Implementation of meta-heuristic and deep learning algorithms for power system cybersecurity

Baddu Naik Bhukya[1], Samanthaka Mani Kuchibhatla[2], Naresh Kumar Bhagavatham[3], Tirumalasetti Lakshmi Narayana[4], Madhava Rao Chunduru[5], Balakrishnan Koustubha Madhavi[6]
[1]Department of Electrical and Electronics Engineering, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, India
[2]Department of Electrical and Electronics Engineering, ACE Engineering College, Hyderabad, India
[3]Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Hyderabad, India
[4]Department of Electrical and Electronics Engineering, Aditya University, Surampalem, India
[5]Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Guntur, India
[6]Department of Information Technology, Vardhaman College of Engineering, Shamshabad, India

Article Info

Article history:

Received Apr 8, 2024
Revised Oct 2, 2025
Accepted Dec 6, 2025

Keywords:

Artificial neural networks
Convolutional neural networks
Cyber security
Deep learning
Meta-heuristic algorithms
Power systems
Support vector machines

ABSTRACT

Power system cyber security is crucial due to their criticality. Cybersecurity is essential to protect vital infrastructure as power systems digitize. Meta-heuristic and deep learning techniques are used to improve power system cyber security in this paper. To evaluate their performance, the suggested approach is compared to traditional supervised machine learning algorithms including artificial neural networks (ANNs), convolutional neural networks (CNNs), and support vector machines (SVMs). The technique optimizes deep learning model hyper parameters and architectures to detect cyber risks. Cyberattacks on power systems can cause service outages and cascading failures with extensive social implications. Meta-heuristic and deep learning algorithms are integrated to improve power system cyber security in this study. Deep learning is good at pattern recognition and anomaly detection, while meta-heuristic algorithms optimize efficiently. A complete threat detection and mitigation strategy is proposed by merging these methodologies. The proposed methodology tests classic supervised machine learning algorithms such ANNs, CNNs, and SVMs. Simulations showed the algorithm worked better. It beat competition in accuracy, precision, recall, and F1-score.

Corresponding Author:

Baddu Naik Bhukya
Department of Electrical and Electronics Engineering, Prasad V Potluri Siddhartha Institute of Technology
Vijayawada, Andhra Pradesh, India
Email: baddunaik@gmail.com

1. INTRODUCTION

Integrating information and communication technology into power networks has transformed electricity generation, transmission, and distribution. These advances have many benefits, but they also make us vulnerable to cyberattacks. Malicious actors target power system infrastructures to disrupt services, ruin the economy, or risk people. Thus, protecting power systems from cyberattacks is essential for their reliability and security [1]. Information and communication technology has changed power systems. These improvements have improved power generation, transmission, and distribution efficiency, dependability, and flexibility, but they have also raised cyber security concerns. Due to power grids' growing reliance on interconnected digital systems, cyberattacks endanger energy supply chain stability [2]. Power outages and blackouts caused by cyberattacks can have major economic and societal consequences. These attacks can jeopardize critical infrastructure integrity, availability, and confidentiality by exploiting control, communication, and data management system flaws. Thus, utilities, regulators, and governments worldwide emphasize power system cyber security [3]. Power system cyber security uses rule-based, intrusion, and anomaly detection. Traditional security measures cannot detect and neutralize cyber breaches in real time in modern power systems [4]. Meta-heuristic algorithms and deep learning models improve power system cyber security to solve these issues. Using evolutionary algorithms, particle swarm optimization (PSO), and simulated annealing (SA), intrusion detection, vulnerability assessment, and resource allocation can be optimized. These algorithms find near-optimal results in large search areas, making them ideal for dynamic and uncertain power system cyber threats [5]. Deep learning is good at pattern recognition, anomaly detection, and domain-wide categorization. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) detect complicated cyber-attack patterns in power system data streams. Deep learning algorithms trained on massive data sets can acquire comprehensive representations of normal and harmful behavior to identify novel and sophisticated cyber threats [6]. Restricted Boltzmann machines (RBMs) improve natural-inspired artificial root foraging optimization. The RBM and natural-inspired artificial root foraging optimization can help smart grid intrusion detection and categorization. RBMs learn unsupervised from unlabeled data. This tech may create a multi-dataset learning system. This may help with minimal annotated data [7]. This work increases power system cyber security with meta-heuristics and deep learning. These computational approaches can detect threats, assess vulnerabilities, and develop adaptive security strategies. The study discusses literature, methods, advantages and cons, and case studies and experiments to verify the strategy works. This research improves cyber security to defend vital infrastructure and power systems from new cyberattacks.

Due to critical infrastructure digitization and interconnection, academics and industry study power system cyber security. A comprehensive literature evaluation covers traditional power system cyber security and revolutionary meta-heuristic and deep learning algorithms [8]. Intrusion, anomaly, and rule-based power system cyber security dominate. Rule-based methods use signatures and patterns to detect cyber hazards. Rule-based methods can detect well-defined attacks but not unique or complicated threats that deviate from patterns [9]. Intrusion detection system (IDS) checks network traffic and system operations for malicious activities and unauthorized access. Signature-based IDS look for attack signatures in network packets or system logs, while anomaly-based IDS use statistical models or machine learning algorithms to detect anomalous behavior. Anomaly-based IDS may have high false positives and low scalability in large power systems [10]. Meta-heuristic algorithms' near-optimal findings and vast search area help cyber security. Many cyber security applications use Georgia, PSO, SA, and ant colony optimization (ACO) meta-heuristics [11]. For intrusion detection, resource allocation, and cryptographic key generation, power system cyber security uses meta-heuristic algorithms. GA-based intrusion detection enhances accuracy, while PSO dynamic resource allocation reduces denial of service (DoS). CNNs and RNNs spot power system and cyber anomalies. CNNs scan network traffic and power grid satellite images for cyber security. RNNs infer temporal dependencies from sequential power system sensor and control device time-series data [12]. Deep learning algorithms recognized power system data stream intrusions, exfiltration, and malware distribution recently. Deep learning learns complex cyber threat patterns using large labeled datasets and powerful neural network topologies [13]. Deep learning and meta-heuristics may help power system cyberdefense. Meta-heuristic methods improve deep learning model hyperparameters like learning rates, regularization parameters, and network designs. Deep learning helps meta-heuristic computers adapt to complex cyber threats by improving feature representation and pattern identification [14]. Numerous research uses meta-heuristic and deep learning algorithms for intrusion detection, malware analysis, and vulnerability assessment. Genetic programming-based feature selection for deep learning models and PSO-based hyperparameter optimization for CNNs improve power system data cyber threat detection [15]. Cybersecurity protects power systems from threats but not sophisticated attackers. Deep learning detects abnormalities; meta-heuristic algorithms optimize. Combining computations boosts power system security. Integrate meta-heuristic and deep learning methods to study power system cyber security innovations and issues [16]. The literature review covers power system security. Most systems catch power system data fraud. To predict its anomalous response to deceptive input, the system's usual behavior was analyzed. Using feature-based analysis, deep learning and machine learning algorithms predict accurately. Metaheuristics-based feature optimization evaluates deep learning-based smart grid supervisory control and data acquisition (SCADA) security vulnerability identification.

2. METHOD

Meta-heuristic algorithms are effective optimization methods for complicated and dynamic cyber security situations. In power systems, where essential infrastructure reliability and security are paramount, meta-heuristic algorithms provide efficient threat detection, vulnerability assessment, and resource allocation. This section discusses meta-heuristic algorithms and their use in cyber security, followed by traditional supervised machine learning algorithms like artificial neural networks (ANNs), CNNs, and support vector machines (SVMs) [17]. Meta-heuristic algorithms optimize using natural or human behavior. These algorithms iteratively search solution spaces for complex problem near-optimal solutions. Genetic algorithms, PSO, SA, ACO, and evolutionary techniques are meta-heuristics [18]. Cyber security uses meta-heuristic methods to optimize IDS parameters, generate cryptographic keys, and allocate network defense resources. These algorithms are flexible, scalable, and adaptable to changing situations, making them ideal for power system cyber threats [19].

ANN structure and function mimic biological brain networks. Weighted connections spread information and learn from training data to improve prediction. Cybersecurity employs ANNs for intrusion, malware, and anomaly detection. ANNs learn complicated data patterns and correlations to detect advanced cyber threats. Overfitting, vanishing gradients, and huge labeled training data can harm ANNs [20]. Photos and time-series signals are grid-like data for CNNs. CNN layers are completely linked, pooling, and convolutional. CNNs learn spatial patterns by hierarchically extracting input data features. CNNs detect dangers in network traffic visualizations and surveillance camera recordings. Spatial patterns and local data linkages help CNNs spot visual anomalies and criminal activities. CNN training and inference may need huge labeled data and processing [21], [22]. SVMs are supervised classification and regression models. Data is classified by SVMs using the hyperplane with the highest margin. Kernels help SVMs handle high-dimensional data and nonlinear decisions. Cyber security uses SVMs for intrusion detection, malware classification, and network traffic analysis. Noise, sparsity, and high-dimensional data resistance allow SVMs to detect modest cyber threat patterns. SVMs need careful kernel function and regularization parameter selection for large datasets [23], [24]. RBMs neural networks replicate input probability distributions for unsupervised machine learning. Boltzmann Machines, stochastic generative models, model RBM complexity. RBMs have visible and buried neurons. Neurons in one layer are fully connected to those in the next but not each other. RBMs are "restricted" to simplify computation and enhance training efficiency, unlike Boltzmann Machines. Energy functions provide RBM energy values to visible and concealed unit configurations. Model parameters (weights, biases) and visible and hidden unit states affect energy function. The Boltzmann distribution models RBMs' visible and hidden unit probability distributions with higher probabilities for lower energy configurations. Contrastive divergence (CD) (training algorithm for RBM) educates RBMs. To close the RBM data distribution gap, network weights and biases are modified during training [25]. CD is suitable for large dataset RBM training since it approximates the log-likelihood function gradient. RBMs may learn hierarchical input feature representations and complex data linkages. AI and machine learning model probability distributions and create samples using RBMs. Artificial root foraging enhances power system sensor and data transmitter data. Internet of things (IoT) voltage and power sensors alert the base station to power concerns. Receivers build databases from data. The base station must examine all data for errors and missing data before building the dataset. Database storage may be reduced by providing data during dataset generation. Figure 1 shows the workflow of the proposed model.

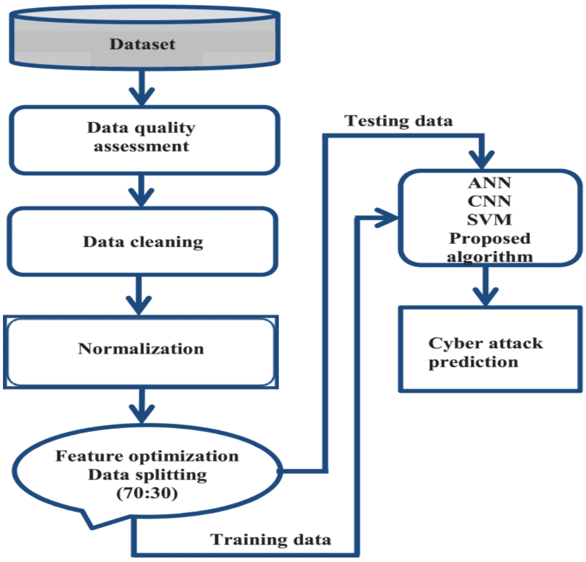

Figure 1. The workflow of the proposed model

The dataset has binary, three, and multi classes. The collection contains 15 sets of data on 37 power issue areas. Figure 2 shows the IEEE four-bus three-generator system converted to two-line transmission. The analysis test framework architecture is given. Although small, this system integrates the core notions of the power structure and is easy to understand. This work suggests classifier-iterative power system component monitoring. Circuit breakers (Bk1–Bk4) are toggled by two generator types and four IEDs, relays (R1–R4). Combining meta-heuristic algorithms and classical machine learning algorithms like ANNs, CNNs, and SVMs in cyber security professions is becoming increasingly common. Meta-heuristic algorithms optimize parameters and structures to increase machine learning model performance, durability, and efficiency. Traditional machine learning methods can define and categorize data to better meta-heuristic cyber threat detection. Meta-heuristic algorithms improve power system cyber security, while ANNs, CNNs, and SVMs classify patterns. Together, meta-heuristic and classical machine learning can increase power system cyber security. Novel approaches and practical obstacles in deploying integrated algorithms for real-world cyber security need further study. This paper uses Mississippi State University's Oak Ridge national laboratory's power system assault detection dataset. The dataset has binary, three, and multi-class categories. One dataset contains 15 sets of data from 37 power system occurrences. The data is CSV except for the multi-class dataset. Table 1 displays dataset content.

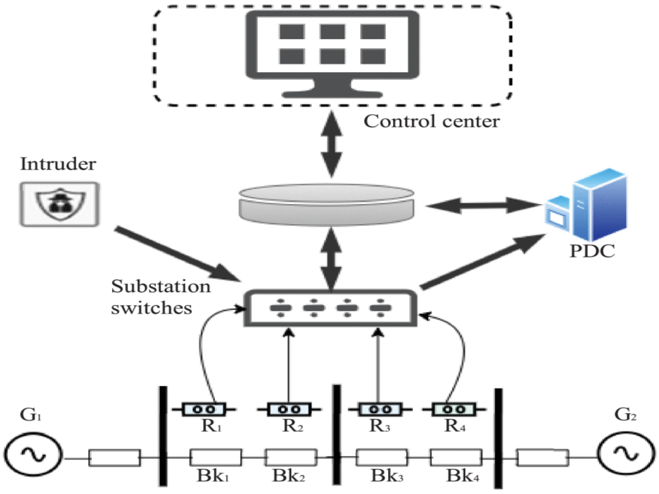

Figure 2. A brief description of the architecture of the power system

Table 1. Describes the dataset that was employed

Data class	Data details	Event count out
Binary classification	Natural event	9
	Attack event	28
Three classifications	No event	1
	Natural event	8
Multi class classification	Attack event	28
	All classes	37

3. RESULTS AND DISCUSSION

This section explains research results and provides a full commentary. Present results in figures, graphs, and tables for easy comprehension [14], [15]. Discussion can be divided into areas. This section compares traditional machine learning algorithms like ANNs, CNNs, and SVMs to the RBM augmented with an artificial root foraging optimization algorithm. Integration of meta-heuristic algorithms with regular machine learning techniques improves power system cyber security. Meta-heuristic optimization methods like genetic algorithms and PSO improve deep learning model accuracy, resilience, and scalability. The integrated strategy enhances adaptability and reactivity to shifting threat landscapes and system conditions. Integrating real-time threat intelligence and system status information into defense plans allows proactive threat identification and rapid response, reducing the impact of cyber-attacks on power grid operations. A single dataset was created from 15 sets of data from 37 power system event categories. In this study, 70% of the data is for training and 30% for testing. Figures 3-6 show the verified algorithms' F1-score, accuracy, precision, recall, and recall. Figure 3 shows the validated algorithms' accuracy from all three experiments.

Except for the ANN algorithm in the three-class classification experiment, the binary classification methods consistently outperformed the other two. The ANN algorithm performed somewhat better in the three-class classification experiment than the binary and multi-class studies.

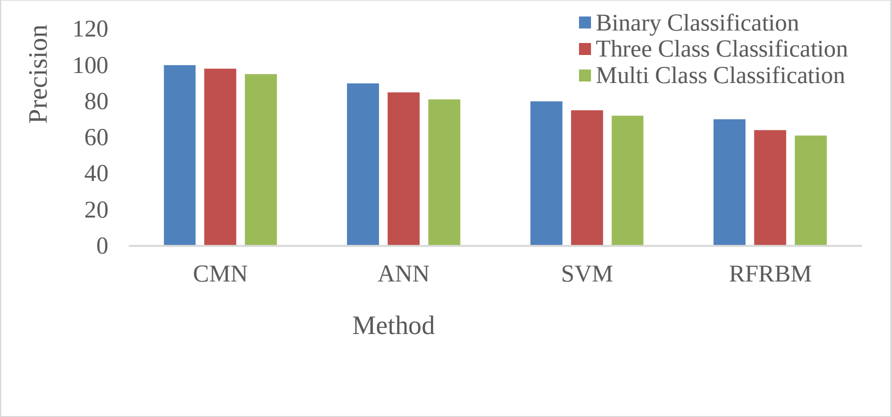

Figure 3. The precision of the investigations performed

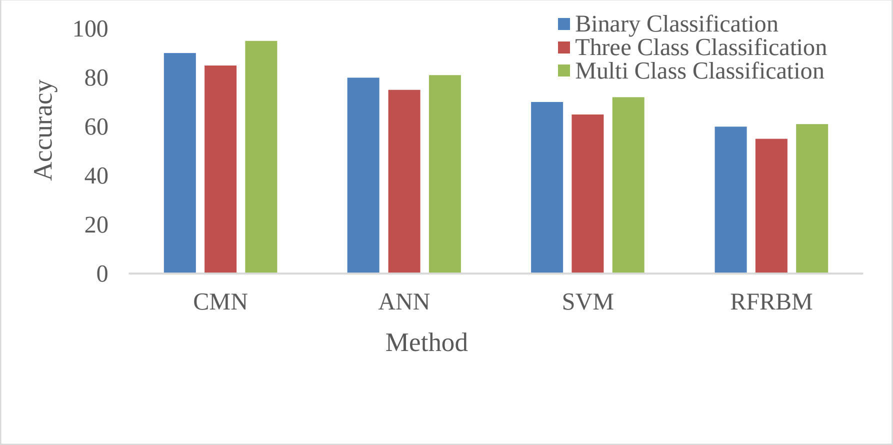

Figure 4. The accuracy of the experiments performed

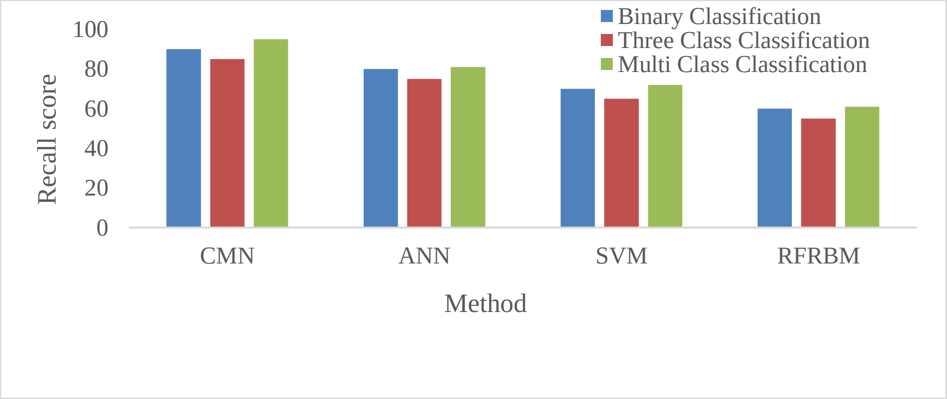

Figure 5. The recall score for the investigations that were conducted

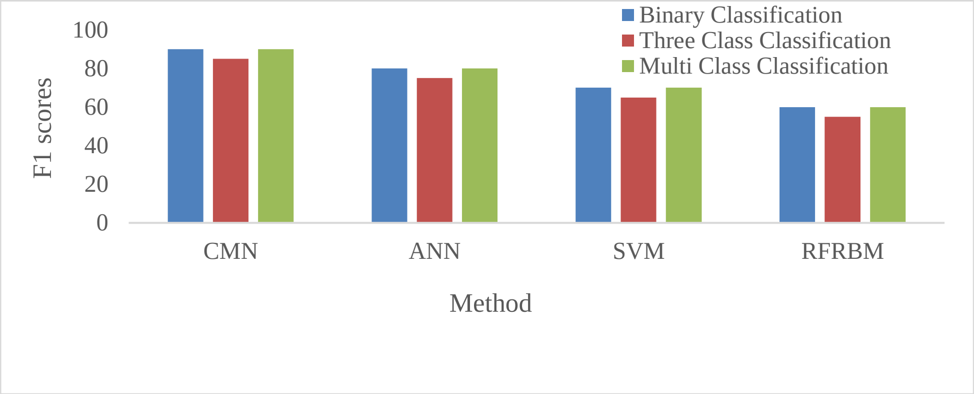

Figure 6. Illustrates the F1-score of the investigations performed

Figure 4 shows that the multi-class classification experiment was more precise than the three-class trial, but only the ANN method. These findings suggest that the ANN algorithm may be more precise in multi-class classification jobs. The CNN and SVM algorithms did not improve the multi-class classification experiment. Figure 5 shows that the ANN and SVM algorithms performed better in three-class classification than the other two experiments. The suggested random forest–restricted Boltzmann machine (RF-RBM) improves binary classification experiments due to the extraordinarily high sample counts for either class. The three-class classification experiment performs poorly due to the large fall in data for the no-event class, which creates an uneven distribution. In every experiment except the proposed RF-RBM, the three-class classification yields better F1-score estimations, as shown in Figure 6. The suggested algorithm outperforms the other three algorithms in three-class and multi-class classification, but it excels in binary classification. The results and discussions emphasize the need of merging meta-heuristic and classical supervised machine learning techniques in power system cyber security. The integrated strategy addresses developing cyber threats and vulnerabilities in a holistic and adaptable manner, providing critical infrastructure stability and security in the face of more sophisticated attacks. Further research and development should refine and enhance integrated algorithms to handle power system cyber security concerns and requirements. Moreover, we assess the findings of this study by comparing them to the outcomes of similar studies that utilized the identical dataset. The Table 2 displays the three-class classification dataset comparison.

Table 2. Three-class classification dataset model comparison

Model	Accuracy	Precision	Recall	F1-score
SVM-ACO	77	79.6	76.3	NA
GA-RBF SVM	89.1	88.8	90.8	84.7
PSO-SVM	84.8	85.9	82.8	NA
Proposed RF-RBM	93.4	94.2	91.3	89.5

4. CONCLUSION

Cyber security in power systems is crucial for critical infrastructure reliability and security. This study examines the integration of meta-heuristic algorithms with typical supervised machine learning methods like ANNs, CNNs, and SVMs to improve power system cyber security. This work offers a limited Boltzmann machine approach inspired by nature to identify and categorize smart grid system assaults. Artificial root forage optimization is based on biological root growth optimization. The artificial root foraging algorithm was used to fine-tune dataset features before the neural network algorithm to demonstrate optimization. The experimental investigation compared the proposed RF-RBM method to three leading neural network algorithms. The study included binary, three-class, and multi-class classification. The algorithm RF-RBM is best at detecting and categorizing power system cyberattacks, according to experiments. The algorithm's strong F1-score, good recall, precision, and accuracy demonstrate this. Using meta-heuristic and standard machine learning algorithms to improve power system cyber security seems promising. Integrating optimization and pattern recognition approaches provides a holistic and adaptable response to cyber threats and vulnerabilities. Further research and development should refine integrated algorithms, handle practical obstacles, and deploy effective cyber security solutions to protect power system essential infrastructure. The experimental study compares the proposed RF-RBM method against three cutting-edge neural network algorithms in classification. The trials show that RF-RBM is excellent for cyberattack detection and classification in smart grid SCADA systems. The suggested algorithm has high F1-score, good accuracy, precision, and recall.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to their respective institutions for providing the necessary facilities, technical support, and encouragement to carry out this research work. We also acknowledge the valuable guidance, constructive suggestions, and insightful comments from our colleagues and reviewers, which significantly helped in improving the quality of this paper.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

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
Baddu Naik Bhukya	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Samanthaka Mani Kuchibhatla	✓	✓				✓		✓	✓	✓	✓	✓		✓
Naresh Kumar Bhagavatham	✓		✓	✓			✓			✓	✓		✓	
Tirumalasetti Lakshmi Narayana	✓	✓				✓		✓	✓	✓	✓	✓		
Madhava Rao Chunduru	✓	✓				✓		✓	✓	✓	✓	✓		
Balakrishnan Koustubha Madhavi	✓	✓				✓		✓	✓	✓	✓	✓		

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

The authors declare that there is no conflict of interest regarding the publication of this paper.

DATA AVAILABILITY

The datasets generated and/or analyzed during the current study are not publicly available due to organizational policy, but are available from the corresponding author on reasonable request.

REFERENCES

[1] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, "Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions," *Energies*, vol. 15, no. 18, pp. 1–37, Sep. 2022, doi: 10.3390/en15186799.

[2] O. M. Butt, M. Zulqarnain, and T. M. Butt, "Recent advancement in smart grid technology: Future prospects in the electrical power network," *Ain Shams Engineering Journal*, vol. 12, no. 1, pp. 687–695, 2021, doi: 10.1016/j.asej.2020.05.004.

[3] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, Apr. 2018, doi: 10.1016/j.compeleceng.2018.01.015.

[4] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," *Sensors*, vol. 23, no. 5, p. 2415, 2023, doi: 10.3390/s23052415.

[5] A. E. Ezugwu *et al.*, "Metaheuristics: a comprehensive overview and classification along with bibliometric analysis," *Artificial Intelligence Review*, vol. 54, no. 6, pp. 4237–4316, Aug. 2021, doi: 10.1007/s10462-020-09952-0.

[6] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review,"

Internet of Things and Cyber-Physical Systems, vol. 4, pp. 110–128, 2024, doi: 10.1016/j.iotcps.2023.09.003.

[7] X. S. Yang, "Nature-inspired optimization algorithms: Challenges and open problems," *Journal of Computational Science*, vol. 46, p. 101104, Oct. 2020, doi: 10.1016/j.jocs.2020.101104.

[8] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data and Information Management*, vol. 8, no. 2, 2024, doi: 10.1016/j.dim.2023.100063.

[9] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," *IEEE Access*, vol. 10, pp. 121173–121192, 2022, doi: 10.1109/ACCESS.2022.3220622.

[10] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[11] K. Rajwar, K. Deep, and S. Das, "An exhaustive review of the metaheuristic algorithms for search and optimization: taxonomy, applications, and open challenges," *Artificial Intelligence Review*, vol. 56, no. 11, pp. 13187–13257, Nov. 2023, doi: 10.1007/s10462-023-10470-y.

[12] Emad-ul-Haq Qazi, M. Imran, N. Haider, M. Shoaib, and I. Razzak, "An intelligent and efficient network intrusion detection system using deep learning," *Computers and Electrical Engineering*, vol. 99, 2022, doi: 10.1016/j.compeleceng.2022.107764.

[13] S. Wu *et al*., "Pelvic bone tumor segmentation fusion algorithm based on fully convolutional neural network and conditional random field," *Journal of Bone Oncology*, vol. 45, p. 100593, 2024, doi: 10.1016/j.jbo.2024.100593.

[14] A. I. A. Alzahrani, M. Ayadi, M. M. Asiri, A. Al-Rasheed, and A. Ksibi, "Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques," *Electronics*, vol. 11, no. 22, pp. 1–20, Nov. 2022, doi: 10.3390/electronics11223665.

[15] G. AL Mukhaini, M. Anbar, S. Manickam, T. A. Al-Amiedy, and A. Al Momani, "A systematic literature review of recent lightweight detection approaches leveraging machine and deep learning mechanisms in Internet of Things networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 1, pp. 1–36, 2024, doi: 10.1016/j.jksuci.2023.101866.

[16] S. Y. Diaba, M. Shafie-Khah, and M. Elmusrati, "Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms," *IEEE Access*, vol. 11, pp. 18660–18672, 2023, doi: 10.1109/ACCESS.2023.3247193.

[17] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.

[18] B. N. Bhukya, P. R. Chinda, S. R. Rayapudi, and S. R. Bondalapati, "Advanced Control with an Innovative Optimization Algorithm for Congestion Management in Power Transmission Networks," *Engineering Letters*, vol. 31, no. 1, pp. 194–205, 2023.

[19] A. M. Nassef, M. A. Abdelkareem, H. M. Maghrabie, and A. Baroutaji, "Review of Metaheuristic Optimization Algorithms for Power Systems Problems," *Sustainability (Switzerland)*, vol. 15, no. 12, pp. 1–27, 2023, doi: 10.3390/su15129434.

[20] S. M. Almufti, A. A. Shaban, Z. A. Ali, R. I. Ali, J. A. D. Fuente, and R. R. Asaad, "Overview of Metaheuristic Algorithms," *Polaris Global Journal of Scholarly Research and Trends*, vol. 2, no. 2, pp. 10–32, 2023, doi: 10.58429/pgjsrt.v2n2a144.

[21] A. Luz, A. Odu, and G. O. Olaoye, "Meta-heuristic Algorithms for Intrusion Detection," 2024, [Online]. Available: https://www.researchgate.net/publication/378434670_Meta-heuristic_Algorithms_for_Intrusion_Detection

[22] A. M. Alnasrawi, A. M. N. Alzubaidi, and A. A. Al-Moadhen, "Improving sentiment analysis using text network features within different machine learning algorithms," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 1, pp. 405–412, 2024, doi: ./eei.v13i1.5576.

[23] M. M. Taye, "Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions," *Computation*, vol. 11, no. 52, pp. 1–23, 2023, doi: 10.3390/computation11030052.

[24] M. Awad and R. Khanna, "Support Vector Machines for Classification," in *Efficient Learning Machines*, Berkeley, CA: Apress, 2015, pp. 39–66, doi: 10.1007/978-1-4302-5990-9_3.

[25] M. Probst, F. Rothlauf, and J. Grahl, "Scalability of using Restricted Boltzmann Machines for combinatorial optimization," *European Journal of Operational Research*, vol. 256, no. 2, pp. 368–383, Jan. 2017, doi: 10.1016/j.ejor.2016.06.066.

BIOGRAPHIES OF AUTHORS

Dr. Baddu Naik Bhukya is received the B.Tech. degree in Electrical and Electronics Engineering from Prasad V potluri Siddhartha Institute of Technology, Vijayawada, India and the M.Tech. and Ph.D. degrees in Electrical and Electronics Engineering with Power System Specialization from Jawaharlal Nehru Technological University Kakinada, India. Currently, he is an Assistant Professor in the Department of Electrical and Electronics Engineering, Prasad V potluri Siddhartha Institute of Technology, Vijayawada, India. His research interests include electrical power systems, optimization techniques, renewable energy sources, FACTS controllers, high voltage engineering, and artificial intelligence applied power system. He can be contacted at email: baddunaik@gmail.com.

Dr. Samanthaka Mani Kuchibhatla is Associate professor and HOD-EEE Department, ACE Engineering College, Hyderabad, India. She did her B.Tech. from JNTU Kakinada, M.Tech. from NIT Warangal and awarded Doctorate from JNTU Kakinada. She has several National and International Publications. She is a reviewer for several reputed journals. She is a Lifetime member of ISTE and IETE. Her areas of interest are power quality improvement using AI techniques, renewable energy sources, FACTS, PLC, and SCADA. She can be contacted at email: drsmanik21@gmail.com.

Dr. Naresh Kumar Bhagavatham is an Associate professor, Department of CSE, Vignana Bharathi Institute of Technology, Ghatkesar, Hyderabad. He received MCA from QIS engineering College Ongole India in 2009 and the M.Tech. in Computer Science Engineering from Lords Institute of Engineering and Technology Hyderabad India in 2011 and Ph.D. degree in computer science engineering from KL University in August 2024 Vijayawada, India. His research interests are computer networks, network security, image processing, software engineering, and cloud computing. He can be contacted at email: bhagavatham.nareshkumar@vbithyd.ac.in.

Mr. Tirumalasetti Lakshmi Narayana is Assistant Professor in the Department of Electrical and Electronics Engineering, Aditya University, Surampalem, Andhra Pradesh, India. He is currently pursuing Ph.D. at Jawaharalal Nehru Technological Univeristy, Kakinada, India. He completed M.Tech. at Jawaharalal Nehru Technological Univeristy, Kakinada. His areas of interest Include, power systems, state estimation, electric power distribution systems and electrical machines, and power electronics. He can be contacted at email: tlaxman17@gmail.com.

Dr. Madhava Rao Chunduru has been working as an Associate Professor of Computer Science and Engineering Department of Koneru Lakshmaiah Deemed to be University, Vaddeswaram, AP, India. He has twenty-four years of national experience in teaching at various disciplines. He has ten research papers. His areas of interests are machine learning, data science, IoT, and bioinformatics. He can be contacted at email: cmadhavarao@kluniversity.in.

Dr. Balakrishnan Koustubha Madhavi is a passionate academician currently working as an Associate Professor in the Department of Information Technology at Vardhaman College of Engineering, Hyderabad. She has a teaching experience of 19+ years in both international and national academic organizations. She has started her career as a lecturer in the School of Computing in INTI University College Sarawak, Malaysia, an Associate Campus of University of Wollongong, Australia. Her research interests are machine learning, deep learning, neural networks, and data mining. In addition, she has one granted Australian patent and several Indian Patents published to her credit. She has authored and edited several technical books on machine learning and C programming. She can be contacted at email: kousmadhu717@gmail.com.