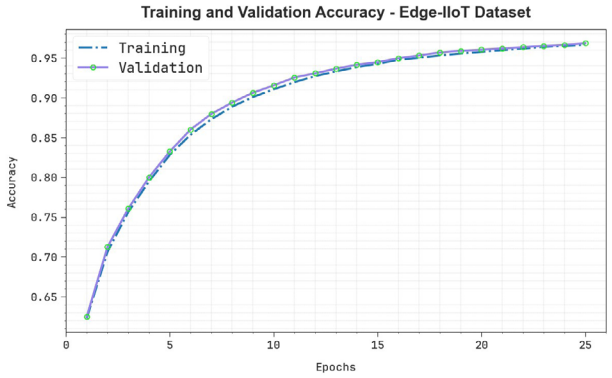

Fig. 6. curve of the BCAD-DRHDLM in the Edge-IIoT database

Fig. 7 presents the TRAN loss (TRANLOSS) and VALN loss (VALNLOSS) graph of the BCAD-DRHDLM based on the Edge-IIoT database. The values are measured over 0–25 epochs. Either value represents falling tendencies, demonstrating the ability of the BCAD-DRHDLM to equalise equilibrium. The progressive reduction in loss values and security is the superior result of the BCAD-DRHDLM, and the computation results can be adjusted afterward.

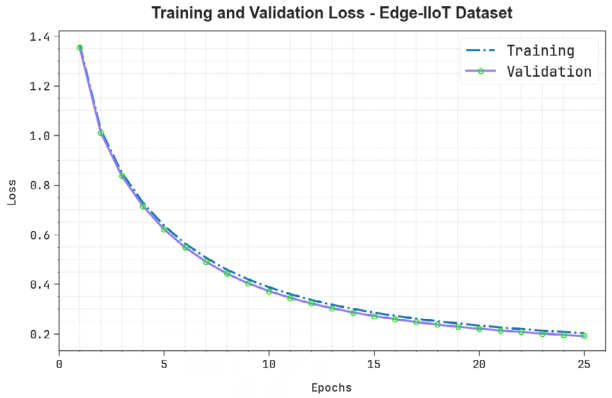

Fig. 7. Loss curve of the BCAD-DRHDLM in the Edge-IIoT database

A comparison analysis of the BCAD-DRHDLM with the existing approaches in the Edge-IIoT database is presented in Table 3 and Fig. 8 [19–20, 40–43]. The results show that the LSTM, FL, FedMLDL-Bayesian HPO, FedMLSL-RIME, random forest (RF), Conv1d, Transformer, DPPML, GAN and HetGNN models attain poor performance. Conversely, the proposed BCAD-DRHDLM indicates higher outcomes, with increased $accu_y$, $prec_{n,\,recal}$ and $F_{Measure}$ of 99.47%, 96.84%, 96.85% and 96.84%, respectively.

Table 3. Comparison analysis of the BCAD-DRHDLM with recent techniques in the Edge-IIoT database [19–20, 40–43]

Edge-IIoT Database				
Technique	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$
LSTM	91.33	90.03	90.97	90.30
FL	90.66	94.89	95.86	90.11
FedMLDL-Bayesian HPO	92.01	89.12	92.68	94.74
FedMLSL-RIME	90.18	91.52	90.20	94.87
RF	91.80	91.21	94.38	93.68
Conv1d Model	92.80	96.08	92.02	91.94
Transformer	97.52	92.11	91.71	89.98
DPPML	91.36	95.59	96.03	90.81
GAN	92.56	89.84	93.24	95.53
HetGNN	90.79	92.27	90.77	95.48
BCAD-DRHDLM	99.47	96.84	96.85	96.84

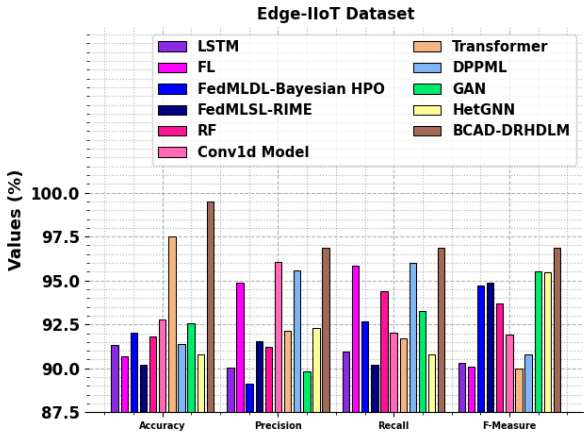

Fig. 8. Comparison analysis of the BCAD-DRHDLM with existing methods in the Edge-IIoT database

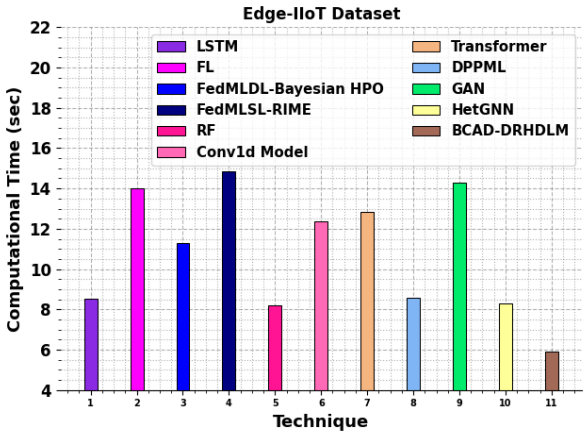

Fig. 9. CT analysis of the BCAD-DRHDLM compared with recent techniques in the Edge-IIoT database

Table 4 and Fig. 9 illustrate the computational time (CT) analysis of the BCAD-DRHDLM compared with recent models. The comparative analysis of CT shows that the BCAD-DRHDLM achieves the lowest CT of 5.93 s, indicating superior proficiency for rapid inference in edge-based IIoT scenarios. Techniques such as RF and HetGNN also perform well, with CT values of 8.21 s and 8.30 s, respectively, followed by LSTM at 8.52 s and DPPML at 8.57 s. By contrast, methods such as FedMLSL-RIME and GAN exhibit higher CT values of 14.86 s and 14.29 s, respectively, indicating slower processing. FL records a CT value of 14.02 s, while Transformer and Conv1d Model register CT values of 12.84 s and 12.36 s, respectively. The FedMLDL-Bayesian HPO technique achieves a moderate CT value of 11.31 s. The performance of the BCAD-DRHDLM with faster CT enhances its applicability to real-time IIoT environments, with an accuracy of 99.03%.

Table 4. CT analysis of the BCAD-DRHDLM compared with recent techniques in the Edge-IIoT database

Edge-IIoT Database	
Technique	**CT (s)**
LSTM	8.52
FL	14.02
FedMLDL-Bayesian HPO	11.31
FedMLSL-RIME	14.86
RF	8.21
Conv1d Model	12.36
Transformer	12.84
DPPML	8.57
GAN	14.29
HetGNN	8.30
BCAD-DRHDLM	5.93

The proposed BCAD-DRHDLM is also examined in the ToN-IoT database, which consists of 119,957 samples in nine classes. Table 5 presents the complete details of this database. This database has 42 features in total, but only 32 are selected.

Table 5. Details of the ToN-IoT database

"ToN-IoT Database"	
"Class"	**"No. of Samples"**
"Normal"	"78,369"
"MiTM"	"336"
"DoS"	"5,440"
"DDoS"	"5,987"
"Password"	"6,016"
"Injection"	"5,867"
"XSS"	"5,951"
"Ransomware"	"5,976"
"Backdoor"	"6,015"
"Total Samples"	**"119,957"**

Fig. 10 presents the classifier outcomes of the BCAD-DRHDLM in the ToN-IoT database. Figs. 10a–10b show the confusion matrix by precisely categorising each class based on 70% TRAPHA and 30% TESPHA. Fig. 10c shows the PR outcomes, indicating higher performance over all classes. Fig. 10d illustrates the outcomes for the ROC, indicating skilful solutions using greater values of ROC for discrete classes.

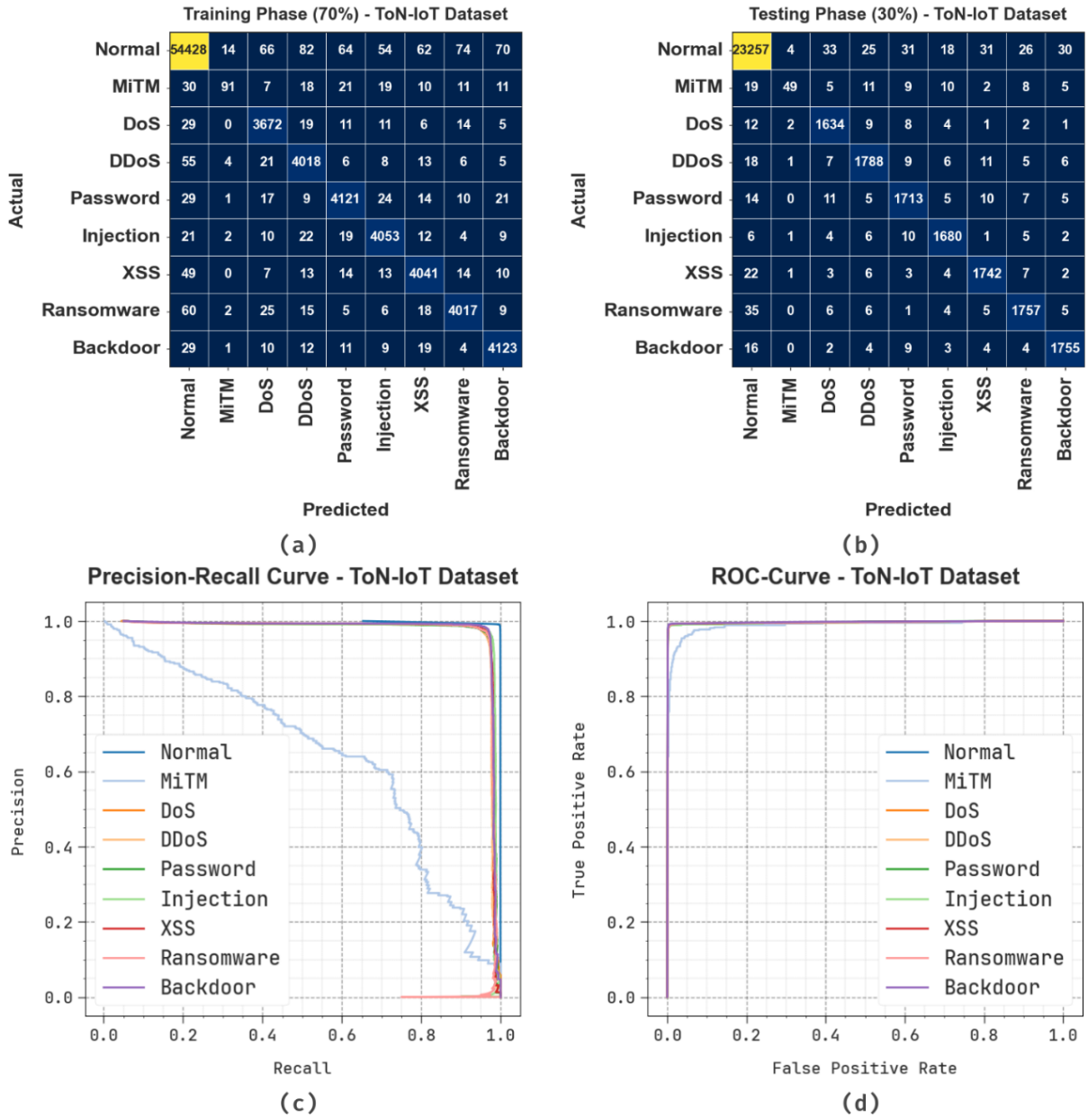

Fig. 10. ToN-IoT database (a–b) 70% TRAPHA and 30% TESPHA and (c–d) PR and ROC curves

Table 6 and Fig. 11 present the attack detection of the BCAD-DRHDLM in the ToN-IoT database. Based on 70% TRAPHA, the proposed BCAD-DRHDLM obtains a typical $accu_y$ of 99.63%, $prec_n$ of 94.73%, $reca_l$ of 91.29%, $F_{Measure}$ of 92.37% and AUC_{Score} of 95.51%. Based on 30% TESPHA, the proposed BCAD-DRHDLM reaches a typical $accu_y$ of 99.62%, $prec_n$ of 95.34%, $reca_l$ of 91.25%, $F_{Measure}$ of 92.48% and AUC_{Score} of 95.49%.

Table 6. Attack detection of the BCAD-DRHDLM in the ToN-IoT database

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$	AUC_{Score}
TRAPHA (70%)					
Normal	99.06	99.45	99.11	99.28	99.04
MiTM	99.82	79.13	41.74	54.65	70.86
DoS	99.69	95.75	97.48	96.61	98.64
DDoS	99.63	95.48	97.15	96.31	98.45
Password	99.67	96.47	97.06	96.76	98.43
Injection	99.71	96.57	97.62	97.09	98.72
XSS	99.67	96.33	97.12	96.72	98.46
Ransomware	99.67	96.70	96.63	96.67	98.23
Backdoor	99.72	96.72	97.75	97.23	98.79
Average	**99.63**	**94.73**	**91.29**	**92.37**	**95.51**
TESPHA (30%)					
Normal	99.06	99.39	99.16	99.27	99.01
MiTM	99.78	84.48	41.53	55.68	70.75
DoS	99.69	95.84	97.67	96.74	98.73
DDoS	99.62	96.13	96.60	96.36	98.19
Password	99.62	95.54	96.78	96.15	98.27
Injection	99.75	96.89	97.96	97.42	98.90
XSS	99.69	96.40	97.32	96.86	98.56
Ransomware	99.65	96.49	96.59	96.54	98.20
Backdoor	99.73	96.91	97.66	97.28	98.75
Average	**99.62**	**95.34**	**91.25**	**92.48**	**95.49**

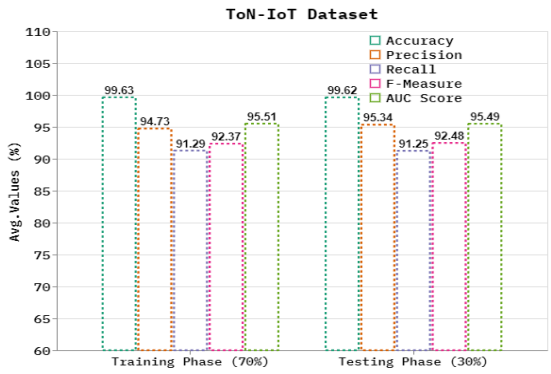

Fig. 11. Average outcomes of the BCAD-DRHDLM in the ToN-IoT database

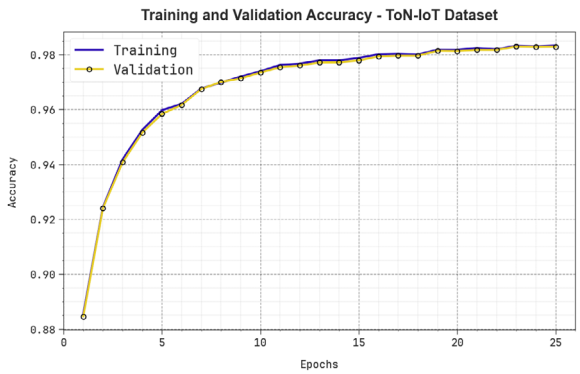

Fig. 12. curve of the BCAD-DRHDLM in the ToN-IoT database

Fig. 12 shows the TRAN $accu_y$ and VALN $accu_y$ performances of the BCAD-DRHDLM in the ToN-IoT database. The values of $accu_y$ are measured over 0–25 epochs. The figure reveals that either $accu_y$ value presents increasing tendencies, indicating the ability of the BCAD-DRHDLM to obtain enhanced performance in various repetitions. Moreover, both $accu_y$ values run closer across the epochs, indicating less overfitting and the improved outcome of the BCAD-DRHDLM and guaranteeing reliable calculation in hidden samples.

Fig. 13 exhibits the TRANLOSS and VALNLOSS graph of the BCAD-DRHDLM in the ToN-IoT database. The loss values are measured over 0–25 epochs. Either value signifies declining tendencies, indicating the ability of the proposed technique to be consistent with balance. The subsequent dilution in loss values ensures the increased outcome of the BCAD-DRHDLM and gradually adjusts the calculation outcomes.

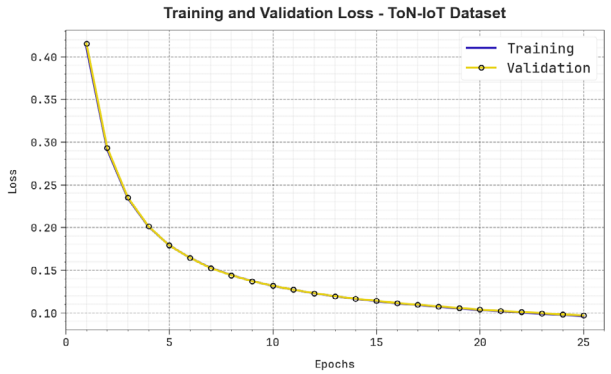

Fig. 13. Loss curve of the BCAD-DRHDLM in the ToN-IoT database

A comparison analysis of the BCAD-DRHDLM with recent models in the ToN-IoT database is shown in Table 7 and Fig. 14 [22–23, 40–43]. The analysis implies that the BCAD-DRHDLM achieves an increased outcome, with higher , and values of 99.63%, 94.73%, 91.29% and 92.37%, respectively. Conversely, the existing approaches, such as Hybrid RNN+ANFIS, Deep CNN+BiLSTM, CapsNets+RNN, decision tree (DT), LuNET, Multi-stage, Auto Encoders, DCGAN, DP-MLP and PCA, reach minimum results.

Table 7. Comparison analysis of the BCAD-DRHDLM with recent methods in the ToN-IoT database [22–23, 40–43]

ToN-IoT Database				
Technique	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$
Hybrid RNN+ANFIS	91.92	86.38	85.01	90.11
Deep CNN+BiLSTM	92.20	87.38	86.79	85.01
CapsNets+RNN	97.03	89.63	85.28	88.11
DT	93.53	86.83	90.49	87.96
LuNET	95.69	88.04	87.54	90.62
Multi-stage	98.92	93.66	85.00	89.56
Auto Encoders	96.09	91.91	87.92	86.53
DCGAN	92.70	87.18	85.79	90.80
DP-MLP	92.94	88.04	87.44	85.59
PCA	97.72	90.30	85.97	88.77
BCAD-DRHDLM	99.63	94.73	91.29	92.37

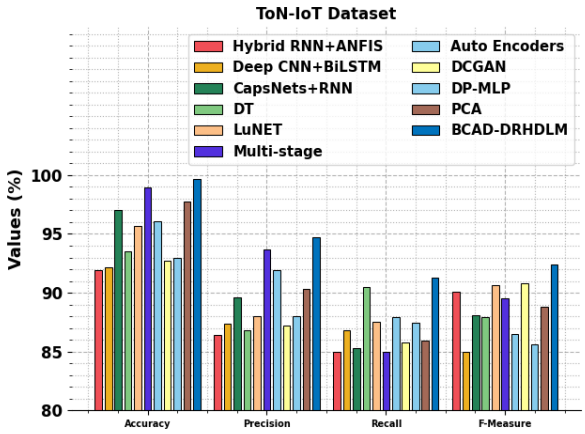

Fig. 14. Comparison analysis of the BCAD-DRHDLM technique with recent methods in the ToN-IoT database

Table 8 and Fig. 15 show the CT estimation of the BCAD-DRHDLM compared with recent models in the ToN-IoT database. The CT analysis on the ToN-IoT database reveals that the Hybrid RNN plus ANFIS technique attains the fastest CT of 7.42 s, followed by DT with 10.65 s and PCA with 12.79 s, indicating their suitability in time-sensitive scenarios. Methods such as DCGAN and CapsNets plus RNN achieve moderate CT values of 13.71 s and 14.02 s, respectively. Deep CNN plus BiLSTM and DP-MLP have similar performances, with 15.23 s and 15.22 s, respectively. The BCAD-DRHDLM records a CT value of 17.59 s, which remains within an acceptable range for complex classification tasks while achieving 99.03% accuracy. Comparatively, the Multi-stage, Auto Encoders and LuNET models show higher CT values of 23.20 s, 22.91 s and 23.31 s, respectively, highlighting the trade-off between accuracy and processing speed.

Table 8. CT assessment of the BCAD-DRHDLM compared with recent models in the ToN-IoT database

ToN-IoT Database	
Technique	**CT (sec)**
Hybrid RNN+ANFIS	7.42
Deep CNN+BiLSTM	15.23
CapsNets+RNN	14.02
DT	10.65
LuNET	23.31
Multi-stage	23.20
Auto Encoders	22.91
DCGAN	13.71
DP-MLP	15.22
PCA	12.79
BCAD-DRHDLM	17.59

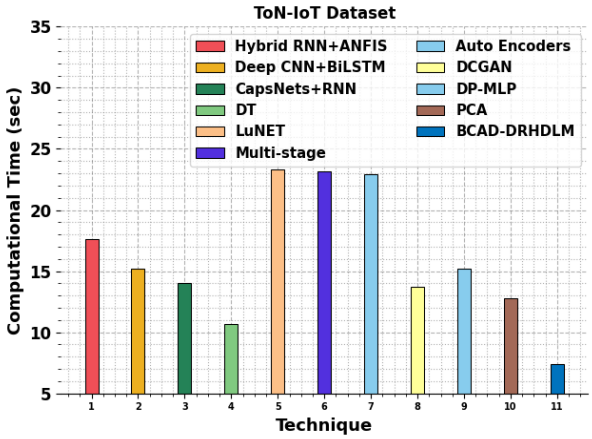

Fig. 15. CT assessment of the BCAD-DRHDLM compared with recent models in the ToN-IoT database

5. Conclusion

This study proposes the BCAD-DRHDLM for IoT environments. The BCAD-DRHDLM is effective in enhancing cybersecurity in IoT networks by developing robust threat detection mechanisms to mitigate evolving security risks. The Z-score method is used in the data pre-processing phase to measure and standardise the data for improved model performance. The SSA is used for the FS model to recognise and retain the related features from the input data. The hybrid Conv-BiGRU-AA method is used for attack classification. The parameter fine-tuning procedure is conducted using FAOA to increase the classification outcome of the Conv-BiGRU-AA classifier. The effectiveness of the BCAD-DRHDLM is verified by the Edge-IIoT and ToN-IoT datasets. The comparison analysis of the BCAD-DRHDLM shows better precision values of 99.47% and 99.63% over existing models in the two datasets. However, the BCAD-DRHDLM also has some limitations, such as restricted generalisability due to dataset-specific evaluations and limited testing under diverse network conditions. Its performance may degrade when applied to heterogeneous environments with varying data distributions. Scalability concerns also arise when the number of nodes or data volume increases, potentially affecting processing time. Real-time performance under adverse scenarios remains unexplored. Thus, future studies could extend the approach to cross-domain datasets, improve adaptability to dynamic network topologies and integrate lightweight modules to deploy ultra-low-power devices. Further experiments in real-world environments could also enhance its reliability and resilience.

6. Data Availability Statement

The data supporting this study's findings are openly available in the Kaggle repository at https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot and https://www.kaggle.com/datasets/dhoogla/cictoniot, reference numbers [38, 39].

7. References

T. R. Gadekallu, M. M K, S. K. S, N. Kumar, S. Hakak and S. Bhattacharya, "Blockchain-Based Attack Detection on Machine Learning Algorithms for IoT-Based e-Health Applications," in IEEE Internet of Things Magazine, vol. 4, no. 3, pp. 30-33, 2021, doi: 10.1109/IOTM.1021.2000160.

H. Vargas, C. Lozano-Garzon, G.A. Montoya and Y. Donoso, "Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach," Electronics, vol. 10, no. 21, p. 2662, 2021.

D. Saveetha and G. Maragatham, "Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning," Pattern Recognition Letters, vol. 153, pp. 24-28, 2022.

R. Kumar, P. Kumar, M. Aloqaily and A. Aljuhani, "Deep-Learning-Based Blockchain for Secure Zero Touch Networks," in IEEE Communications Magazine, vol. 61, no. 2, pp. 96-102, 2023, doi: 10.1109/MCOM.001.2200294.

M. A. Ferrag and L. Maglaras, "DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1285-1297, 2020, doi: 10.1109/TEM.2019.2922936.

N. Waheed, X. He, M. Ikram, M. Usman, S.S. Hashmi et al., "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," ACM computing surveys (csur), vol. 53, no. 6, pp. 1-37, 2020.

P. Kumar, R. Kumar, A. Kumar, A.A. Franklin, S. Garg et al., "Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network," IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2802-2813, 2022.

M. Sharma, S. Pant, D. Kumar Sharma, K. Datta Gupta, V. Vashishth et al., "Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 7, 2021, doi: https://doi.org/10.1002/ett.4137.

P. Kumar, R. Kumar, G.P. Gupta, R. Tripathi and G. Srivastava, "P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot," IEEE Transactions on industrial informatics, vol. 18, no. 9, pp. 6358-6367, 2022.

A. Maseleno, "Design of optimal machine learning-based cybersecurity intrusion detection systems," Journal of Cybersecurit., Information Management, vol. 2019, no. 1, pp. 32-43, 2019.

S. Selvarajan, A. Shankar, M. Uddin, A.S. Alqahtani, T. Al-Shehari et al., "A smart decentralized identifiable distributed ledger technology-based blockchain (DIDLT-BC) model for cloud-IoT security," Expert Systems, vol. 42, no. 1, 2025, doi: https://doi.org/10.1111/exsy.13544.

S.S. Sefati, R. Craciunescu, B. Arasteh, S. Halunga, O. Fratu et al., "Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT)," Smart Cities, vol. 7, no. 5, pp. 2802-2841, 2024.

R. B. Ponnuru, S. A. P. Kumar, M. Azab and G. R. Alavalapati, "BAAP-FIoT: Blockchain-Assisted Authentication Protocol for Fog-Enabled Internet of Things Environment," in IEEE Internet of Things Journal, vol. 12, no. 11, pp. 15681-15696, 2025, doi: 10.1109/JIOT.2025.3528746.

B. Alamri, I. Richardson and K. Crowley, "Cybersecuriy Risk Management and Evaluation Framework of Blockchain Identity Management Systems in HIoT: Experts Evaluation," in IEEE Access, vol. 12, pp. 144652-144683, 2024, doi: 10.1109/ACCESS.2024.3468379.

V. Kumar and S.K. Das, "Enhancing Security in IIoT: RFID Authentication Protocol for Edge Computing and Blockchain-enabled Supply Chain," Cyber Security and Applications,, p. 100087, 2025, doi: https://doi.org/10.1016/j.csa.2025.100087.

J. Makhahlela, G. M. Komba and S. P. Maswikaneng, "An Enhanced Cybersecurity Strategies for Internet of Things using Lightweight Blockchain-Based Secure Communication Protocol," 2024 5th International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering (ELECOM), Balaclava, Mauritius, 2024, pp. 1-4, doi: 10.1109/ELECOM63163.2024.10892173.

B.P. Pokharel, N. Kshetri, S.R. Sharma and S. Paudel, "blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems," Information, vol. 16, no. 2, p. 133, 2025.

S. Ismail, M. Nouman, D.W. Dawoud and H. Reza, "Towards a lightweight security framework using blockchain and machine learning," Blockchain: Research and Applications, vol. 5, no. 1, p. 100174, 2024.

K. Kuru and K. Kuru, "UMetaBE-DPPML: Urban Metaverse & Blockchain-Enabled Decentralised Privacy-Preserving Machine Learning Verification And Authentication With Metaverse Immersive Devices," Internet of Things and Cyber-Physical Systems., 2025, doi: https://doi.org/10.1016/j.iotcps.2025.02.001.

A. Rajasekar and V. Vetrian, "A Privacy-Preserving Graph Neural Network Framework with Attention Mechanism for Computational Offloading in the Internet of Vehicles," CMES-Computer Modeling in Engineering and Sciences, vol. 143, no. 1, pp. 225-254, 2025.

A.B. Kathole, K. Vhatkar, S.A. Ubale, V.V. Kimbahune, A. Dhumane et al., "Enhanced security mechanism in vehicular networks using ensemble machine learning to detect malicious activity in VANETs," J. Discrete Math. Sci. Cryptogr., vol. 27, no. 7, pp. 2005-2014, 2024.

A.G. Andrei, M.G. Constantin, M. Graziani, H. Müller and B. Ionescu, "Privacy preserving histopathological image augmentation with Conditional Generative Adversarial Networks," Pattern Recognition Letters, vol. 188, pp. 185-192, 2025.

L.K.G. Danquah, S.Y. Appiah, V.A. Mantey, I. Danlard and E.K. Akowuah, "Computationally Efficient Deep Federated Learning with Optimized Feature Selection for IoT Botnet Attack Detection," Intelligent Systems with Applications, vol. 25, p. 200462, 2025.

A.B. Kathole, K. Vhatkar, G. Dharmale, S. Chiwhane, V.V. Kimbahune et al., "A novel approach to IoT security for intrusion detection system using ensemble network and heuristic-assisted feature fusion," J. Discrete Math. Sci. Cryptogr., vol. 27, no. 7, pp. 2207-2217, 2024.

A. Nazir, J. He, N. Zhu, A. Wajahat, F. Ullah et al., "Empirical evaluation of ensemble learning and hybrid CNN-LSTM for IoT threat detection on heterogeneous datasets," The Journal of Supercomputing, vol. 81, no. 6, p. 775, 2025.

B. Kathole et al., "Secure Federated Cloud Storage Protection Strategy Using Hybrid Heuristic Attribute-Based Encryption With Permissioned Blockchain," in IEEE Access, vol. 12, pp. 117154-117169, 2024, doi: 10.1109/ACCESS.2024.3447829.

R. Loganathan and S. SelvakumaraSamy, "An efficient privacy-preserving authentication scheme for internet of vehicles based on blockchain technology with hybrid adaptive network," Peer-to-Peer Networking and Applications, vol. 18, no. 3, p. 99, 2025.

A. Nazir, J. He, N. Zhu, A. Wajahat, X. Ma et al., "Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets," Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 10, p. 101820, 2023.

N.S. Ganesh, V. Balasubramanian, D. Prasad and S.S. Velan, "Deep learning-based user authentication with hybrid encryption for secured blockchain-aided data storage and optimal task offloading in mobile edge computing," Wireless Networks, vol. 31, no. 3, pp. 2389-2417, 2025.

A. Nazir, J. He, N. Zhu, A. Wajahat, F. Ullah et al., "Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration," Journal of King Saud University-Computer and Information Sciences, vol. 36, no. 2, p. 101939, 2024.

B. Kadiyala, C. Vasamsetty, S. Boyapati, S.K. Alavilli, R.P. Nippatla et al., "Decentralized anomaly detection and data privacy preservation for IoT networks using blockchain and homomorphic encryption," Intelligent Data Analysis,, p. 1088467, 2025, doi: https://doi.org/10.1177/108846X251339365.

Nazir, J. He, N. Zhu, M.S. Anwar and M.S. Pathan, "Enhancing IoT security: a collaborative framework integrating federated learning, dense neural networks, and blockchain," Cluster Computing, vol. 27, no. 6, pp. 8367-8392, 2024.

O. Slama, W. Dhifallah, S. Zidi, J. Lloret, B. Alaya et al., "Blockchain-based privacy-preserving technology to secure shared data in vehicular communication," International Journal of Communication Networks and Distributed Systems, vol. 31, no. 3, pp. 346-371, 2025.

S. Anthoniraj, R. Mishra, S. Loonkar, T. Agarwal, G. Ahluwalia et al., "Design of Novel Cryptographic Model Using Zero-Knowledge Proof Structure for Cyber Security Applications," Journal of Cybersecurity & Information Management, vol. 14, no. 1, 2024.

S. Li, Q. Zhao, J. Liu, X. Zhang and J. Hou, "Noise Reduction of Steam Trap Based on SSA-VMD Improved Wavelet Threshold Function," Sensors, vol. 25, no. 5, p. 1573, 2025.

S. Liu, W. Lin, Y. Wang, D.Z. Yu, Y. Peng et al., "Convolutional neural network-based bidirectional gated recurrent unit–additive attention mechanism hybrid deep neural networks for short-term traffic flow prediction," Sustainability, vol. 16, no. 5, p. 1986, 2024.

A. Asghari, M. Zeinalabedinmalekmian, H. Azgomi, M. Alimoradi and S. Ghaziantafrishi, "Farmer Ants Optimization Algorithm: A Novel Metaheuristic for Solving Discrete Optimization Problems," Information, vol. 16, no. 3, p. 207, 2025.

https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot

https://www.kaggle.com/datasets/dhoogla/cictoniot

G. Logeswari, J. Deepika Roselind, K. Tamilarasi and V. Nivethitha, "A Comprehensive Approach to Intrusion Detection in IoT Environments Using Hybrid Feature Selection and Multi-Stage Classification Techniques," in IEEE Access, vol. 13, pp. 24970-24987, 2025, doi: 10.1109/ACCESS.2025.3532895.

Jitendra Chandnani, V. Agarwal, S. Chetan Kulkarni, A. Aren, D. G. B. Amali and K. Srinivasan, "A Physics-Based Hyper Parameter Optimized Federated Multi-Layered Deep Learning Model for Intrusion Detection in IoT Networks," in IEEE Access, vol. 13, pp. 21992-22010, 2025, doi: 10.1109/ACCESS.2025.3535952.

S. Hariharan, Y. Annie Jerusha, G. Suganeshwari, S. P. Syed Ibrahim, U. Tupakula and V. Varadharajan, "A Hybrid Deep Learning Model for Network Intrusion Detection System Using Seq2Seq and ConvLSTM-Subnets," in IEEE Access, vol. 13, pp. 30705-30721, 2025, doi: 10.1109/ACCESS.2025.3541399.

M. Rodríguez, D.P. Tobón and D. Múnera, "A framework for anomaly classification in Industrial Internet of Things systems," Internet of Things, vol. 29, p. 101446, 2025.