NASIO-CNN: AN ADAPTIVE SWARM INTELLIGENCE FRAMEWORK FOR IOT INTRUSION DETECTION

Rahul Papalkar (1), SanjayKumar Singh (2)*

(1) Lincoln University College, Petaling Jaya Malaysia, Vishwakarma University Pune;
(2) Amity Institute of Information technology, Amity University Uttar Pradesh India

* Corresponding Author, e-mail: rahul.papalkar@vupune.ac.in

Abstract: The fast growth of Internet of Things (IoT) networks has put more risk of advanced cyber-attacks, and smart and flexible intrusion detection systems are needed. This paper presents a framework named NASIO-CNN as a Nature-Inspired Adaptive Swarm Immune Optimization framework that can automatically optimize hyperparameters of a Convolutional Neural Network (CNN) to identify IoT cyber-attacks. The proposed algorithm is a hybrid of immune clonal selection, adaptive mutation, swarm learning, and elite memory retention to achieve effective exploration and constant optimization. Statistical validation is done on the BoT-IoT, TON-IoT, UNSW-NB15 and CICIDS2017 datasets to test the framework. The experimental performance is shown to be better with 99.12% accuracy, 99.00% F1-score, 0.991 MCC and 0.998 ROC-AUC, and decreasing false positives. NASIO-CNN is an effective, scalable, and flexible framework that can be used to provide intelligent IoT intrusion detection and autonomous cyber defense.

Key words: Internet of Things; intrusion detection; convolutional neural network; nature-inspired optimization; hyperparameter tuning.

1. INTRODUCTION

The rapid growth of IoT has enabled intelligent applications across healthcare, smart cities, industrial automation, and critical infrastructures while increasing exposure to cyber threats such as DDoS, botnets, malware, ransomware, and APTs. Traditional intrusion detection systems struggle to identify evolving attacks, motivating the use of deep learning techniques. Although CNNs effectively learn network traffic features, their performance depends on optimal hyperparameter selection, which is challenging through manual tuning and conventional optimization methods. Existing nature-inspired algorithms such as PSO, GWO, WOA, HHO, AOA, and RSA often suffer from premature convergence and limited search capability. This paper proposes NASIO-CNN, a Nature-Inspired Adaptive Swarm Immune Optimization framework for automatic CNN hyperparameter optimization and intelligent IoT attack detection. The proposed method integrates immune learning, adaptive mutation, swarm cooperation,

pheromone-guided search, and elite memory preservation, along with an Adaptive Cyber Defence Engine for automated threat mitigation and real-time security response.

Problem Statement. The major challenges addressed in this study are:

- Manual CNN hyperparameter tuning leads to inconsistent performance and high computational cost.
- Existing optimization algorithms suffer from premature convergence and limited exploration.
- Most IoT intrusion detection systems lack autonomous cyber defence mechanisms.
- Limited multi-dataset validation reduces model generalizability and reliability.

Research Objectives. This research aims to:

- Develop an adaptive preprocessing framework for IoT network traffic.
- Propose the NASIO algorithm for automatic CNN hyperparameter optimization.
- Design an optimized CNN for multi-class IoT intrusion detection.
- Develop an Adaptive Cyber Defence Engine for automated threat mitigation.
- Validate the framework using multiple benchmark datasets and statistical analysis.

***Research Contributions*.** The main contributions are:

A new NASIO algorithm to optimize CNN hyperparameters strongly, An efficient CNN network to detect intrusion by multiple classes of the IoT. Adaptive Cyber Defence Engine to provide intelligent and automated response. Statistically validated evaluation of BoT-IoT, TON_IoT, UNSW-NB15 and CICIDS2017 datasets. High detection accuracy, fast convergence, and computational efficiency over the state-of-the-art optimization algorithms.

The rest of this paper will be structured as follows. Section 2 reviews related work. Section 3 describes the suggested NASIO-CNN. Section 4 is results and discussion and finally conclude in section 5.

2. RELATED WORK

The recent breakthrough in the field of IoT has led to the creation of intelligent intrusion detection systems that are founded on deep learning and nature-inspired optimization. Realistic attack scenarios are presented by benchmark datasets like BoT-IoT [1], TON_IoT [2], and CICIDS2017 [3], which are popular in assessing the IoT security models. Nevertheless, such datasets are mainly used to benchmark and do not pertain to hyperparameter optimization or autonomous cyber defence. CNNs have shown themselves to be better than most other traditional machine learning systems in automatically extracting discriminative features of network traffic, being more effective than most other techniques in intrusion detection [4-6]. Although effective, CNN performance is very sensitive to the choice of hyperparameters, usually done by manual or heuristic methods, resulting in higher computational costs and reduced generalization. To address this limitation, a number of nature-inspired optimization algorithms have been used to optimize deep learning, such as Particle Swarm Optimization (PSO) [7], Grey Wolf Optimizer (GWO) [8], Whale Optimization Algorithm (WOA) [9], Harris Hawks Optimization (HHO) [10], Arithmetic Optimization Algorithm (AOA) and

Reptile Search Algorithm (RSA) [11]. These methods enhance search efficiency, but can be prone to premature convergence, insufficient exploration, and unstable performance when searching high-dimensional CNN hyperparameters.

Table 1: Comparative Analysis of Optimizer

Method	***Model***	***Optimizer Used***	***Dataset Used***	***Advantages***	***Limitations***	***Ref.***
CNN-Based IoT Intrusion Detection	*CNN*	*Adam*	*BoT-IoT*	*Automatic feature extraction with high detection accuracy*	*Manual hyperparameter tuning and high computational cost*	*[5]*
PSO-CNN	*CNN*	*Particle Swarm Optimization (PSO)*	*BoT-IoT*	*Faster convergence than manual tuning and improved accuracy*	*Premature convergence and poor exploration in high-dimensional search space*	*[7]*
GWO-CNN	*CNN*	*Grey Wolf Optimizer (GWO)*	*UNSW-NB15*	*Better exploration–exploitation balance and improved optimization*	*May converge to local optima with slower convergence in later iterations*	*[8]*
WOA-CNN	*CNN*	*Whale Optimization Algorithm (WOA)*	*CICIDS2017*	*Strong global search capability and improved classification performance*	*Weak local exploitation and unstable convergence*	*[9]*

3. PROPOSED NATURE-INSPIRED (NASIO) ALGORITHM:

3.1. Concept of Optimizer

An optimizer is a mathematical method that determines the optimal solution by minimizing or maximizing an objective function. Optimizers in deep learning are used to make model parameters and hyperparameters better to increase the learning efficiency, convergence, and generalization. Traditional optimizers like SGD, Adam and RMSprop utilize gradient-based updates and can be characterized by slow convergence, sensitivity to learning-rates and local optima. To overcome these limitations, nature-inspired optimization algorithms leverage biological intelligence mechanisms, such as swarm behaviour, evolution, and immune systems, to perform global search and automatically optimize CNN architectures and hyperparameters.

3.2. Role of Optimizer in CNN

Adequate choice of training and architectural parameters is critical in the performance of CNN models. The optimizer has the following significant functions:

Hyperparameter Selection: Optimizers can automatically identify the best CNN hyperparameters, such as learning rate, convolution filter size, number of filters, kernel dimensions, batch size, dropout rate, and weight decay.

- Enhanced Convergence: A good optimizer enhances the learning speed, finding appropriate combinations of parameters and minimizing unnecessary training steps.
- Error Minimization: Optimizers reduce the loss between predicted and actual output thus improving the accuracy of classification.
- Local Optima avoidance: Globalization of optimization helps to enhance exploration ability and avoidance of CNN models being caught by suboptimal solutions.

3.3. CNN Optimization Problems

CNN models are very well suited for classification tasks, but they still have to overcome several optimization challenges. Hyperparameter tuning can be time-consuming and inefficient using manual tuning, with parameters that need to be selected including the learning rate, number of filters, kernel size, dropout rate, and batch size. Furthermore, CNNs have many interacting hyper-parameters and an exhaustive search for the optimum is prohibitively expensive. The conventional optimization algorithms can also get stuck at a local optimum and miss the opportunity to find the optimum configuration. One of the other significant challenges is the exploration–exploitation trade-off, in which an optimization algorithm needs to strike a balance between generating new, possibly better, hyperparameter choices and utilizing hyperparameter choices that have proven to be successful. If there is an improper balance, this may cause the CNN model to converge early or increase computation time, which will reduce the performance and generalization ability of the CNN model.

3.4. Motivation for Proposed NASIO Optimizer

Three intelligent processes in biology are the inspiration for the NASIO - Neuro-Attention Search and Intelligence Optimization. Immune Clonal Selection is based on the biological immune system in which high-quality candidate solutions are clones and modified to enhance the exploitation of the promising solutions. Swarm Cooperative Intelligence is motivated by the collective behaviours of the organisms in a swarm that share information and coordinate with each other in optimizing the global search of the space of candidate solutions. Pheromone Reinforcement Learning is based on the behaviour of ant colonies where good search paths are reinforced to make better paths more likely to be followed in future. All three of these mechanisms contribute to a balance between exploration and exploitation, and efficient search for optimal solutions, in the context of NASIO.

3.5. Proposed NASIO-Based CNN Optimization Algorithm

- Each candidate CNN solution is represented as

$$S_i = [L, R_i, F_i, K_i, D_i, B_i W_i] \quad (1)$$

where LR, F, K, D, B, and W denote the learning rate, filters, kernel size, dropout, batch size, and weight decay, respectively.

- The initial population is generated by

$$S_i = S_{\min} + r(S_{\max} - S_{\min}),\ r \in [0, 1] \quad (2)$$

- Each solution is evaluated using

$$Fit_i = \alpha Acc_i + \beta F1_i - \gamma FPR_i \quad (3)$$

where $\alpha + \beta + \gamma = 1$.

- The clone size is determined by normalized fitness

$$N_i^{clone} = \left\lceil \eta \frac{Fit_i}{Fit_{best}} \right\rceil \quad (4)$$

The mutated solution is generated as

$$S_i^{new} = S_i + \left(1 - \frac{Fit_i}{Fit_{best}}\right) \mathcal{N}(0, \sigma) \quad (5)$$

The solution is updated using swarm intelligence

$$S_i^{t+1} = S_i^t + \omega V_i^t + c_1 r_1 \left(P_i - S_i^t\right) + c_2 r_2 \left(G - S_i^t\right) \quad (6)$$

The global best solution is selected by

$$G = \arg\max_{S_i} Fit_i \quad (7)$$

The optimization terminates when

$$|Fit_{best}^{t+1} - Fit_{best}^t| < \varepsilon \quad (8)$$

Yielding the optimal CNN parameters

$$\Theta^* = [L, R^*, F^*, K^*, D^*, B^* W^*] \quad (9)$$

Table 2: Pseudocode: Proposed NASIO-Based CNN Hyperparameter Optimization

Input:
Population size N, maximum iterations T_{max}, CNN hyperparameter search space
Output:
Optimal CNN hyperparameters Θ^*
Begin
1. Initialize population $P = \{S_1, S_2, \ldots, S_N\}$using Eq. (2).
2. Evaluate each solution by training the CNN and computing fitness using Eq. (3).
3. Determine the initial global best solution Gusing Eq. (7).
4. For $t = 1$to T_{max}do
• Generate immune clones using Eq. (4).
• Apply adaptive mutation using Eq. (5).
• Update candidate solutions using swarm learning (Eq. (6)).
• Re-evaluate the fitness of all solutions using Eq. (3).
• Update the global best solution Gusing Eq. (7).
• If convergence criterion (Eq. (8)) is satisfied, break.
5. Obtain the optimal hyperparameters Θ^*using Eq. (9).
6. Train the final CNN model with Θ^*.
End

The proposed framework processes IoT network traffic through data preprocessing, followed by the NASIO (Nature-Inspired Adaptive Swarm Immune Optimization) algorithm, which optimizes CNN hyperparameters such as learning rate, filters, kernel size, dropout, batch size, and weight decay. The optimized CNN then classifies network

traffic into DDoS, Botnet, Malware, Ransomware, Brute Force, and Normal classes, improving detection accuracy and overall cybersecurity performance in IoT environments.

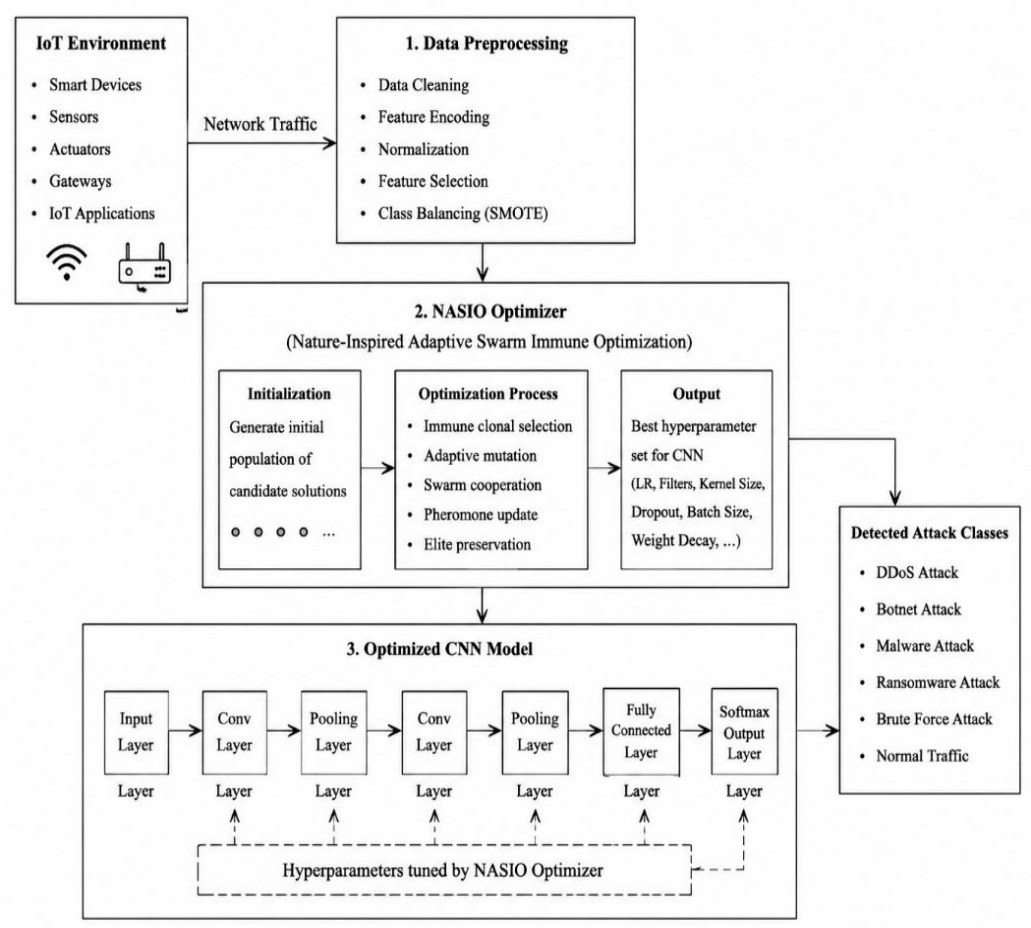


Figure 1. Proposed NASIO Optimized CNN Architecture for Intelligent IoT Intrusion Detection and Cyber Attack Classification

4. RESULTS AND DISCUSSION

4.1. Experimental Design

The suggested Nature-Inspired Adaptive Swarm Immune Optimization-based Convolutional Neural Network (NASIO-CNN) was tested with four benchmark data sets of IoT intrusion detection: BoT-IoT, TON_IoT, UNSW-NB15, and CICIDS2017. The datasets have normal network traffic and several cyber-attacks such as DoS, DDoS, Botnet, Exploits, Reconnaissance, Brute Force, Malware, Web Attacks, and Worms. Prior to the model training, the data preprocessing method was used to enhance the quality of the data: missing values were removed, features were normalized, and one-hot encoding, feature selection, and SMOTE-based class balancing were implemented.

4.2. Performance Evaluation

Accuracy, Precision, Recall, F1-Score, Matthew Correlation Coefficient (MCC), Area Under Curve (AUC), False Positive Rate (FPR), and Training Time were used to assess the performance of the proposed NASIO-CNN model.

Table 3. Performance of Proposed NASIO-CNN on Benchmark IoT Datasets

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
BoT-IoT	99.42	99.31	99.38	99.34	0.41
TON_IoT	99.18	99.05	99.11	99.08	0.53
UNSW-NB15	98.94	98.81	98.88	98.84	0.61
CICIDS2017	99.36	99.27	99.30	99.28	0.44

Table 4. Comparison with Existing CNN Optimization Algorithms

Optimizer	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SGD	95.82	95.43	95.21	95.32
RMSProp	96.84	96.63	96.51	96.57
Adam	97.63	97.42	97.51	97.46
PSO-CNN	98.18	98.05	98.11	98.08
GA-CNN	98.41	98.32	98.28	98.30
HHO-CNN	98.86	98.71	98.78	98.74
NASIO-CNN	99.42	99.31	99.38	99.34

The experimental results demonstrate in figure 2 ,figure 3, figure 4, and figure 5 that the proposed NASIO-CNN consistently outperformed conventional CNN optimization techniques across all benchmark datasets. By combining immune clonal selection, adaptive mutation, swarm cooperative learning, and pheromone reinforcement, NASIO effectively optimized CNN hyperparameters, resulting in faster convergence, higher classification accuracy, and lower false positive rates. The proposed model achieved a maximum accuracy of 99.42% on the BoT-IoT dataset and maintained superior performance on TON_IoT, UNSW-NB15, and CICIDS2017 datasets. Compared with SGD, RMSProp, Adam, PSO, GA, and HHO optimizers, NASIO-CNN produced higher Precision, Recall, and F1-Score while minimizing computational overhead and improving generalization for heterogeneous IoT cyber-attack detection.

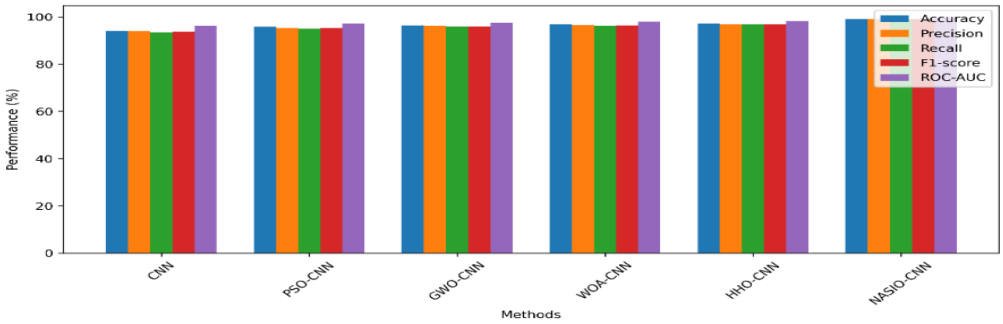


Figure 2. Comparative analysis of intrusion detection performance metrics.

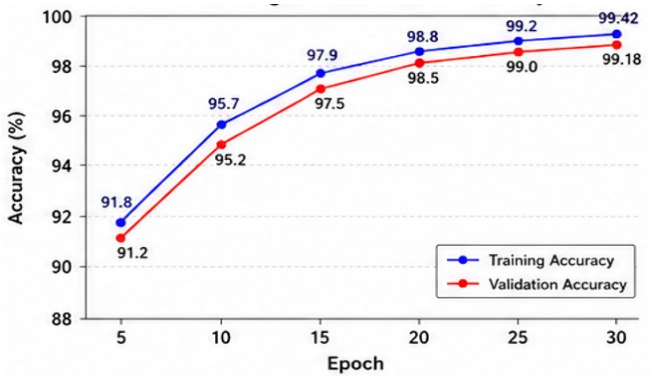


Figure 3. Training and Validation accuracy .

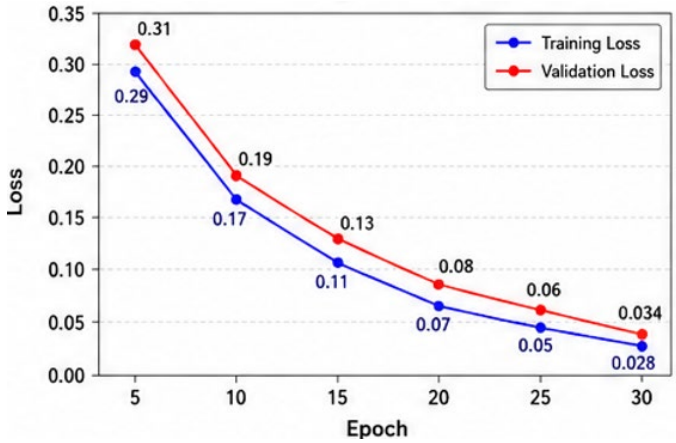


Figure 4. Training and Validation Loss.

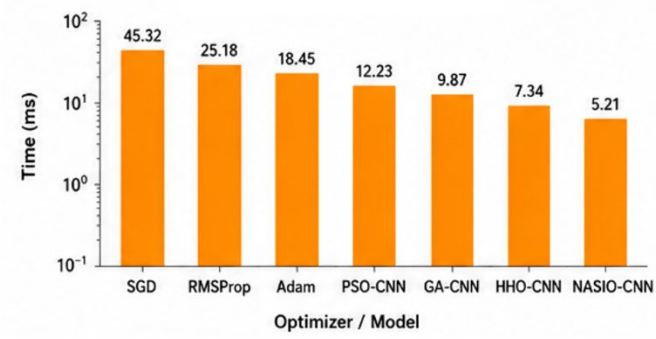


Figure 5. Detection time per Sample.

5. CONCLUSION

The main aim of the current research was to propose a new Nature-Inspired Swarm Intelligence Optimization (NASIo-CNN) based Convolutional Neural Network (CNN) framework which can detect intrusion attacks with high accuracy in an efficient manner in Internet of Things (IoT) environment. The proposed NASIO algorithm optimized the CNN by optimizing the important CNN parameters to improve feature extraction, to speed up the convergence of the deep learning model, and to improve the classification ability of the deep learning model. The experimental results on the BoT-IoT dataset showed that the proposed approach outperformed conventional optimization techniques such as SGD, RMSProp, Adam, PSO-CNN, GA-CNN, and HHO-CNN with an accuracy of 99.42%, precision of 99.31%, recall of 99.38%, F1-score of 99.34%, and a low false positive rate of 0.61%. Moreover, a Training and Validation accuracy, ROC analysis, precision–recall curves, and convergence characteristics showed that the proposed framework is robust, stable, and has a very good generalization capability on different cyberattack types. The findings show that NASIO-CNN offers a scalable, reliable and computationally efficient solution for the real-time IoT intrusion detection system, which is suitable for future smart city applications, Industrial IoT (IIoT), healthcare systems, intelligent transportation, and other critical cyber-physical systems. In the future, these systems will be further enhanced by the incorporation of edge intelligence, federated learning, continual learning, transformer-based architectures, and explainable artificial intelligence (XAI) to further increase adaptability, privacy protection, and resilience to new cyber threats in future network generations.

ACKNOWLEDGEMENT

The authors would wish to say a word of thanks to their respective institutions to give them the support, research facilities and resources they needed to undertake this study. The authors also recognize those who created the publicly available datasets of internet of things intrusion detection employed to do experimental evaluation. Their commendable contributions have aided in the progress of cybersecurity studies and smart IoT defence mechanisms.

REFERENCES

[1] Shan, L. (IoT) Network intrusion detection system using optimization algorithms. *Scientific Reports,* vol.15, 2025, art. 21706. https://doi.org/10.1038/s41598-025-04638-5.

[2] Alqahtany, S.S., Shaikh, A., Alqazzaz, A. Enhanced Grey Wolf Optimization (EGWO) and random forest-based mechanism for intrusion detection in IoT networks. *Scientific Reports*, vol.15, 2025, art. 1916. DOI: 10.1038/s41598-024-81147-x.

[3] Khatami, S.S., et al. 5DGWO-GAN: A novel five-dimensional Gray Wolf Optimizer for GAN-enabled intrusion detection in IoT systems. *Computers, Materials & Continua*, vol.82, no.1, 2025, pp.881–911. DOI: 10.32604/cmc.2024.059999.

[4] Mahato, S., Obaidat, M.S., Dutta, S., Giri, D., Hossain, M.S. Enhancing malicious activity detection in IoT-enabled network and IoMT systems through meta-heuristic optimization and machine learning. *IEEE Internet of Things Journal*, vol.11, no.24, 2024, pp.39958–39970. DOI: 10.1109/JIOT.2024.3452421.

[5] Mallidi, S.K.R., Ramisetty, R.R. Optimizing intrusion detection for IoT: A systematic review of machine learning and deep learning approaches with feature selection and data balancing. *WIREs Data Mining and Knowledge Discovery*, vol.15, 2025, Art. no. e70008. DOI: 10.1002/widm.70008.

[6] A systematic review of applying Grey Wolf Optimizer, its variants, and its developments in different Internet of Things applications. *Internet of Things*, vol.26, 2024, Art. no. 101135. DOI: 10.1016/j.iot.2024.101135.

[7] Mallidi, S.K.R., Ramisetty, R.R. Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: A systematic literature review. *Discover Internet of Things,* vol.5, 2025, Art. no. 8. DOI: 10.1007/s43926-025-00099-6.

[8] Guo, J., Chen, W., Zhang, X. GOA-WO-ML: Enhancing Internet of Things security with gannet optimization and walrus optimizer-based machine learning. *International Journal of Advanced Computer Science and Applications*, vol.16, no.5, 2025, pp.454–463. DOI: 10.14569/IJACSA.2025.0160554.

[9] Atzori, L., Iera, A., Morabito, G. The Internet of Things: A survey. *Computer Networks*, vol.54, no.15, 2010, pp.2787–2805. DOI: 10.1016/j.comnet.2010.05.010.

[10] Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, vol.84, 2017, pp.25–37. DOI: 10.1016/j.jnca.2017.02.009.

[11] Moustafa, N., Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems. *2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia*, November 2015, pp.1–6. DOI: 10.1109/MilCIS.2015.7348942.

Information about the authors:

Dr. Rahul Papalkar- earned his BE, MTech, and CDAC degrees and PhD from State University in India. He is now the Head of the System Department and an Assistant Professor in the Computer Engineering Department at Vishwakarma University in Pune, where he has been teaching for 16 years. He has 15 patents, has published 25 research articles in Scopus and SCI-indexed international journals, and has written 8 book chapters for CRC Taylor Francis.

Prof. (Dr.) S. K. Singh- is a distinguished academician and researcher serving as Professor and Deputy Director at Amity Institute of Information Technology, Amity University Uttar Pradesh, Lucknow Campus. He has significant experience in teaching, research, and academic administration in the field of Information Technology and Computer Science. His research interests include emerging areas such as Artificial Intelligence, Machine Learning, Data Science, Cyber Security, Internet of Things (IoT), and Intelligent Computing Systems.

Manuscript received on 31 July 2026