JOURNAL OF BASIC SCIENCE AND ENGINEERING

ADAPTIVE CONFIDENCE-BASED DECISION MAKING IN DEEP LEARNING FOR CYBER THREAT DETECTION AND MITIGATION IN IoT

[1]Thanuja Narasimhamurthy, [2]Gunavathi Hosahalli Swamy

[1]Assistant Professor, Department of Computer Science & Engineering,
Bangalore Institute of Technology, Bengaluru, Affiliated to Visvesvaraya Technological University,
Belagavi-590018, Karnataka, India

[2]Associate Professor, Dept. of Computer Science & Engineering,
Bangalore Institute of Technology, Bengaluru, Affiliated to Visvesvaraya Technological University,
Belagavi-590018, Karnataka, India

DOI: https://doie.org/10.10399/JBSE.2025517916

Article History: **Received: July 2025** **Revised: October 2025** **Accepted: December 2025**

***Abstract*: -** Cyber threat has been always a critical concern in Internet-of-Things (IoT) while the problem is still an open-ended. Review of existing literatures shows significant contribution of Artificial Intelligence (AI) in form of Machine Learning (ML) and Deep Learning (DL) approaches. Yet the shortcoming in security has not been mitigated. In the line of addressing this problem, this paper introduces an AI-driven intrusion detection system capable of identifying the nature of inbound traffic in IoT. The system uses Random Forest for selecting most potential feature while Convolution Neural Network is used on ranked feature for further optimization in prediction process based on empirically evaluated confidence score. Assessment with benchmarked UNSW-NB15 dataset shows proposed system with 94.25% accuracy, 91.96% of F1-Score, and 1.93s of response time which are significantly better in contrast to frequently adopted AI models in literatures to exhibit highly secure and computationally cost-effective solution in IoT.

***Keywords*:-** MIMO Internet-of-Things, Artificial Intelligence, Machine Learning, Deep Learning, Cyber threats.

1. Introduction

Internet-of-Things (IoT) can be stated as network of various forms of physical devices via internet with a purpose to acquire, share, and process/analyze the data without involving human. There are wider ranges of applications hosted by IoT viz. retail and logistic, smart cities, agriculture, industry, healthcare, smart homes [1]. In future, IoT will play a core role in edge computing integration, 6G, and AI mainly towards smart environment and automation. However, there are various ongoing challenges too viz. cost and infrastructure, energy consumption, data overload, interpretability, scalability, and privacy. Out of all, security is the primary concerns. It is not feasible to offer high-end security scheme in IoT devices which have low processing capabilities along with lower memory and power.

Hence, although there are various potential encryption and cryptographic-based scheme in IoT [2], they are actually not proven for their theoretical applicability in commercial or practical world of IoT. As IoT devices originates from different manufacturers and service providers, hence there is currently no solution towards standardizing them while this incompatible system continues increasing security gaps. Further, the large number of inter-connected IoT device also creates increasing entry points for adversaries while adopted web interfaces are highly insecure while there is a rising risk of data privacy too. In perspective of real-time deployment, the most effective security solution noted for IoT security are device authentication and access control, secure firmware updates, end-to-end encryption, anomaly-detection, and blockchain. In all these,

Artificial Intelligence (AI) has promising solution via Machine Learning (ML) and Deep Learning

(DL) models [3]. AI models is capable of learning different types of patterns associated with device communication or behaviour for confirming the presence of any anomalies. AI is also used for Intrusion Detection System (IDS) for detecting malware infection, spoofing, Distributed Denial-of-Service, etc using supervised and deep learning. ML model is capable of creating a behavioral fingerprint associated with each IoT equipment while DL model can analyze network traffic, system calls, binary code etc. This capability let the system to identify malware signatures and thereby a potential threat intelligence model is evolved that can predict and respond based on historical data and contributes to proactive measure of security.

However, it is not easy to directly implement AI on traffic data and sort out security problems in IoT. The biggest problem in adopting AI in IoT security is either sub-optimal or degraded data quality while it has time-consuming labelling process. Another critical problem in AI deployment is lack of generalization which means a successfully performing model doesn't offer any assurance or reliability for similar consistency when the environment is changed. ML models are usually preferred as DL models are quite resource consuming leading to slower outcome not suitable for detecting threats in real-time. Hence, it is essential to have a brief recap of the latest research models and methodologies emerged out in AI towards solving security issues in IoT.

The *related work* towards adoption of dominant part of AI i.e., ML and DL-based strategies evolved recently have been studied. Existing research work adopting Support Vector Machine (SVM) are noted to contribute towards high-dimensional spaces in IoT traffic features leading to good binary classification [4]-[6]. However, these approaches are noted to possess scalability issues. The next frequently adopted ML model is Random Forest (RF), which is noted to be used in both standalone and ensemble form [7]-[9]. With capability to handle non-linear relationship, RF-based models are suitable for multi-class problems; however, they are also noted to be resource intensive. Recent studies have been also recorded for using Gaussian Naïve Bayes (GNB) which is known for their faster training duration and effective for anomaly detection [10].

However, this approach exhibits degraded performance when exposed to complex features. Recent works have also been witnessed adopting k-Nearest Neighbors (KNN) for their simplified implementation [11]; however, these approaches cannot be applied for large-sized dataset. There has been an extensive work towards IoT security adopting Logistic Regression (LR) which is proven good not only for binary classification but also for better interpretability [12][13]; however, majority of IoT dataset are imbalanced and LR performs sub-optimally on such data while it also demands extensive feature engineering. From the perspective of DL models, many of recent studies have implemented Convolution Neural Network (CNN) which is known to exhibit its superior detection accuracy in majority of cases [14]-[19]; however, they are computationally expensive and demands voluminous labelled data which is unlikely the case of practical world traffic data. There are recent studies adopting Long Short-Term Memory (LSTM) which is proven effective towards anomaly detection in IoT [20]-[21]; majority of studies using LSTM is recorded with slower training and inference rate while they are also resource heavy which makes it questionable for their real-time IoT deployment. Finally, there are some good number of recent studies using Autoencoders (AE) that is claimed to performed better for unsupervised anomaly detection [22]-[25]; however, its shortcoming is limited interpretability. The identified *research problems* concluded after reviewing the existing models are as follows:

i) Majority of existing ML models eventually struggles with just differentiating normal to malicious network traffic leading to outliers,

ii) Majority of existing DL models are well figured with higher accuracy score; however, their

response time is evidently longer unsuitable for real-time IoT application,

iii) Existing research papers considers larger dataset but doesn't discuss much about optimal feature selection process, which not only increase computational cost but also potentially affect model performance, and

iv) Majority of existing system doesn't log systematically nor they analyze ambiguous event or emerging threat for future enhancement; thereby their adaptability is limited with increasing score of emerging threats.

The *aim* of proposed study is to introduce an efficient and robust AI-driven intrusion detection scheme that is capable of detecting and resisting potential cyberthreats with proactive and intelligent strategy powered by ML methodologies. The *value-added contribution* of the study are:

i) The proposed scheme presents a unique selection of potential features using RF where model enhancement is prioritized by choosing network traffic attributes with higher significance,

ii) The model architecture uses one-dimensional CNN which is capable of acquiring both spatial and temporal attributes from network traffic data in IoT,

iii) The scheme introduces a novel decision making system using empirical-driven confidence score for differentiating predictive outcomes based on multiple classes of decision, and

iv) The scheme also introduces a possibilities of middleware component which takes the input of ambiguous even for further research work to confirm its intention.

The paper's organization is portrayed as shown here. A brief introduction was given in the Section 1 in the previous paragraphs. The Section 2 presents a discussion of methods, while the result is discussed in Section 3, and the conclusion is presented in Section-4. This is followed by exhaustive set of reference papers & the author biographies.

2. Methodology Adopted

The prime aim of the adopted research methodology is towards developing a simplified, sustainable, robust, and cost-effective machine learning-based solution that can perform detection and prevention of lethal attacks in IoT environment. The method adopts learning mechanism using semi-supervised approach with an inclusion of various operational modules in it. The Fig. 1 highlights the adopted methodology which shows inbound traffic data is subjected to series of operation for obtaining the enriched data which upon subjected to training model yields a predictive outcome. The model forms a conditional logic to detect and classify three types of events where normal event is proceeded for cooperation (packet forwarding), attack event is subjected to be declined, while uncertain event is further forwarded to middleware to confirm its nature of behaviour. This section elaborates various operational modules involved in proposed architecture.

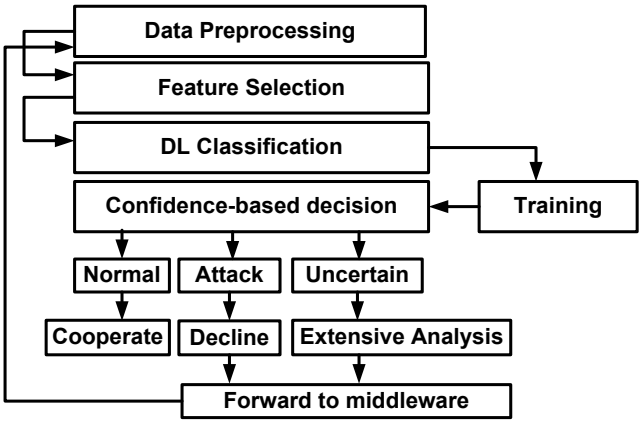


Fig.1. Proposed Architectural Model

2.1 Data Preprocessing

This is first operational block which performs transformation of the raw traffic data to generate highly structured and cleaner form of data appropriate for ML operation. It addresses the issues pertaining to original data e.g., inconsistent entries, categorical features, and missing values. Consider the inbound traffic data is empirically depicted as $D = \{x_i, y_i\}_{i=1}^{N}$ where feature vector associated with ith sample is represented as x_i while class label associated with sample is represented as y_i (attack category), where $y_i \in Y$ and $Y=\{1, 2, \ldots.(C-1)\}$, where C represents classes of attack. Further, d represented feature number and N represents sample number. The system also explores missing values x_{ij} and substitutes them with either zero or mode followed by encoding labels of categorical features (e.g. *proto*, *service*). Finally, normalization is carried out for all features adopting min-max scaling as follows,

$$x_{ij}^{norm} = \frac{x_{ij} - \min(x_j)}{\max(x_j) - \min(x_j)} \quad (1)$$

The above expression (1) mitigates the challenges associated with conventional detection system that doesn't efficiently permits to address data irregularities leading to outliers in classification results. This model enforces data consistency and integrity thereby facilitating stability towards learning process. The prime novelty of this operational block resides in its comprehensive normalization and encoding process that is dynamically applied to traffic vectors characterized with multiple sources of IoT attacks.

2.2 Feature Selection

This operational block performs identification of highly potential feature from massive archives of network traffic data. Majority of IoT dataset related to dynamic traffic consists of more potential and irrelevant data while this module filters only essential information that has higher probability of detecting anomalies in IoT environment. The proposed scheme performs feature selection using RF which performs computation of the feature as follows given by Eqn. (2) as

$$I_j = \sum_{t=1}^{T} \Delta G_j^{(t)} \quad (2)$$

In the above expression (2), the importance factor to be dependent on number of trees T and $\Delta G_j^{(t)}$ as minimization of Gini impurity considering x_j features at t tree. The system selects only the top k features which is characterized by maximum score of I_j thereby minimizing the dimensions from d to k where $k << d$. A significant amount of computational burden is also minimized by proposed feature

Vol. 22, No. 1, (2025)
ISSN: 1005-0930

selection module thereby providing minimal resource usage and faster training operations. The module filters out all irrelevant data and noise for better detection of malicious activities. Different from conventional schemes adopting fixed set of features or manually selection is carried out, proposed scheme offers novelty by adopting data-driven autonomous ranking mechanism. This scheme dynamically chooses features that have significant relevance to the patterns of specific form of attack in IoT ecosystem.

2.3 DL Classification

The prime aim of this module is to carry out intelligence operation in vulnerable IoT environment crafted to learn exclusive patterns associated with normal and anomalies-oriented behaviour. The proposed system considers CNN where the input vector x is mapped to probabilities of classes. The system considers X as reshaped input for convolution while $b^{(l)}$ and $W^{(l)}$ is considered as biases and weights associated with l^{th} convolution layer. Further, Rectified Linear Unit (ReLU) is considered as activation function denoted as $f(.)$ while one-dimensional convolution operator is denoted as *. Each standalone layer of convolution performs following computation $Z^{(l)} = f\left(a + b^{(i)}\right)$, where the variable α represents dot product of weight $W^{(l)}$ and reshaped input $X^{(l-1)}$ while $b^{(l)}$ represent bias. The next step is to generate the class probabilities using pooling layers and softmax layer as follows,

$$P\left(y = x_{|x}\right) = \frac{e^{z_c}}{\sum_{j=0}^{C-1} e^{z_j}} \qquad (3)$$

In the above-expression (3), the computation of class probabilities is carried out for $c \in Y$ while the variable z_c represents logit associated with c class i.e. the outcome before softmax layer. The model also uses cross-entropy as a loss function L while it is minimized by adopting Adam optimizer. This module assists in identification of priorly unseen and subtle actions of malicious event which is a significant enhancement in contrast to conventional signature-based methods that is permitted to detection only known patterns of adversaries. The key innovation of this module is associated with generalization of detection of multiple form of attacks without demanding any manual engineering process. The module also offers adaptive and scalable detection operation towards emerging cyberthreats.

2.4 Confidence-based Decision

This module participates in interpreting the outcome of prediction from prior module using classifier for determining the suitable remedial countermeasures to be undertaken. Instead of considering all the predictive outcomes equally, this module assesses the confidence level associated with each prediction. A target event is classified by this module depending on predefined cut-off score into multiple categories where prediction with higher confidence is considered normal event which lead to forward the data packet (or cooperate). In case of prediction score to be of minimal confidence score, the system confirms it as a threat while the data-packets are dropped, while prediction with moderate confidence score is treated as uncertain and forwarded to middleware for further analysis. This module is activated after the prediction of class probabilities in prior operational module. This module computes the confidence score towards decision making that is empirically represented as following,

$$\gamma_i = \max_{c} P(y) \qquad (4)$$

In the above expression (4), the argument y represents $(y = c|x_i)$ while the system defines a predicted class as $\hat{y}_i = arg(\gamma_i)$, where the system formally defines functional outcomes depending on score of $\gamma_i$as follows:

Vol. 22, No. 1, (2025)
ISSN: 1005-0930

i) *Cooperate*: The rule of cooperation is valid and applicable for normal IoT nodes meant for forwarding data packets. If the system encounters $\gamma_i > \theta_h$, it chooses to forward data packet. The variable θ_h is a highest cut-off value chosen as 0.8.

ii) *Decline*: The rule of declination is valid once the system encounters a malicious node positively. This rule entails to drop the data packet if it encounters a situation where $\gamma_i < \theta_h$. The variable θ_h is a lowest cut-off value chosen as 0.4.

iii) *Uncertain*: The rule of uncertainty is valid when the system fails to undertake any discrete or significant decision towards identifying a node as malicious or normal. Such situation is encountered when $\theta_l \leq \gamma_i \leq \theta_h$.

The consideration of this cut-off θ confirms that predictions of higher confidence have increasing impact to the IoT network. Any form of hard-decision is avoided by the proposed system by embedding the confidence score when the model is found to be uncertain. Such adaptive nature of proposed model makes it more trusted by the normal nodes while it permits the system for managing complex pattern of traffic dynamically. The key novelty of this module is about integration of probabilistic decision making into real-time decision process for permitting the system to manage the uncertainty use-cases without sacrificing communication efficiency or security.

2.5 Middleware Analysis

This is the final operational module which is meant for analyzing all the prediction score with moderate confidence level in prior module. The middleware component receives the samples that are reposited along with their metadata (e.g. timestamp, confidence scores, predicted labels, etc.). For all the samples x_i that is found to be fall under category of uncertain rule will be forwarded to middleware along with their timestamp t_i, confidence score γ_i, and predicted class $\hat{y}_i$. Consider, $U = \{\beta | \theta_l \leq \gamma_i \leq \theta_h\}$ is a set of information acting as an input to middleware module, where β represents a set consisting of x_i, t_i, γ_i, $\hat{y}_i$. All these data are forwarded to middleware for performing data forensics analysis. The outcome of this module can be also adopted for further enriching the quality of training model in future. The proposed design also leverages a feedback loop which carry out reviewing and re-labelling of uncertain events that are further exploited for retraining the model in semi-supervised manner.

2. Result and discussions

The assessment of the proposed study has been carried out using standard benchmarked dataset of UNSW-NB15 [26] on normal 64-bit windows machine of Intel Core *i*7 processor with 32 GB DDR4 RAM. The scripting is carried out using python on Jupyter notebook using following machine learning libraries e.g., NumPy 1.25, Pandas 2.0, scikit-learn 1.3 and TensorFlow 2.12 as deep learning framework. The complete dataset is split to 80:20 ratio for training and testing. With 50 epochs considered, the assessment is carried out with 64 units of dense layer, 0.3 dropout rate, 0.0001 learning rate, and 64 as batch size. The adaptive learning is boosted using Adam optimizer. This section highlights the accomplished outcome and interprets it.

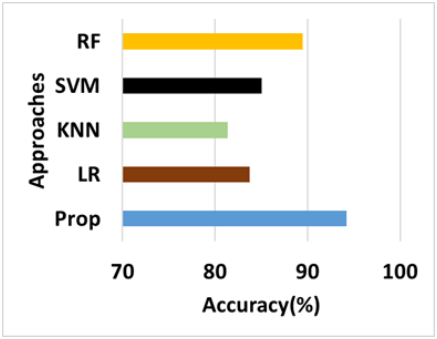
3.1 Accomplished Results

The Table 1 highlights the numerical outcome accomplished for the study by comparing proposed system with 4 frequently adopted conventional ML models e.g., LR, KNN, SVM, and RF with respect to accuracy-oriented parameters and response time. The outcome shows that proposed scheme offers approximately 10.55% of accuracy, 9.30% of improved precision, 9.31% of improved recall, and 9.14% of improved F1-Score in contrast to all conventional ML models. Apart from this, the

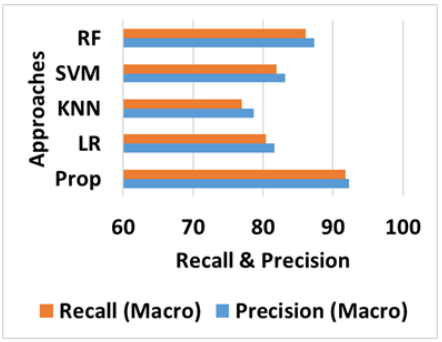
computational efficiency of proposed scheme is proven by exhibiting its 3.94 *s* of faster processing response in contrast to others. Hence, proposed system balances both security demands and computational efficiency at same time.

Table 1. Numerical Study Outcome

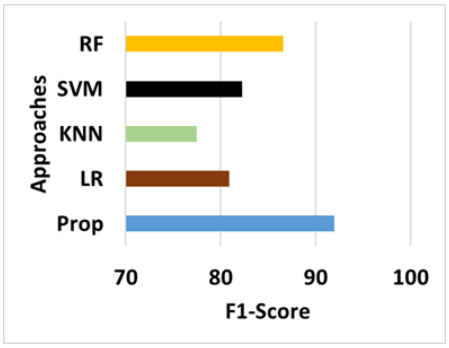
Classifier	Accuracy (%)	Precision (Macro)	Recall (Macro)	F1-Score (Macro)	Response Time (s)
Proposed (CNN)	94.26	92.34	91.80	91.96	1.93
Logistic Regression	83.75	81.62	80.40	80.85	4.68
KNN ($k = 5$)	81.40	78.71	76.95	77.48	7.92
SVM (RBF Kernel)	85.03	83.17	81.90	82.26	10.54
Random Forest	89.46	87.32	86.10	86.61	3.56



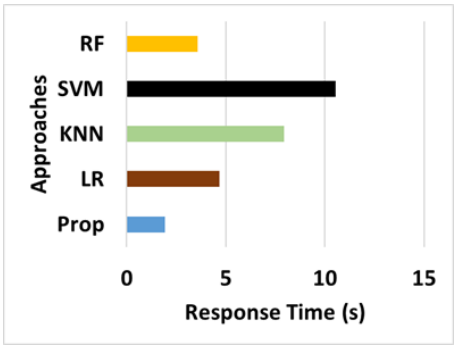
(a)



(b)



(c)



(d)

Fig. 2. Benchmark Outcome of Study

3.2 Discussion

On the ground of accomplished result, the robustness of proposed scheme is quite evident. The accomplishment of 94.26% accuracy can be attributed to the ability of convolution architecture for acquiring and learning the local patterns contributing to identify even very minor forms of deviation inflicted by attackers {Fig. 2(a)}. This ability can also be witnessed for conventional ML models under consideration but only for higher values of deviation, hence, they cannot identify smarter and intelligence malicious modules. Hence, the outcome of accuracy is quite novel as it contributes

towards generalization by integrating adaptive selection of feature with analysis of temporal flow. This enables proposed module to identify diverse form of complex attack patterns where existing models fails to do so.

The precision of 92.34% by proposed module is also found on higher side compared to other ML models which states that there is fewer decision of false positives (outliers) exhibiting proposed scheme can accurately differentiate normal from anomaly-based event {Figure 2(b)}. This accomplishment can be attributed to feature importance and improved filtering via hybrid preprocessing leading to ranking scores. Such form of integration operation is out of scope for SVM or KNN where outliers have higher chances to increase with more events. Hence, the reason for better precision score is mainly due to usage of decision logic driven by confidence score which acts as an indicator towards malicious and normal events. Proposed scheme has accomplished a recall score of 91.80% which represents increased sensitivity towards identifying original malicious events (Figure 2(b)). A closer look into outcome also shows that RF (recall = 86.10%) and SVM (recall = 81.90%) has also recorded better performance while LR model has exhibited poor performance. However, proposed scheme surpasses all the them which is mainly due to adoption of semi-supervised capability of learning that facilitates it to work similarly for traffic information with known or unknown pattern.

The proposed scheme has scored 91.96% of macro F1 score to state a proper balance between recall and precision score {Figure 2(c)}. The underperformance of LR and KNN is mainly due to skewed performance towards maximum classes which results in underrepresenting critical attacks in IoT. Adoption of dynamic thresholding with class balancing and smart sampling, proposed scheme provides more robustness in contrast to existing system. Further, proposed scheme has recorded 1.93s as response time which means it offers lowest latency when exposed to increasing IoT network {Figure 2(d)}. On the contrary, conventional ML models has recorded slower operation on larger volume of test data. The optimal performance of proposed scheme is mainly due to a joint operation of conditional decision logic and deep inference system with dimensional reduction simplified.

3. Conclusion

The proposed study introduces a novel, smart, and intelligent identification scheme for dynamic threats in IoT adopting efficient feature engineering and unique ML model towards addressing cyberthreats. The study model accomplishes superior accuracy by applying RF towards feature selection that is further optimized using CNN. Different from any existing ML model, proposed scheme is capable of classifying various category of attacks using confidence score while an uncertainty logging module in incorporated for detecting the ambiguous input. Hence, proposed scheme introduces a highly proactive strategy of cybersecurity. The future work will be in direction towards including more complex form of attacks and extending the AI modelling to more optimal level for multiple and heterogeneous attacker detection in IoT.

References

[1] N. Gowda Puttaswamy and A. Narasimha Murthy, “Optimizing real-time data preprocessing in IoT-based fog computing using machine learning algorithms,” *IAES Int. J. Artif. Intell.* (*IJ-AI*), vol. 14, no. 3, p. 1900, 2025, doi: 10.11591/ijai.v14.i3.pp1900-1909

[2] M. W. P. Maduranga, V. Tilwari, R. M. M. R. Rathnayake, and C. Sandamini, “AI-enabled 6G internet of things: Opportunities, key technologies, challenges, and future directions,” *Telecom Journal*, vol. 5, no. 3, pp. 804–822, 2024, doi: 10.3390/telecom5030041

[3] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, “Securing internet of things using machine and deep learning methods: a survey,” *Cluster Comput*. *Journal*, vol. 27, no. 7, pp. 9065–9089, 2024, doi: 10.1007/s10586-024-04509-0

[4] M.W.A. Ashraf, A.R. Singh, A. Pandian, R.S. Rathore, M. Bajaj, and I. Zaitsev, “A hybrid approach using support vector machine rule-based system: detecting cyber threats in internet of things,” *Sci. Rep*., vol. 14, no. 1, p. 27058, 2024, doi: 10.1038/s41598-024-

78976-1

[5] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," *Journal of Sens. Actuator Netw.*, vol. 10, no. 3, p. 58, 2021, doi: 10.3390/jsan10030058

[6] Y.B. Abushark, S. Hassan, and A.I. Khan, "Optimized AdaBoost support vector machine-based encryption for securing IoT-cloud healthcare data," *Journal of Sensors* (*Bessel Functions*), vol. 25, no. 3, 2025, doi: 10.3390/s25030731

[7] S. S. Alqahtany, A. Shaikh, and A. Alqazzaz, "Enhanced Grey Wolf Optimization (EGWO) and random forest based mechanism for intrusion detection in IoT networks," Sci. Rep., vol. 15, no. 1, p. 1916, 2025, doi: 10.1038/s41598-024-81147-x

[8] A. Alrefaei and M. Ilyas, "Using machine learning multiclass classification technique to detect IoT attacks in real time," *Journal of Sensors* (Basel), vol. 24, no. 14, p. 4516, 2024, doi: 10.3390/s24144516

[9] K.S. Adewole, A. Jacobsson, and P. Davidsson, "Intrusion detection framework for Internet of Things with rule induction for model explanation," *Journal of Sensors* (Basel), vol. 25, no. 6, 2025, doi: 10.3390/s25061845

[10] V. Prakash, O. Odedina, A. Kumar, L. Garg, and S. Bawa, "A secure framework for the Internet of Things anomalies using machine learning," *Discov. Internet Things*, vol. 4, no. 1, 2024, doi: 10.1007/s43926-024-00088-z

[11] P. R. Agbedanu, S. J. Yang, R. Musabe, I. Gatare, and J. Rwigema, "A scalable approach to Internet of Things and Industrial Internet of Things security: Evaluating adaptive self-adjusting memory K-nearest neighbor for zero-day attack detection," *Journal of Sensors* (*Basel*), vol. 25, no. 1, p. 216, 2025, doi: 10.3390/s25010216

[12] S. Chalichalamala, N. Govindan, and R. Kasarapu, "Logistic Regression Ensemble Classifier for Intrusion Detection System in Internet of Things," *Journal of Sensors* (*Basel*), vol. 23, no. 23, 2023, doi: 10.3390/s23239583

[13] J.R. Arunkumar, S. Velmurugan, B. Chinnaiah, G. Charulatha, M. Ramkumar Prabhu, and A. Prabhu Chakkaravarthy, "Logistic regression with elliptical curve cryptography to establish secure IoT," *Comput. Syst. Sci. Eng.*, vol. 45, no. 3, pp. 2635–2645, 2023, doi: 10.32604/csse.2023.031605

[14] H. El-Sofany, S.A. El-Seoud, O.H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports*, vol. 14, no. 1, p. 12077, 2024, doi: 10.1038/s41598-024-62861-y

[15] A. Gueriani, H. Kheddar, and A. C. Mazari, "Enhancing IoT security with CNN and LSTM-based intrusion detection systems," arXiv [cs.CR], 2024. [Online]. Available: http://arxiv.org/abs/2405.18624

[16] B.B. Gupta, A. Gaurav, R.W. Attar, V. Arya, A. Alhomoud, and K.T. Chui, "Sustainable IoT Security in entrepreneurship: Leveraging univariate feature selection and deep CNN model for innovation and knowledge," *Journal of Sustainability*, vol. 16, no. 14, p. 6219, 2024, doi: 10.3390/su16146219

[17] A. Mazid, S. Kirmani, and M. Abid, "Enhanced intrusion detection framework for securing IoT network using principal component analysis and CNN," *Inf. Secur. J. Glob. Perspect.*, pp. 1–21, 2024, doi: 10.1080/19393555.2024.2408256

[18] A. Deshmukh and K. Ravulakollu, "An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity," *Journal of Technologies* (*Basel*), vol. 12, no. 10, p. 203, 2024, doi: 10.3390/technologies12100203

[19] A. Mohamadi, H. Ghahramani, S.A. Asghari, and M. Aminian, "Securing healthcare with deep learning: A CNN-based model for medical IoT threat detection," *arXiv* [*cs.CR*], 2024. DOI: http://arxiv.org/abs/2410.23306

[20] A. Nazir et al., "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem," *Ain Shams Eng. Journal*, vol. 15, no. 7, p. 102777, 2024, doi: 10.1016/j.asej.2024.102777

[21] G. Zhao, X. Li, and H. Li, "A trusted authentication scheme using semantic LSTM and blockchain in IoT access control system," *Int. J. Semant. Web Inf. Syst.*, vol. 20, no. 1, pp. 1–27, 2024, doi: 10.4018/ijswis.341233

[22] A. G. Ayad, M. M. El-Gayar, N. A. Hikal, and N. A. Sakr, "Efficient real-time anomaly detection in IoT networks using one-class autoencoder and Deep Neural Network," *Journal of Electronics* (*Basel*), vol. 14, no. 1, p. 104, 2024, doi: 10.3390/electronics14010104

[23] H. Rhachi, Y. Balboul, and A. Bouayad, "Enhanced anomaly detection in IoT networks using deep autoencoders with feature selection techniques," *Journal of Sensors* (*Basel*), vol. 25, no. 10, 2025, doi: 10.3390/s25103150

[24] W. Yao, L. Hu, Y. Hou, and X. Li, "A Lightweight Intelligent network intrusion detection system using One-class Autoencoder and Ensemble Learning for IoT," *Journal of Sensors* (*Basel*), vol. 23, no. 8, 2023, doi: 10.3390/s23084141

[25] K. Saranya and A. Valarmathi, "A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms," *Scientific Reports*, vol. 15, no. 1, p. 10246, 2025, doi: 10.1038/s41598-025-93473-9

[26] M. B. Musthafa et al., "Optimizing IoT intrusion detection using balanced class distribution, feature selection, and ensemble machine learning techniques," *Journal of Sensors* (*Basel*), vol. 24, no. 13, p. 4293, 2024, doi: 10.3390/s24134293