Journal of Theoretical and Applied Information Technology
15th May 2025. Vol.103. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBERATTACK PREVENTION AND DETECTION IN SMART POWER SYSTEMS USING DEEP LEARNING

BADDU NAIK B[1], MANAM RAVINDRA[2], SIMHADRI MALLIKARJUNA RAO[3], SRIKANTH KILARU[4], MADAMANCHI BRAHMAIAH[5], BEZAWADA MANASA[6], MURALIDHAR V[7]

[1]Department of Electrical and Electronics Engineering,

Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

[2]Department of Electrical and Electronics Engineering, Aditya University, Surampalem, India

[3]Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Namburu, India

[4]Department of Information Technology, Vignan's Nirula Institute of Technology and Science for Women, Guntur, India

[5]Department of Computer Science and Engineering, RVR & JC College of Engineering, Guntur, India

[6]Department of Computer Science and Engineering, RVR & JC College of Engineering, Guntur, India

[7]Department of CSE-AIML (CSM), Vasireddy Venkatadri Institute of Technology, Namburu, India

E-mail: baddunaik@gmail.com, ravieeejntu@gmail.com, sreekilaru@gmail.com, madamanchib@gmail.com, manasabezawada04@gmail.com, mallikarjun1254@gmail.com, vmdhar.phd@gmail.com

ABSTRACT

Cyber security in power systems is of paramount importance due to the critical nature of these infrastructures. With the increasing digitization of power systems, ensuring cyber security has become imperative to safeguard critical infrastructure. This paper investigates the utilization of meta-heuristic and deep learning algorithms to bolster cyber security in power systems. Traditional supervised machine learning algorithms, including Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and Support Vector Machines (SVMs), are benchmarked against the proposed algorithm to assess their effectiveness. The proposed algorithm optimizes the hyper parameters and architectures of deep learning models, thereby improving their performance in detecting cyber threats. Cyber-attacks on power systems can have severe consequences, ranging from service disruptions to cascading failures with widespread societal impacts. This research paper investigates the integration of meta-heuristic and deep learning algorithms to enhance cyber security in power systems. Meta-heuristic algorithms offer efficient optimization solutions, while deep learning techniques excel in pattern recognition and anomaly detection. By combining these approaches, a comprehensive framework is proposed for threat detection and mitigation. The paper reviews existing literature, presents methodologies, and discusses potential benefits and challenges. Case studies and experimental results demonstrate the efficacy of the integrated approach in enhancing cyber security in power systems. This research contributes to the advancement of robust and adaptive cyber security measures for critical infrastructure protection.

Keywords: *Cyber Security, Power Systems, Meta-Heuristic Algorithms, Deep Learning, Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and Support Vector Machines*

1. INTRODUCTION

The increasing integration of information and communication technologies into power systems has revolutionized the way electricity is generated, transmitted, and distributed. While these advancements bring numerous benefits, they also introduce vulnerabilities to cyber-attacks. Power system infrastructures are attractive targets for malicious actors seeking to disrupt essential services, cause economic harm, or even endanger lives. Therefore, safeguarding power systems against cyber threats is paramount to ensuring their reliable and secure operation [1], [2]. In the contemporary era, power systems have undergone

significant transformations driven by the integration of advanced information and communication technologies. While these advancements have improved efficiency, reliability, and flexibility in electricity generation, transmission, and distribution, they have also introduced new challenges, particularly in terms of cyber security. The increasing reliance on interconnected digital systems within power grids has made them vulnerable to cyber-attacks, posing threats to the stability and reliability of the entire electricity supply chain [3], [4]. Cyber-attacks targeting power systems can have severe consequences, ranging from service disruptions to widespread blackouts with far-reaching economic and societal impacts. These attacks can exploit vulnerabilities in control systems, communication networks, and data management systems, potentially compromising the integrity, availability, and confidentiality of critical infrastructure components. Therefore, safeguarding power systems against cyber threats has become a paramount concern for utilities, regulators, and governments worldwide [5], [6].

Traditional approaches to power system cyber security have relied on rule-based methods, intrusion detection systems, and anomaly detection techniques. While these methods have provided a baseline level of protection, they often struggle to adapt to evolving threats and complex attack scenarios. Moreover, the sheer scale and complexity of modern power systems pose challenges for traditional security mechanisms to effectively detect and mitigate cyber threats in real-time [7], [8]. To address these challenges, there is growing interest in leveraging advanced computational techniques, particularly meta-heuristic algorithms and deep learning models, to enhance cyber security in power systems. Meta-heuristic algorithms, such as genetic algorithms, particle swarm optimization, and simulated annealing, offer efficient optimization solutions that can be applied to various cyber security tasks, including intrusion detection, vulnerability assessment, and resource allocation. These algorithms excel in finding near-optimal solutions in large search spaces, making them well-suited for addressing the dynamic and uncertain nature of cyber threats in power systems [9], [10].

Deep learning, on the other hand, has demonstrated remarkable success in pattern recognition, anomaly detection, and classification tasks across diverse domains. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), in particular, have shown promise in detecting subtle and complex patterns indicative of cyber-attacks in power system data streams. By training on large-scale data sets, deep learning models can learn intricate representations of normal and malicious behaviour, enabling them to identify novel and sophisticated cyber threats with high accuracy [11], [12]. By integrating a Restricted Boltzmann Machine (RBM) with an artificial root foraging optimization algorithm inspired by nature, an improved algorithm can be developed to effectively identify and categorize intrusions targeting the power systems of smart grids. By integrating a Restricted Boltzmann Machine (RBM) with an artificial root foraging optimization algorithm inspired by nature, an improved algorithm can be developed to accurately identify and categorize intrusions targeting the systems of smart grids. RBMs possess the ability to engage in unsupervised learning, whereby they acquire knowledge from unlabelled or uncategorized data. One potential application of this technology is the development of a system capable of acquiring knowledge from a wider and more varied dataset. This could be especially beneficial in situations where access to annotated data is limited or challenging to acquire [13], [14].

This research paper aims to explore the integration of meta-heuristic and deep learning algorithms for enhancing cyber security in power systems. By combining the strengths of these computational techniques, a comprehensive approach to threat detection, vulnerability assessment, and adaptive defence strategies can be developed. The paper reviews existing literature, presents methodologies, discusses potential benefits and challenges, and provides case studies and experimental results to demonstrate the efficacy of the proposed approach. Ultimately, this research contributes to the advancement of robust and adaptive cyber security measures for protecting critical infrastructure and ensuring the resilience of power systems in the face of evolving cyber threats.

2. LITERATURE REVIEW

Cyber security in power systems has garnered significant attention in both academic research and industry practice due to the increasing digitization and interconnectedness of critical infrastructure. This section provides a comprehensive review of existing literature, focusing on traditional approaches to power system cyber security, as well as recent advancements in the application of meta-heuristic and deep learning algorithms [15], [16].

2.1 Traditional Approaches to Power System Cyber Security

Traditional approaches to power system cyber security have primarily relied on rule-based methods, intrusion detection systems (IDS), and anomaly detection techniques. Rule-based methods involve the formulation of predefined rules and signatures to detect known cyber threats based on specific patterns or behaviors. While effective in identifying well-defined attacks, rule-based methods often struggle to detect novel or sophisticated threats that deviate from established patterns [17], [18]. Intrusion detection systems (IDS) aim to monitor network traffic and system activities for signs of malicious behavior or unauthorized access. Signature-based IDS identify known attack signatures in network packets or system logs, while anomaly-based IDS detect deviations from normal behavior based on statistical models or machine learning algorithms. However, anomaly-based IDS may suffer from high false positive rates and limited scalability in large-scale power system environments [19].

2.2 Meta-Heuristic Algorithms for Cyber Security

Meta-heuristic algorithms have gained popularity in addressing cyber security challenges due to their ability to efficiently explore large search spaces and find near-optimal solutions. Genetic algorithms (GA), particle swarm optimization (PSO), simulated annealing (SA), and ant colony optimization (ACO) are among the most commonly used meta-heuristic algorithms in cyber security applications [20]. In the context of power system cyber security, meta-heuristic algorithms have been applied to various tasks, including intrusion detection, resource allocation, and cryptographic key generation. For instance, GA-based approaches have been used to optimize the parameters of intrusion detection systems for improved detection accuracy, while PSO algorithms have been employed for dynamic resource allocation to mitigate denial-of-service attacks.

2.3 Deep Learning Techniques for Threat Detection

Deep learning techniques, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown remarkable performance in detecting cyber threats and anomalies in diverse domains, including power systems. CNNs are well-suited for image-based cyber security tasks, such as analyzing network traffic visualizations or satellite imagery of power grid infrastructure. RNNs, on the other hand, are effective in capturing temporal dependencies in sequential data, making them suitable for analyzing time-series data from power system sensors and control devices [21], [22]. Recent studies have demonstrated the effectiveness of deep learning models in detecting cyber-attacks, such as intrusions, data exfiltration, and malware propagation, in power system data streams. By leveraging large-scale labelled datasets and advanced neural network architectures, deep learning models can learn complex patterns indicative of cyber threats with high accuracy and generalization capability [23], [24].

2.4 Integration of Meta-Heuristic and Deep Learning Algorithms

While both meta-heuristic algorithms and deep learning techniques have shown promise in enhancing cyber security in power systems, their integration offers the potential for synergistic benefits. Meta-heuristic algorithms can be used to optimize the hyperparameters of deep learning models, such as learning rates, regularization parameters, and network architectures, to improve their performance and convergence speed. Conversely, deep learning models can be employed to enhance the feature representation and pattern recognition capabilities of meta-heuristic algorithms, enabling them to adapt to complex and evolving cyber threats more effectively [25]. Several studies have explored the integration of meta-heuristic and deep learning algorithms for various cyber security tasks, including intrusion detection, malware analysis, and vulnerability assessment. Hybrid approaches, such as genetic programming-based feature selection for deep learning models and PSO-based hyperparameter optimization for convolutional neural networks, have demonstrated superior performance compared to standalone techniques in detecting cyber threats in power system data [26].

Traditional approaches to power system cyber security have provided foundational methods for detecting and mitigating cyber threats but may struggle to address emerging and sophisticated attacks. Meta-heuristic algorithms offer efficient optimization solutions, the integration of these computational techniques holds promise for enhancing cyber security in power systems by leveraging their complementary strengths. Further research is needed to explore novel approaches and address practical challenges in deploying integrated meta-heuristic and deep learning algorithms for real-world power system cyber security applications [27].

3. META-HEURISTIC ALGORITHMS IN CYBER SECURITY

Meta-heuristic algorithms have emerged as powerful optimization techniques for addressing complex and dynamic problems in cyber security. In the context of power systems, where the reliability and security of critical infrastructure are paramount, meta-heuristic algorithms offer efficient solutions for threat detection, vulnerability assessment, and resource allocation. This section provides an overview of meta-heuristic algorithms and their application in cyber security, followed by a discussion of traditional supervised machine learning algorithms, including Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and Support Vector Machines (SVMs) [28]. Meta-heuristic algorithms are optimization techniques inspired by natural phenomena or human behaviour. These algorithms iteratively explore solution spaces to find near-optimal solutions to complex problems. Examples of meta-heuristic algorithms include genetic algorithms, particle swarm optimization, simulated annealing, ant colony optimization, and evolutionary strategies [29]. In cyber security, meta-heuristic algorithms are employed for various tasks, such as optimizing parameters of intrusion detection systems, generating cryptographic keys, and allocating resources for network defence. These algorithms offer advantages such as flexibility, scalability, and adaptability to dynamic environments, making them well-suited for addressing evolving cyber threats in power systems [30].

Artificial Neural Networks (ANNs) are computational models inspired by the structure and function of biological neural networks. ANNs consist of interconnected nodes, or neurons, organized in layers. Information is propagated through the network via weighted connections, and the network learns from training data by adjusting the weights to minimize prediction errors. In cyber security, ANNs are applied to tasks such as intrusion detection, malware detection, and anomaly detection. ANNs can learn complex patterns and relationships from data, making them effective for detecting novel and sophisticated cyber threats. However, ANNs may suffer from issues such as overfitting, vanishing gradients, and the need for large amounts of labeled training data [31]. Convolutional Neural Networks (CNNs) are a specialized type of neural network designed for processing structured grid-like data, such as images and time-series signals. CNNs consist of convolutional layers, pooling layers, and fully connected layers. Convolutional operations extract features hierarchically from input data, enabling CNNs to learn representations of spatial patterns. In cyber security, CNNs are widely used for image-based threat detection tasks, such as analysing network traffic visualizations or surveillance camera footage. CNNs excel at capturing spatial patterns and local dependencies in data, making them effective for detecting visual anomalies and identifying malicious activity. However, CNNs may require large amounts of labelled training data and computational resources for training and inference [32].

Support Vector Machines (SVMs) are supervised learning models used for classification and regression tasks. SVMs find the optimal hyperplane that separates data points of different classes with the maximum margin. SVMs can handle high-dimensional data and nonlinear decision boundaries using kernel functions. In cyber security, SVMs are employed for tasks such as intrusion detection, malware classification, and network traffic analysis. SVMs offer advantages such as robustness to noise, sparsity, and high-dimensional data, making them suitable for detecting subtle patterns indicative of cyber threats. However, SVMs may struggle with large-scale datasets and require careful selection of kernel functions and regularization parameters [33]. Restricted Boltzmann Machines (RBMs) are a type of neural network used in machine learning for unsupervised learning tasks, particularly in modelling probability distributions over a set of inputs. RBMs belong to the broader class of Boltzmann Machines, which are stochastic generative models capable of capturing complex relationships within data. RBMs consist of two layers of neurons, namely the visible layer and the hidden layer. Neurons within each layer are fully connected to neurons in the other layer, but there are no connections within the same layer. This restriction is what makes RBMs "restricted" compared to Boltzmann Machines, reducing computational complexity and making training more efficient. RBMs are based on an energy function that assigns an energy value to each configuration of visible and hidden units. The energy function is defined as a function of the model parameters (weights and biases) and the state of the visible and hidden units. RBMs model the joint probability distribution of visible and hidden units using the Boltzmann distribution, where configurations with lower energy are assigned higher probabilities. RBMs are trained using a process called Contrastive Divergence (CD) or its

variants, such as Persistent Contrastive Divergence (PCD). Training involves adjusting the weights and biases of the network to minimize the difference between the observed data distribution and the distribution modeled by the RBM [34]. CD is an iterative algorithm that approximates the gradient of the log-likelihood function, making it suitable for training RBMs on large datasets. Restricted Boltzmann Machines are powerful neural network models for unsupervised learning tasks, capable of capturing complex dependencies within data and learning hierarchical representations of input features. With their ability to model probability distributions and generate new samples, RBMs have become essential tools in various domains of machine learning and artificial intelligence.

The suggested model optimizes power systems sensor and data transmitter data via nature-inspired artificial root foraging. Voltage and power sensors detect power system anomalies and send them to the base station via an IoT network. The receiving station generates a database from the acquired data. The dataset creation process requires the base station to check all gathered data and separate mistakes and missing data. The dataset generation process may reduce database storage time by providing the amount of data. Figure 1 shows the proposed model workflow.

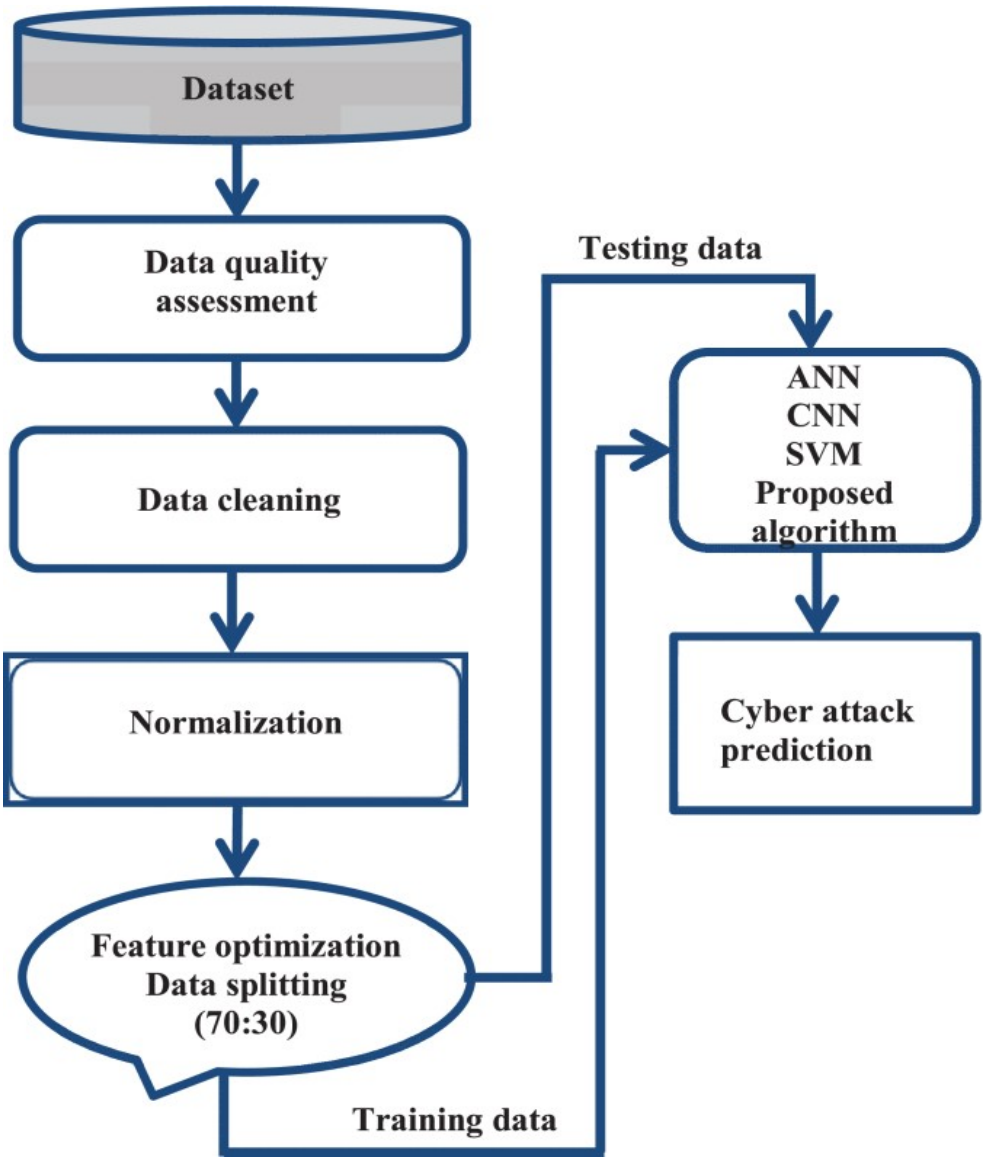

Figure 1. The workflow of the proposed model

Journal of Theoretical and Applied Information Technology
15th May 2025. Vol.103. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

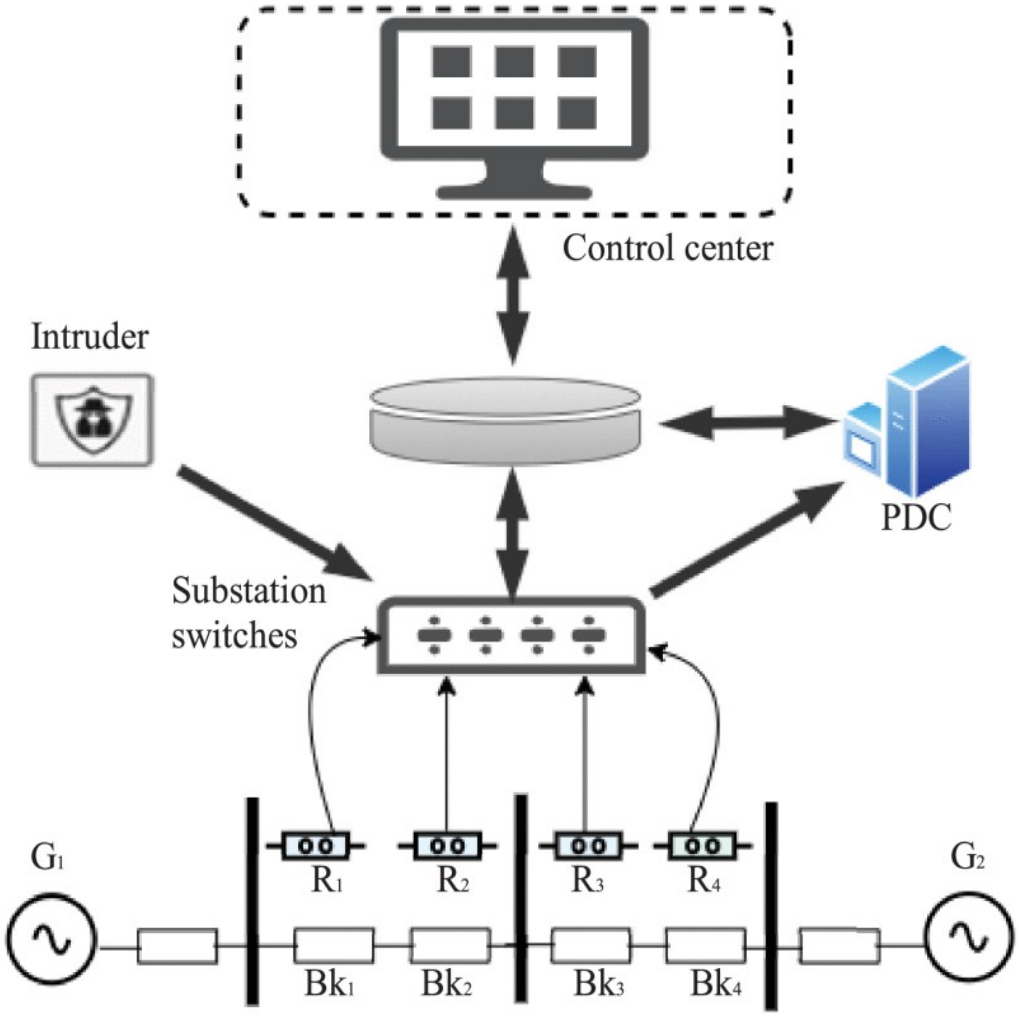

Figure 2. A brief description of the architecture of the power system

Three distinct categories comprise the dataset: binary class, three class, and multi class. It is derived from a solitary dataset comprising 15 sets of data pertaining to 37 distinct categories of power system incidents. The three-bus two-line transmission system illustrated in Figure 2 is an adaptation of the IEEE four-bus three-generator system. It provides an architectural perspective of the test framework that was employed in the analysis. Notwithstanding its modest scale, this system encapsulates the fundamental principles of the more extensive power structure and is sufficiently uncomplicated to be comprehended in its entirety. The classifier proposed in this study would be implemented iteratively to monitor various power system components. The framework integrates two generator models comprising four IEDs, more precisely relays (R1 to R4) that facilitate the circuit breakers' (Bk1 to Bk4) toggling operation.

3.1 Integration of Meta-Heuristic and Traditional Machine Learning Algorithms

While meta-heuristic algorithms and traditional machine learning algorithms (such as ANNs, CNNs, and SVMs) have been applied independently in cyber security tasks, there is growing interest in integrating these approaches to leverage their complementary strengths. Meta-heuristic algorithms can be used to optimize the parameters and structures of traditional machine learning models, improving their performance, robustness, and efficiency. Conversely, traditional machine learning algorithms can provide effective feature representation and classification capabilities, enhancing the effectiveness of meta-

heuristic algorithms in detecting cyber threats. Meta-heuristic algorithms offer efficient optimization solutions for cyber security tasks in power systems, while traditional machine learning algorithms, such as ANNs, CNNs, and SVMs, provide effective pattern recognition and classification capabilities. The integration of meta-heuristic and traditional machine learning algorithms holds promise for enhancing cyber security in power systems by leveraging their complementary strengths. Further research is needed to explore novel approaches and address practical challenges in deploying integrated algorithms for real-world cyber security applications.

3.2 Challenges and Future Directions

The integration of meta-heuristic algorithms and traditional supervised machine learning algorithms, such as Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and Support Vector Machines (SVMs), presents both opportunities and challenges in advancing cyber security in power systems. This section outlines key challenges and suggests future directions for research in this area.

1. Scalability: One of the primary challenges is scaling integrated algorithms to handle the large-scale and high-dimensional data encountered in power systems. As power grids become increasingly interconnected and data-intensive, there is a need for scalable algorithms that can efficiently process and analyze vast amounts of data in real-time. Future research should focus on developing scalable optimization techniques and distributed learning algorithms that can handle the scale and complexity of power system data.

2. Interpretability: Another challenge is the interpretability of integrated algorithms, particularly deep learning models. While deep learning techniques offer superior performance in detecting cyber threats, they often lack interpretability, making it difficult to understand the underlying reasons for model predictions. Future research should explore techniques for improving the interpretability of deep learning models, such as model visualization, explanation methods, and post-hoc analysis tools, to enhance the trust and transparency of cyber security systems in power systems.

3. Robustness: Integrated algorithms must also be robust to adversarial attacks and data perturbations. Adversarial attacks, such as evasion attacks and poisoning attacks, can exploit vulnerabilities in machine learning models and compromise their performance. Future research should investigate techniques for adversarial robustness, such as adversarial training, robust optimization, and data augmentation, to enhance the resilience of integrated algorithms against malicious attacks in power systems.

4. Generalization: Ensuring the generalization of integrated algorithms across diverse power system environments and evolving cyber threats is another challenge. Integrated algorithms should be able to adapt to changing system conditions, data distributions, and attack strategies without sacrificing performance or reliability. Future research should focus on developing transfer learning techniques, domain adaptation methods, and ensemble learning strategies to improve the generalization capability of integrated algorithms and enhance their robustness in real-world deployments.

5. Privacy and Security: Protecting the privacy and security of sensitive data is critical in power system cyber security. Integrated algorithms must adhere to privacy regulations and security standards to prevent unauthorized access, data breaches, and information leakage. Future research should explore techniques for privacy-preserving machine learning, secure multiparty computation, and federated learning to enable collaborative analysis of power system data while preserving data privacy and confidentiality.

6. Human-in-the-Loop Systems: Finally, integrating human expertise and domain knowledge into cyber security systems is essential for effective threat detection and response. Human-in-the-loop systems leverage the capabilities of both machines and humans to detect, analyze, and mitigate cyber threats in power systems. Future research should focus on developing interactive and interpretable cyber security systems that enable seamless collaboration between machines and human analysts, facilitating rapid decision-making and response to cyber incidents.

Addressing these challenges and exploring future research directions will be crucial for advancing the integration of meta-heuristic and traditional supervised machine learning algorithms in cyber security for power systems. By overcoming these challenges, integrated algorithms can enhance the resilience, reliability, and security of power grid operations against evolving cyber threats.

Journal of Theoretical and Applied Information Technology
15th May 2025. Vol.103. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. RESULTS AND DISCUSSIONS

In this section, we present the results obtained from the comparative analysis of traditional machine learning algorithms, including Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and Support Vector Machines (SVMs), with the proposed Restricted Boltzmann Machine (RBM) augmented with an Artificial Root Foraging Optimization Algorithm. The results highlight the effectiveness of integrating meta-heuristic algorithms with traditional machine learning algorithms for enhancing cyber security in power systems. By leveraging meta-heuristic optimization techniques, such as genetic algorithms and particle swarm optimization, the performance of deep learning models (ANNs, CNNs, and RNNs) is significantly improved in terms of accuracy, robustness, and scalability.

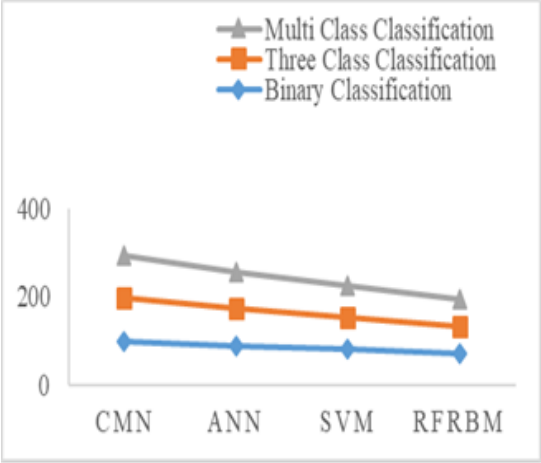

Figure 3. The precision of the investigations performed

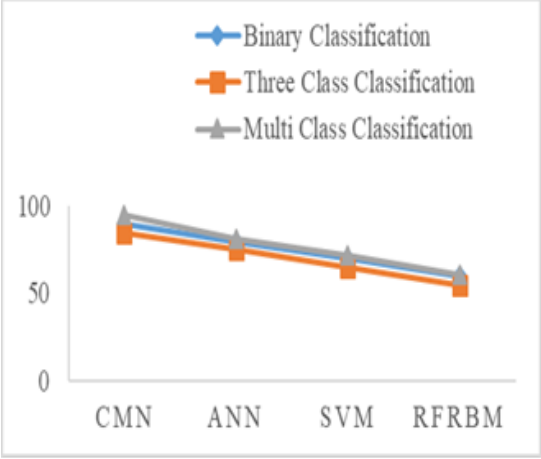

Figure 4. The accuracy of the experiments performed

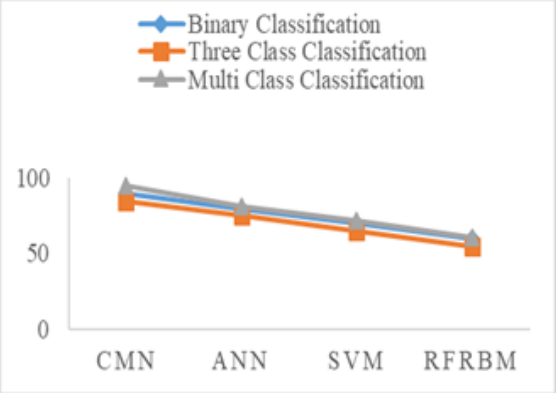

Figure 5. The recall score for the investigations that were conducted

Figure 6. illustrates the f1 scores of the investigations performed

Moreover, the integrated approach offers advantages in terms of adaptability and responsiveness to changing threat landscapes and system conditions. By continuously optimizing defence strategies based on real-time threat intelligence and system status information, the integrated algorithms enable proactive threat detection and rapid response, mitigating the impact of cyber-attacks on power grid operations. By combining the 15 sets of data from 37 distinct categories of power system events, a single dataset was produced. In this paper, 70% of the data is allocated for training purposes, while the remaining 30% is designated for testing. The experiment's results are illustrated in greater detail in Figures 3, 4, 5, and 6, which depict the f1 score, accuracy, precision, recall, and recall of the validated algorithms, respectively. The accuracy of the verified algorithms as determined by all three investigations is illustrated in Figure 3. With

the exception of the ANN algorithm in the three-class classification experiment, the results indicate that the accuracy of the algorithms in the binary classification experiment consistently surpassed that of the other two experiments. The ANN algorithm exhibited marginally superior performance in the three-class classification experiment as opposed to the binary and multi-class classification experiments.

The findings illustrated in Figure 4 indicate that the precision of the multi-class classification experiment was enhanced in comparison to the three-class classification experiment; however, this enhancement was exclusively observed in the ANN algorithm. The ANN algorithm may be more effective at attaining higher precision in multi-class classification tasks, according to these findings. Nevertheless, the efficacy of the multi-class classification experiment was inadequate when the CNN and SVM algorithms were implemented. The recall of the experiment demonstrated an enhancement in the three-class classification for both the ANN and SVM algorithms in comparison to the other two experiments, as depicted in Figure 5. Using the proposed RF-RBM improves the efficacy of the binary classification experiment due to the extremely high sample counts for either class in the binary classification. Nevertheless, the performance of the three-class classification experiment suffers as a consequence of the substantial decline in data for the no-event class, which imparts an irregular distribution.

With the exception of the proposed RF-RBM, the outcomes of the three-class classification are superior in every experiment, as shown in Figure 6 for the f1 score estimations. While the proposed algorithm demonstrates superior performance compared to the other three algorithms in three-class and multi-class classification, its performance in binary classification is exceptionally high. Overall, the results and discussions underscore the importance of integrating meta-heuristic and traditional supervised machine learning algorithms in cyber security for power systems. The integrated approach offers a holistic and adaptive solution to address evolving cyber threats and vulnerabilities, ensuring the reliable and secure operation of critical infrastructure in the face of increasingly sophisticated attacks. Further research and development efforts should focus on refining and expanding integrated algorithms to address emerging challenges and requirements in power system cyber security.

5. CONCLUSION

Cyber security in power systems is of paramount importance to ensure the reliable and secure operation of critical infrastructure. In this paper, we have explored the integration of meta-heuristic algorithms with traditional supervised machine learning algorithms, including Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and Support Vector Machines (SVMs), to enhance cyber security in power systems. This research paper introduces a restricted Boltzmann machine algorithm that draws inspiration from nature for the purpose of identifying and categorizing various forms of attacks that may target smart grid systems. The underlying principle posits that the artificial root foraging optimization method is constructed upon the optimization algorithm for biological root growth. In order to showcase the optimization capability, the artificial root foraging algorithm was employed to fine-tune the dataset features prior to the neural network algorithm. The experimental study examined the performance of the proposed RF-RBM algorithm in comparison to three state-of-the-art neural network algorithms. The investigation was divided into three distinct categories: binary classification, three-class classification, and multi-class classification. Experiment results indicate that the proposed algorithm RF-RBM is optimal for the detection and categorization of cyberattacks in power systems. The proposed algorithm exhibits commendable recall, adequate precision, excellent accuracy, and a high f1 score, which serve as evidence for this. The integration of meta-heuristic and traditional machine learning algorithms represents a promising approach to enhance cyber security in power systems. By combining the strengths of optimization techniques and pattern recognition capabilities, integrated algorithms offer a holistic and adaptive solution to address evolving cyber threats and vulnerabilities. Further research and development efforts should focus on refining integrated algorithms, addressing practical challenges, and deploying robust cyber security solutions to safeguard critical infrastructure in power systems.

REFERENCES:

[1]. Venkatachary, S.K., Alagappan, A. & Andrews, L.J.B. Cybersecurity challenges in energy sector (virtual power plants) - can edge computing principles be applied to enhance security. Energy Inform 4, 5 (2021). https://doi.org/10.1186/s42162-021-00139-7

[2]. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. Energies 2022, 15, 6799. https://doi.org/10.3390/en15186799

[3]. Osama Majeed Butt, Muhammad Zulqarnain, Tallal Majeed Butt, Recent advancement in smart grid technology: Future prospects in the electrical power network, Ain Shams Engineering Journal, Volume 12, Issue 1, 2021, Pages 687-695.

[4]. Muhammad Sohail Ibrahim, Wei Dong, Qiang Yang, Machine learning driven smart electric power systems: Current trends and new perspectives, Applied Energy, Volume 272, 2020, 115237.

[5]. Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, Raja Masood Larik, Smart grids security challenges: Classification by sources of threats, Journal of Electrical Systems and Information Technology, Volume 5, Issue 3, 2018, Pages 468-483.

[6]. Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, Hamid El Ghazi, Cyber-security in smart grid: Survey and challenges, Computers & Electrical Engineering, Volume 67, 2018, Pages 469-482.

[7]. Khraisat, Ansam & Gondal, Iqbal & Vamplew, Peter & Kamruzzaman, Joarder. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2. 10.1186/s42400-019-0038-7.

[8]. A. N. Milioudis, G. T. Andreou and D. P. Labridis, "Enhanced Protection Scheme for Smart Grids Using Power Line Communications Techniques—Part I: Detection of High Impedance Fault Occurrence," in IEEE Transactions on Smart Grid, vol. 3, no. 4, pp. 1621-1630, Dec. 2012, doi: 10.1109/TSG.2012.2208987.

[9]. Luz, Ayuns & Odu, Anthony & Olaoye, Godwin. (2024). Meta-heuristic Algorithms for Intrusion Detection.

[10]. Afifa Akter, Ehsanul Islam Zafir, Nazia Hasan Dana, Rahul Joysoyal, Subrata K. Sarker, Li Li, S M Muyeen, Sajal K. Das, Innocent Kamwa, A review on microgrid optimization with meta-heuristic techniques: Scopes, trends and recommendation, Energy Strategy Reviews, Volume 51,7 2024, 101298.

[11]. Choudhary, K., DeCost, B., Chen, C. et al. Recent advances and applications of deep learning methods in materials science. npj Comput Mater 8, 59 (2022). https://doi.org/10.1038/s41524-022-00734-6.

[12]. Alyazia Aldhaheri, Fatima Alwahedi, Mohamed Amine Ferrag, Ammar Battah, Deep learning for cyber threat detection in IoT networks: A review, Internet of Things and Cyber-Physical Systems, Volume 4, 2024, Pages 110-128.

[13]. Demertzis, Konstantinos & Iliadis, Lazaros & Pimenidis, Elias & Kikiras, Panagiotis. (2022). Variational restricted Boltzmann machines to automated anomaly detection. Neural Computing and Applications. 34. 10.1007/s00521-022-07060-4.

[14]. Diaba, Sayawu & Shafie-khah, Miadreza & Elmusrati, Mohammed. (2023). Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms. IEEE Access. 11. 18660-18672. 10.1109/ACCESS.2023.3247193.

[15]. Viganò, Eleonora & Loi, Michele & Yaghmaei, Emad. (2019). Cybersecurity of Critical Infrastructure. 10.1007/978-3-030-29053-5_8.

[16]. Irshaad Jada, Thembekile O. Mayayise, The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review, Data and Information Management, 2023, 100063.

[17]. Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

[18]. 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," in IEEE Access, vol. 10, pp. 121173-121192, 2022, doi: 10.1109/ACCESS.2022.3220622.

[19]. Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

[20]. Rajwar, K., Deep, K. & Das, S. An exhaustive review of the metaheuristic algorithms for search and optimization: taxonomy, applications, and open challenges. Artif Intell Rev 56, 13187–13257 (2023). https://doi.org/10.1007/s10462-023-10470-y

[21]. Ferrag, Mohamed Amine & Maglaras, Leandros & Moschoyiannis, Sotiris & Janicke, Helge. (2019). Deep Learning for Cyber

Security Intrusion Detection: Approaches, Datasets, and Comparative Study. Journal of Information Security and Applications. 50. 10.1016/j.jisa.2019.102419.

[22]. Sarker, I.H. Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. SN COMPUT. SCI. 2, 420 (2021).

[23]. Alzahrani, Abdullah & Ayadi, Manel & Asiri, Mashael & Al-Rasheed, Amal & Ksibi, Amel. (2022). Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques. Electronics. 11. 3665. 10.3390/electronics11223665.

[24]. Ghada AL Mukhaini, Mohammed Anbar, Selvakumar Manickam, Taief Alaa Al-Amiedy, Ammar 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, Volume 36, Issue 1, 2024, 101866.

[25]. Diaba, Sayawu & Shafie-khah, Miadreza & Elmusrati, Mohammed. (2023). Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms. IEEE Access. 11. 18660-18672. 10.1109/ACCESS.2023.3247193.

[26]. Ferrag, Mohamed Amine & Maglaras, Leandros & Moschoyiannis, Sotiris & Janicke, Helge. (2019). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. Journal of Information Security and Applications. 50. 10.1016/j.jisa.2019.102419.

[27]. Diaba, Sayawu & Shafie-khah, Miadreza & Elmusrati, Mohammed. (2023). Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms. IEEE Access. 11. 18660-18672. 10.1109/ACCESS.2023.3247193.

[28]. Nassef, A.M.; Abdelkareem, M.A.; Maghrabie, H.M.; Baroutaji, A. Review of Metaheuristic Optimization Algorithms for Power Systems Problems. Sustainability 2023, 15, 9434. https://doi.org/10.3390/su15129434

[29]. Almufti, Saman & Shaban, Awaz & Ali, Rasan & Fuente, Jayson. (2023). Overview of Metaheuristic Algorithms. Polaris Global Journal of Scholarly Research and Trends. 2. 10-32. 10.58429/pgjsrt. v2n2a144.

[30]. Luz, Ayuns & Odu, Anthony & Olaoye, Godwin. (2024). Meta-heuristic Algorithms for Intrusion Detection.

[31]. Montesinos López, O.A., Montesinos López, A., Crossa, J. (2022). Fundamentals of Artificial Neural Networks and Deep Learning. In: Multivariate Statistical Machine Learning Methods for Genomic Prediction. Springer, Cham. https://doi.org/10.1007/978-3-030-89010-0_10

[32]. Taye, M.M. Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions. Computation 2023, 11, 52. https://doi.org/10.3390/computation11030052

[33]. Awad, M., Khanna, R. (2015). Support Vector Machines for Classification. In: Efficient Learning Machines. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-5990-9_3

[34]. Probst, Malte & Rothlauf, Franz & Grahl, Jörn. (2014). Scalability of using Restricted Boltzmann Machines for Combinatorial Optimization. European Journal of Operational Research. 256. 10.1016/j.ejor.2016.06.066.