IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 2, April 2026, pp. 1497~1504
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i2.pp1497-1504

A reinforcement-guided multi-phase hybrid architecture for threat profiling and defense towards IoT handheld device

Pushpa Rajput Narayana Singh[1,2], Neelambike Siddalingaiah[1,3]
[1]Department of Information Science and Engineering, GM Institute of Technology, Davanagere, India
[2]Department of Computer Science and Engineering, Jawaharlal Nehru New College of Engineering, Shivamogga, India
[3]Data Engineering, GM School of Advanced Studies, GM University, Davangere, India

Article Info

Article history:

Received Sep 25, 2025
Revised Jan 15, 2026
Accepted Jan 25, 2026

Keywords:

Artificial intelligence
Deep learning
Handheld device
Internet of things
Machine learning
Reinforcement learning

ABSTRACT

The contribution of artificial intelligence (AI) towards offering proactive security in handheld devices of internet of things (IoT) is in evolving stage. Review of literature showcases noteworthy attempts of machine learning (ML) and deep learning (DL) models; however, they are a large scope of improvement towards bridging the trade-off between security and computational-communication efficiency. This problem is addressed in this manuscript by presenting a unique and innovative solution where reinforcement learning (RL) has been hybridized with standalone ML and DL models. The model reads the permission-based data in cloud, followed by vulnerability prediction carried out by hybridization of RL and logistic regression (LR). Further, RL is integrated with deep neural network (DNN) for exploring a secure path to facilitate data transmission. The proposed model witnessed 97.9% accuracy, 67.35% of higher accuracy, 55.14% of reduced latency, and 52.54% of faster response time in contrast to baselines.

Corresponding Author:

Pushpa Rajput Narayana Singh
Department of Information Science and Engineering, GM Institute of Technology
P B Road, Davangere 577006, India
Email: pushpa@jnnce.ac.in

1. INTRODUCTION

The majority of the applications hosted in internet of things (IoT) are managed by a dedicated handheld device which consistently keeps on acquiring definitive data, subject them to processing, and exchange them accordingly [1]. Such form of data bear various higher-valued confidential information and this lead them to attract attention of different scales of an attacker. Conventional encryption-based solution will be heavy-weighted application of resource-limited IoT handheld device and hence lightweight-solution is seeked for optimal performance. In this perspective, artificial intelligence (AI) has been noted to contribute to offer a proactive security solution with an aid of various algorithms mechanized by machine learning (ML) and deep learning (DL). The AI-centric security solution modelling offers significant supportability of real-time threat monitoring, higher adaptiveness, and increased incorporation of intelligence [2].

Various related work has been studied towards realizing the effectiveness of existing system. Existing approaches has been noted to use reinforcement learning (RL) models towards adapting the security policies in a dynamic manner from lethal threats in IoT [3]–[6]. Existing studies have also noted usage of logistic regression (LR) towards classification of either actions or incoming data as regular or attacker utilizing faster and simpler boundaries of linear decision [7]–[11]. Random forest (RF) is noted to be implemented in standalone as well as in ensembled approach for identifying intrusion using voting of decision tree for encapsulating diversified patterns associated with device activity [12]–[19]. Deep neural network (DNN) based strategic security solution has also been noted towards learning high-dimensional

representation of network behavior for determining subtle forms of vulnerabilities [20]–[22]. Existing studies have also implemented long short-term memory (LSTM) for identifying various forms of anomalies or intruders emerging in IoT [23]–[25].

The research problems associated with existing literatures are as follows. First, almost majority of existing solutions have been design based on known behavior of an intruder which is not applicable when exposed to unseen adversarial environment. Second, an IoT handheld device has lesser memory and lesser processing capabilities which doesn't justifies its supportability towards hosting any of highly-claimed ML/DL models from literatures. Third, there are lesser degree of innovativeness associated with way the ML/DL models are implemented in either standalone or in ensembled method that doesn't offer more competitive edge towards leveraging security. Fourth, almost none of existing solution is claimed to present any actionable solution after threat detection which completely ignores demand of data transmission for IoT.

The aim of the proposed study is to introduce a robust security framework formulated by a distinct hybridization of RL model meant explicitly for determine the emerging threats in IoT handheld devices. The value-added contribution of study is as follows. First, the study presents a three-layered architecture that is capable of structuring permission-information followed by prediction of threats and exploration of secured routes. Second, the model introduces a novel mechanism towards ranking vulnerability for optimizing the containment method for proactive threats. Third, RL is hybridized by LR for exploring adversaries without sacrificing communication performance, while RL is also hybridized with DL architecture for exploring communication routes with minimal vulnerabilities.

2. METHOD

The proposed system introduces an innovative hybridized analytical framework harnessing the potential of RL towards securing the IoT devices from all the vulnerable forms of traffic systems. Figure 1 highlights the architecture exhibiting multi-stage learning, which involves the acquisition of knowledge based on spanning permission, vulnerability prediction based on RL, and optimization of a safer route. The ideation of proposed architecture is towards identifying the most vulnerable and dynamic form of threat following by providing them an alternative transmission route. The key benefit lies in parallel compliance of security operations as well as data transmission by handheld devices in an IoT. The complete operation is carried out by performing sequential and multiple operational modules, which are discussed as follows.

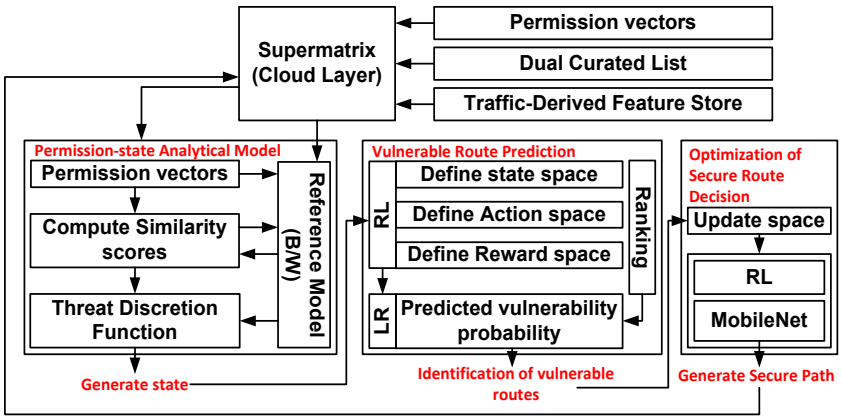

Figure 1. Architecture of the proposed system

2.1. Permission-state analytical model

This is the first core implementation module responsible for aggregating, structuring, and transforming all permission-based behavioral and traffic information into a usable form for analytical processing. All the permission-oriented information is aggregated from IoT handheld device where the types of information collected are traffic characteristics, interaction patterns, and access capabilities. All this information is stored in a supermatrix, which is a form of structured storage unit hosted within cloud ecosystem. Consider $p_1, p_2, \ldots, p_m$ represent the feasible set of permissions i.e., $P = \{p_1, p_2, \ldots, p_m\}$ associated with an IoT handheld device. Assume a_j be specific application that is characterized by permission vector v empirically represented as in (1).

$$v_j = [v_{j1}, v_{j2}, \dots, v_{jm}]$$
$$\text{Where, } v_j = \begin{cases} 1 & a_j \; deploys \; p_k \\ 0 & otherwise \end{cases} \quad (1)$$

The study considers the presence of whitelist (*W*) and blacklist (*B*) as two reference models present within the supermatrix. This curated information of *B* and *W* are stored and maintained in a supermatrix that is based on the patterns of historical behavior. Similarity scores are defined for them empirically in (2).

$$S_W(a_j) = \frac{|\alpha_1|}{|W|}, S_B(a_j) = \frac{|\alpha_2|}{|B|} \quad (2)$$

Where the variable α_1 and α_2 is mathematically represented as $(v_j \cap W)$ and $(v_j \cap B)$ respectively. After the information is aggregated from the dual curated list, this module structurize them into a matrix-based representation for segregating normal behavior from patterns involving traces of attacks. An empirical definition of threat discretion function is as in (3).

$$T(a_j) = \begin{cases} 0 & S_B(a_j) \geq \theta_W \\ 1 & S_B(a_j) \geq \theta_B \\ 2 & otherwise \end{cases} \quad (3)$$

Where the score of 0, 1, and 2 will represents benign, malicious, and suspicious (but not confirmed). Further, θ_W and θ_B represent the accepted cut-off for classifying whitelist (*W*) and cut-off for labelling blacklist node (*B*), respectively. This module is also responsible for yielding the state of RL in form of $S_j = \{v_j, T(a_j), f_i\}$, where the entity f_i represents the feature related to traffic (viz. device interaction, entropy, and packet rate).

2.2. Vulnerable route prediction

The outcome of the prior operation module generates traffic features which acts like an input for this module, which is meant for determining the specifics of communication routes with peak security threat to or from the particular IoT device. This module performs the unification of RL and LR towards prediction of vulnerability associated with the ML model. The system chooses LR for its higher interpretability and consumption of low resources. The state space is defined as $S_2 = \{S_1, X\}$ where the behavioral and traffic feature vector is represented by variable *X*. The action space is represented as A_2={inspect, mark vulnerable, and ignore}, while reward function is represented as in (4).

$$R_2(s, a) = \begin{cases} +1 & positive \\ -1 & outlier \\ 0 & neutral \end{cases} \quad (4)$$

The transition model $P_2(s`|s, a)$ is defined by alterations associated with the likelihood of threat after each action. It is to be noted that probabilistic feedback is yielded by this model, associated with the possibility that an IoT handheld device is vulnerable to potential cyberthreats. This feedback is used by RL for refining its process of decision-making that facilitates the model to learn potential features and its role in exhibiting risky behavior. The model then implements LR, which is represented as in (5).

$$\hat{y} = \sigma(w^T X + b) \quad (5)$$

In (5) consists of computation of the probability of an IoT handheld device being vulnerable $\hat{y}$ based on input arguments of the sigmoid function $\sigma(.)$, feature vector *X*. It also involves model parameters (*w*, *b*) representing weights and biases, respectively. The model implements a vulnerability ranking mechanism where the vulnerability score V_n is empirically defined in (6).

$$V_n = \beta . \hat{y} + h_1 + h_2 \quad (6)$$

In (6), the computation of the vulnerability score is carried out by addition of three components. The first component represents the product of weighing parameter β and probability of predicted vulnerability $\hat{y}$. The second component h_1 represents the product of weighing parameter β_1 and $(1 - S_w(a_j))$ while the third component h_2 represents product of weighing parameter β_2 and $S_B(a_j)$. The ranking of the IoT handheld device is carried out as $R_n = sort(V_n)$. The outcome of this module is mainly two-fold determination of vulnerable IoT handheld device (V_n) and rank list of potentially threat-prone communication channels (R_n).

2.3. Optimization of secure route decision

This module extends the prior operation by facilitating an alternative secure route for data transmission, choosing communication channels that are empirically confirmed to have the lowest threats. This module unifies a highly compact architecture of a DL known as MobileNet with RL for carrying out this operation. The state variable is defined as $S_3 = \{F_2, G\}$ where the network graph is represented as G, while action is represented as A_3={select next hop (n_i)|n_i∈neighbors}. The reward $R_3(s,a)$ is indexed as +5, -5, +10, and -10, representing a secure hop leading to a destination node, a hop leading to a vulnerable node, a completed secured route successfully, and a detected attack or blocked route of transmission. The security prediction for IoT handheld device $\hat{s}_i = \mu(Z_i)$, where the valuation of $\hat{s}_i$ ranges to [0, 1]. Therefore, it can be seen that MobileNet is used for assessing which IoT handheld device is found secure for routing. This DL-based prediction is utilized by RL for selecting the consecutive optimal hops at every point of decision. An empirical formulation of the secure route score is shown in (7).

$$SR(path) = \sum_{i=1}^{k} \hat{s}_i - \tau \text{ where } \tau = \rho \sum_{i=1}^{k} V_{n_i} \quad (7)$$

After the expression (7) is computed, the accomplished SR(path) is used for finding the optimal secure route as $S_p = arg_{max}[SR(path)]$. Hence, the module is progressive to be highly intelligent in resisting all vulnerable areas which it can effectively determine the best secured data transmission channels. The novelty of this module is the proactive selection of secure routes depending upon real-time prediction of DL and patterns of learned behavior. This strategy completely differs from existing solution where static routing tables or blocking mechanism based on threats have been utilized.

3. RESULTS AND DISCUSSION

A specific and highly controlled research environment has been chosen in order to carry out the implementation of the proposed study model. This section discusses the rationale of the dataset adopted followed by the adoption of an environment to carry out an assessment. The assessment claims the effectiveness of the proposed model based on the accomplished result that is also discussed in this section for better insight.

3.1. Dataset adoption

The implementation of the proposed system is carried out considering Edge-IIoTset dataset [26]. The dataset consists of raw packet traces of traffic acquired from smart-home handheld controllers, surveillance cameras, smartphone, and Raspberry Pi devices. The prime reason for adopting this dataset is the inclusion of maximum numbers of traffic features in contrast to other existing datasets for similar purposes. There are 61 traffic features extracted viz. entropy values, flag distribution, inter-arrival time, packet size, flow duration, and metadata on signatures associated with communication of handheld IoT devices.

3.2. Environment adopted in simulation

From the perspective of hardware adoption, the implementation chooses to use Intel i5 unit as CPU with 32 GB DD4 RAM and 1 TB of storage in 64-bit windows machine. Further, from a software involvement perspective, the scripting is carried out using Python libraries such as TensorFlow, Pandas, NumPy, and scikit-learn, while the verification of feature extraction is conducted using CICFlowMeter. The analysis of the packet is carried out using Wireshark. The hyperparameters and their values are as follows: the script involves choosing 0.0004 as the learning rate, 128 batch size, and 100 epoch. The exploration rate decay is 0.992 while 0.91 is considered as the discount factor considering 4 hidden layers. Rectified linear unit (ReLU) and SoftMax is chosen as activation functions, while Adam optimizer is used with 15,000 replay buffer size.

3.3. Achieved result

The accomplished outcome of the study is compared with multiple baseline models viz. conventional LR model, conventional RL model, RF model, and DNN. The analysis is carried out in dual perspective viz., estimation based on accuracy performance (Table 1) and estimation based on communication performance (Table 2). The outcome of Table 1 showcases that proposed study model offers maximum strength of adversary detection while it is shown maximum resilient against the following adversaries viz. botnet-related traffic, reconnaissance, packet injection, spoofing, man-in-the-middle attack, and distributed denial-of-service (DDoS). Similarly, the numerical outcome exhibited in Table 2 represents a higher throughput capability of the proposed model along with minimal latency and reduced response time.

Table 1. Estimated accuracy performance in benchmark analysis

Model		Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Existing baseline models	LR	82.7	81.2	80.9	81.0
	RF	89.4	88.1	87.6	87.9
	RL	90.6	89.4	88.9	89.1
	DNN	92.3	91.5	90.7	91.1
Proposed model		97.9	97.3	96.8	97.0

Table 2. Estimated communication performance in benchmark analysis

Model		Throughput (samples/sec)	Latency (ms)	Response time (ms)
Existing baseline models	LR	380	36	54
	RF	460	29	48
	RL	530	23	41
	DNN	590	19	34
Proposed model		820	12	21

3.4. Discussion

The study outcome shows some interesting patterns as exhibited in Figure 2. Figures 2(a) and 2(b) represents outcome related to accuracy and throughput, respectively. The exhibits of Figures 2(c) and 2(d) represent latency and response time, respectively.

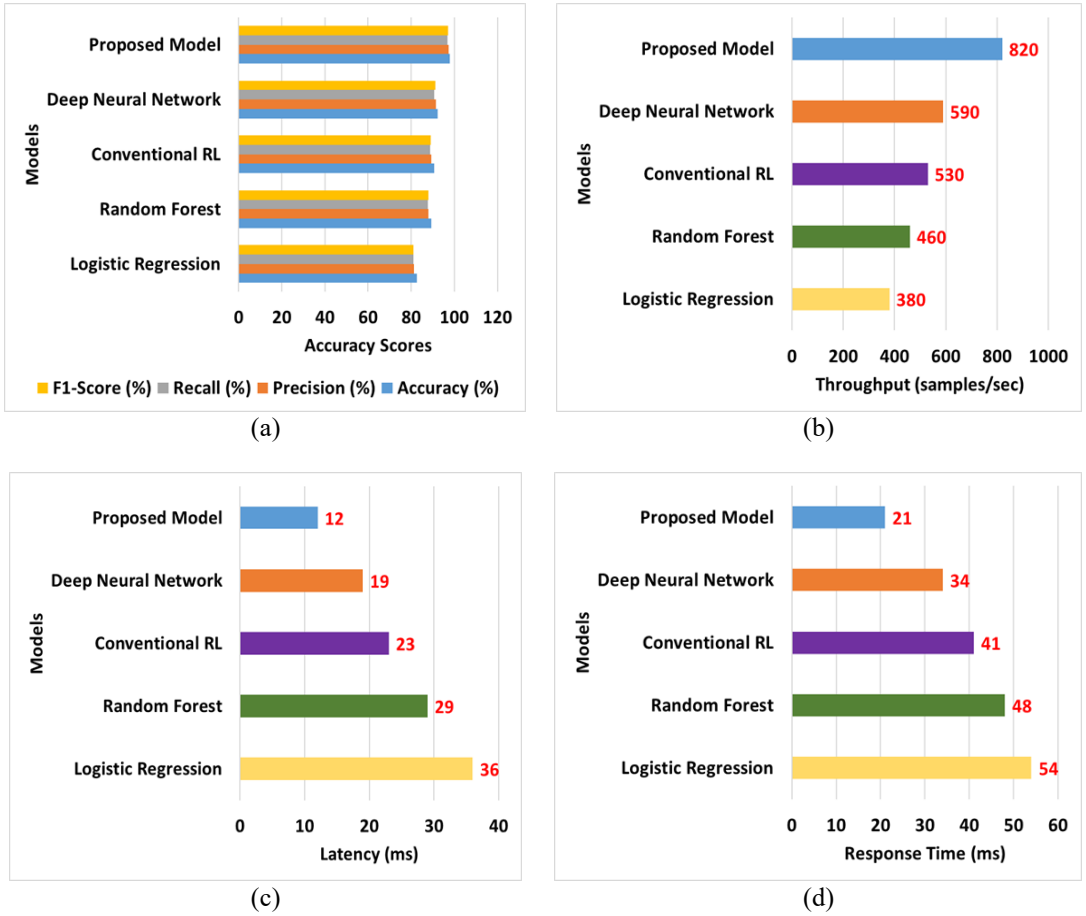

Figure 2. Graphical outcome of benchmark analysis of (a) accuracy scores, (b) throughput, (c), latency, and (d) response time

From the exhibits of Figure 2(a), it can be seen that the proposed system has accomplished 97.9% of detection accuracy which is mainly attributed for inclusion of dynamic multi-module adaptation and it doesn't consider any static signatures, which is seen usually in existing approaches. It shows an

accomplishment of 97.3% precision which means there is extremely few occurrences of outliers. This outcome trend can be attributed by isolation capability of the model towards patterns of noise usually generated by IoT handheld devices. The outcome shows the proposed system to achieve 96.8% of recall, exhibiting potential detection capability against true attacks which is reinforced by involvement of pattern learning of temporal flow. It shows 97% of F1-score accomplished for proposed model exhibiting highly balanced performance which is due to parallel unification of reactive and predictive analysis.

Figure 2(b) showcases the proposed model to accomplish 820 samples per second which is noted to be the maximized throughput among all the baseline models. The outcome of this trend can be reasoned with multi-threaded optimized inference and execution in the proposed model. The proposed system is noted to offer only 12 ms of latency as seen in Figure 2(c) which is drastically better in contrast to any existing baseline models. The prime reason for this is a strategic access pattern with memory efficiency and lightweight prediction of attack. Finally, Figure 2(d) shows only 21 ms of response time which is highly reduced in contrast to other models. The outcome shows its high inclination towards potential threat mitigation. The prime reason for this is faster evaluation of state and significantly reduced buffering.

3.5. Novelty of study

While adoption of baseline models is witnessed to be used for resisting a priori adversaries or a set of known adversaries, the proposed model is designed considering lack of any a priori information of the threats. Table 3 showcases the potential capability of proposed system, where it's exhibited to show its resilience from zero-day attacks apart from other standard form of standard attacks frequently reported. Apart from this, it is also capable of resisting permission-misuse attacks, polymorphic and adaptive form of threats, and lateral movement attacks.

Table 3. Estimated communication performance in benchmark analysis

Attribute	Existing baselines				Proposed model
	RL	LR	RF	LSTM	
Ability for threat categorization	No	No	No	Good	Potential profiling capability for multi-dimensional attackers
Zero-day attacks	Poor exploration	Not capable	Limited generalization	Moderate	Superior adaptive exploration, supportive of adversarial simulation study
Responsiveness	High	Low	Moderate	Very high	Very low (due to transition logic of optimized state)
Suitability to IoT edge nodes	Low-moderate	High	Moderate	Moderate	Very high (due to lightweight optimization)

4. CONCLUSION

The proposed study introduces an innovative security framework for securing IoT handheld devices adopting two different hybrid variants of RL model itself. The model is capable of resisting both known and unknown form of threats in network layers. It does so by combining supermatrix with permission information into adaptive decision-making strategy by RL, filtering by lightweight ML and route refinement using DL. A self-optimized and holistic structure has been presented in proposed study that can operate over different states of communication dynamics facilitating the agents to consistently realize the updated traffic state followed by identification of vulnerable routes and exploring safer routes. The study outcome shows optimal performance for proposed study model in contrast to existing baseline models. The future work can be initiated towards improving the privacy preservation by further incorporating federated learning in the current state of model. Further, an energy optimized modelling can be carried out towards ensuring enhancement of lifespan of battery-operated handheld IoT device. Future work can be also carried out towards involvement blockchain technology for evolving trust scores in model to offer an optimal security.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Pushpa Rajput	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Narayana Singh Neelambike Siddalingaiah		✓				✓		✓	✓	✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

This section not applicable. This study did not involve any human subjects, personal identifiable information, or scenarios requiring individual informed consent, as it exclusively utilized publicly available datasets, computational simulations, and machine learning algorithms without breaching privacy rights or necessitating written permissions from participants.

ETHICAL APPROVAL

This section not applicable. The research complied with all relevant institutional policies but did not involve human subjects or animal use, relying solely on non-biological computational methods such as optimization algorithms and data analysis, thus exempt from review by an institutional review board, ethics committee, or adherence to the Helsinki Declaration.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author [PRNS], upon reasonable request.

REFERENCES

[1] A. Sharma and K. Bhushan, "A comprehensive survey on IoT security: challenges, security issues, and countermeasures," *Computer Science Review*, vol. 59, 2026, doi: 10.1016/j.cosrev.2025.100839.
[2] K. Dubey, R. Dubey, S. Panedy, and S. Kumar, "A review of IoT security: machine learning and deep learning perspective," *Procedia Computer Science*, vol. 235, pp. 335–346, 2024, doi: 10.1016/j.procs.2024.04.034.
[3] M. Mouyart, G. M. Machado, and J. Y. Jun, "A multi-agent intrusion detection system optimized by a deep reinforcement learning approach with a dataset enlarged using a generative model to reduce the bias effect," *Journal of Sensor and Actuator Networks*, vol. 12, no. 5, 2023, doi: 10.3390/jsan12050068.
[4] J. A. Shaikh *et al.*, "A deep reinforcement learning-based robust intrusion detection system for securing IoMT healthcare networks," *Frontiers in Medicine*, vol. 12, 2025, doi: 10.3389/fmed.2025.1524286.
[5] K. Ren, Y. Zeng, Y. Zhong, B. Sheng, and Y. Zhang, "MAFSIDS: a reinforcement learning-based intrusion detection model for multi-agent feature selection networks," *Journal of Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00814-4.
[6] C. Mahjoub, M. Hamdi, R. I. Alkanhel, S. Mohamed, and R. Ejbali, "An adversarial environment reinforcement learning-driven intrusion detection algorithm for internet of things," *Eurasip Journal on Wireless Communications and Networking*, vol. 2024, no. 1, 2024, doi: 10.1186/s13638-024-02348-6.
[7] V. S, "Logistic regression with elliptical curve cryptography to establish secure IoT," *SSRN Electronic Journal*, 2025, doi: 10.2139/ssrn.5219859.
[8] S. Chalichalamala, N. Govindan, and R. Kasarapu, "Logistic regression ensemble classifier for intrusion detection system in internet of things," *Sensors*, vol. 23, no. 23, 2023, doi: 10.3390/s23239583.
[9] D. Gladić, J. Petrovački, S. Sladojević, M. Arsenović, and S. Ristić, "Analysis of different IDS-based machine learning models for secure data transmission in IoT networks," *Open Computer Science*, vol. 15, no. 1, 2025, doi: 10.1515/comp-2025-0032.
[10] A. Hafid, M. Rahouti, and M. Aledhari, "Optimizing intrusion detection in IoMT networks through interpretable and cost-aware machine learning," *Mathematics*, vol. 13, no. 10, 2025, doi: 10.3390/math13101574.
[11] K. Rahman *et al.*, "Cognitive lightweight logistic regression-based IDS for IoT-enabled FANET to detect cyberattacks," *Mobile Information Systems*, vol. 2023, pp. 1–11, 2023, doi: 10.1155/2023/7690322.
[12] O. Z. Akif, S. M. Ali, A. F. Sabih, A. T. Sadiq, and S. K. Subramaniam, "Intrusion detection system for IoT based on modified random forest algorithm," *Iraqi Journal for Computer Science and Mathematics*, vol. 6, no. 2, pp. 221–229, 2025, doi: 10.52866/2788-7421.1258.

[13] V. Pai, K. Pai, S. Manjunatha, S. Hirmeti, and V. V. Bhat, "Adaptive network anomaly detection using machine learning approaches," *Eurasip Journal on Information Security*, vol. 2025, no. 1, 2025, doi: 10.1186/s13635-025-00216-4.
[14] C. Lu, Y. Cao, and Z. Wang, "Research on intrusion detection based on an enhanced random forest algorithm," *Applied Sciences*, vol. 14, no. 2, 2024, doi: 10.3390/app14020714.
[15] K. S. Adewole, A. Jacobsson, and P. Davidsson, "Intrusion detection framework for internet of things with rule induction for model explanation," *Sensors*, vol. 25, no. 6, 2025, doi: 10.3390/s25061845.
[16] M. Sasi, O. R. Adegboye, and A. Alzubi, "Explainable and optimized random forest for anomaly detection in IoT networks using the RIME metaheuristic," *Electronics*, vol. 14, no. 22, 2025, doi: 10.3390/electronics14224465.
[17] H. Alrakah, Y. A. Adam, M. Abdalraheem, P. Mansur, S. Rizwan, and I. Al-Shourbaji, "Leveraging random forest to detect botnet attacks in IoT environments," *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 3, 2025, doi: 10.22399/ijcesen.3717.
[18] M. Aly and M. H. Behiry, "Enhancing anomaly detection in IoT-driven factories using logistic boosting, random forest, and SVM: A comparative machine learning approach," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-08436-x.
[19] J. B. Awotunde, F. E. Ayo, R. Panigrahi, A. Garg, A. K. Bhoi, and P. Barsocchi, "A multi-level random forest model-based intrusion detection using fuzzy inference system for internet of things networks," *International Journal of Computational Intelligence Systems*, vol. 16, no. 1, 2023, doi: 10.1007/s44196-023-00205-w.
[20] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered intrusion detection system," *Internet of Things*, vol. 24, 2023, doi: 10.1016/j.iot.2023.100936.
[21] M. A. Hossain, "Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach," *Eurasip Journal on Information Security*, vol. 2025, no. 1, 2025, doi: 10.1186/s13635-025-00202-w.
[22] M. Vishwakarma and N. Kesswani, "DIDS: a deep neural network based real-time intrusion detection system for IoT," *Decision Analytics Journal*, vol. 5, 2022, doi: 10.1016/j.dajour.2022.100142.
[23] T. B. Ogunseyi and G. Thiyagarajan, "An explainable LSTM-based intrusion detection system optimized by firefly algorithm for IoT networks," *Sensors*, vol. 25, no. 7, 2025, doi: 10.3390/s25072288.
[24] P. Sinha, D. Sahu, S. Prakash, T. Yang, R. S. Rathore, and V. K. Pandey, "A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-94500-5.
[25] A. Nazir *et al.*, "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem," *Ain Shams Engineering Journal*, vol. 15, no. 7, 2024, doi: 10.1016/j.asej.2024.102777.
[26] O. B. Samin, N. A. A. Algeelani, A. Bathich, M. Omar, M. Mansoor, and A. Khan, "Optimizing agricultural data security: harnessing IoT and AI with latency aware accuracy index (LAAI)," *PeerJ Computer Science*, vol. 10, pp. 1–22, 2024, doi: 10.7717/PEERJ-CS.2276.

BIOGRAPHIES OF AUTHORS

Pushpa Rajput Narayana Singh is an accomplished academic and professional with a M.Tech. in Computer Science and Engineering from Jawaharlal Nehru New College of Engineering, Shimoga, under Visvesvaraya Technological University, Belagavi and a B.E. in the same field from Jawaharlal Nehru New College of Engineering, Shimoga. She has 13 years of teaching experience, she is currently working as an assistant professor, in the Department of Computer Science and Engineering at Jawaharlal Nehru New College of Engineering, Shimoga. Her expertise spans networks, internet of things, and machine learning. She can be contacted at email: pushpa@jnnce.ac.in.

Dr. Neelambike Siddalingaiah is an accomplished academic and professional with a Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi. She holds an M.Tech. in the same field from Bapuji Institute of Engineering and Technology and a B.E. in Information Science from Jawaharlal Nehru New College of Engineering, Shimoga with over 18 years of experience, she is currently working as a professor and head of the Department of Information Science and Engineering at GM Institute of Technology, Davangere. In addition, she is also program director for Data Engineering at GM School of Advanced Studies, GM University. Her expertise spans networks, data analytics, cloud computing, artificial intelligence, and vehicular ad hoc networks. She has also published several papers and holds several patents, recognized for her contributions, she received the "Excellent and innovation academician" award at international convention 2021 and excellent faculty award at GM University 2023. She can be contacted at email: neelambikes@gmit.ac.in.