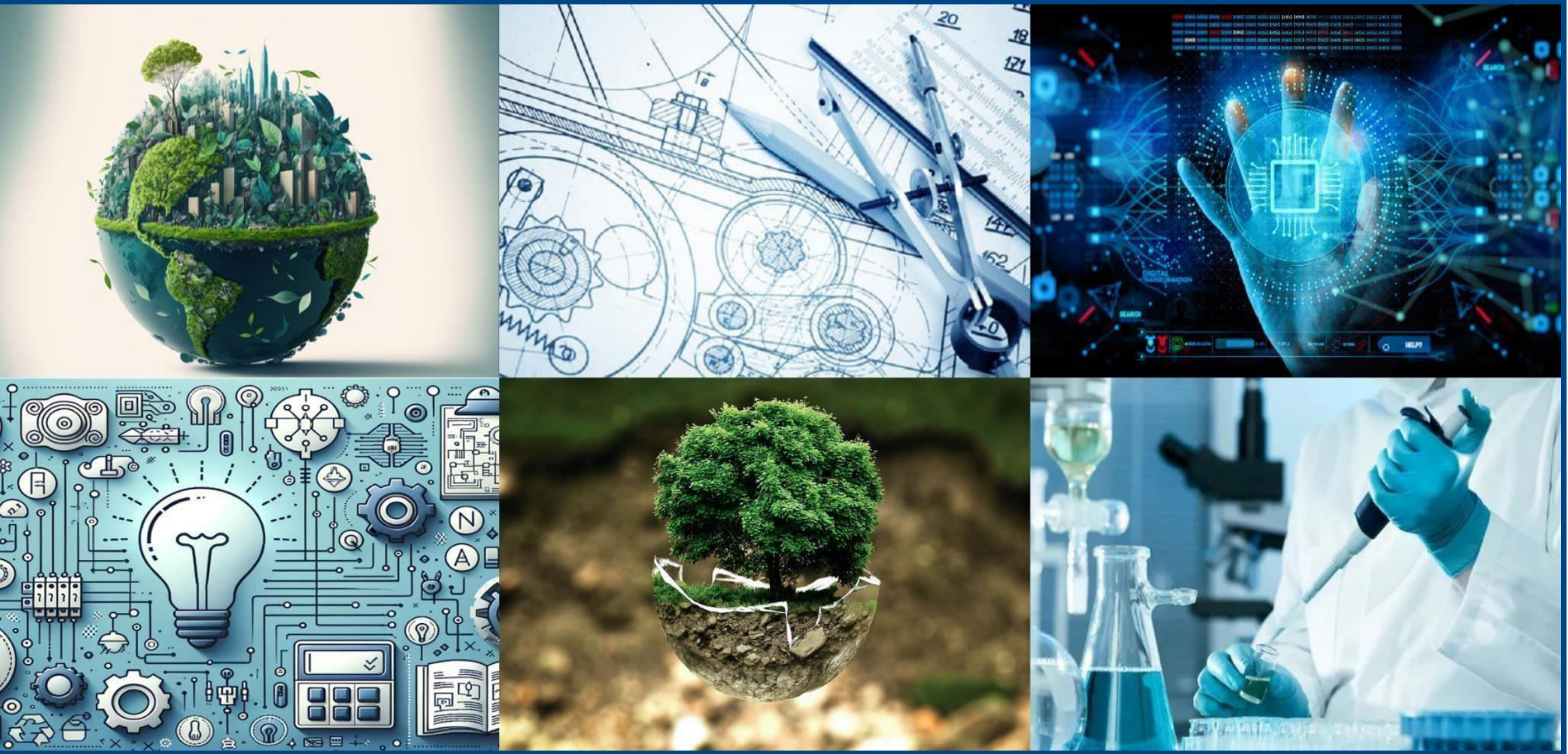
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

🌐 www.ijmrset.com ✉ ijmrset@gmail.com ☎ +91 6381 907 438 ☎ +91 63819 07438

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

CYBER SECURITY IN POWER SYSTEM USING META-HEURISTIC AND DEEP LEARNING ALGORITHMS

Dr. Vidya Pol, Shree Lakshmi A

Associate Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: The rapid digitalization of modern power systems has introduced significant vulnerabilities to cyber-attacks, , economic stability, and national security. Conventional cybersecurity approaches often struggle to detect sophisticated, evolving attack patterns in real time. This paper presents a hybrid methodology combining meta-heuristic optimization and deep learning algorithms to enhance cyber-attack detection and mitigation in power systems. A meta-heuristic algorithm is then applied for optimal feature selection, reducing dimensionality while retaining essential threat indicators. These optimized features are fed into a deep learning architecture—comprising Convolutional Neural Networks and Long Short-Term Memory layers—for accurate classification of attack types, including false data injection, denial of service, and load-altering events. Experimental evaluations using benchmark smart grid datasets demonstrate improved detection accuracy, faster response time, and reduced false positives compared to conventional methods. This integrated approach offers a scalable and adaptive solution for securing modern power systems against emerging cyber threats.

KEYWORDS: Cybersecurity,Power Systems, Deep Learning, SCADA Security, Smart Grid, Intrusion Detection, Feature Selection, CNN-LSTM, False Data Injection.

I. INTRODUCTION

The rapid modernization of power systems, driven by the integration of digital control, monitoring, and communication technologies, has ushered in the era of the smart grid. While these advancements have enhanced operational efficiency, fault tolerance, and automation, they have simultaneously introduced significant cybersecurity vulnerabilities. Cyber-attacks targeting Supervisory Control and Data Acquisition (SCADA) systems, Intelligent Electronic Devices (IEDs), and other critical components can compromise system integrity, disrupt power delivery, and cause widespread socio-economic consequences. Incidents such as false data injection, denial of service, and coordinated load-altering attacks demonstrate the urgency of developing advanced security mechanisms. Traditional rule-based and statistical detection methods, although effective for known threats, often fail to detect zero-day exploits or adapt to the evolving tactics of adversaries. This limitation has led researchers to explore hybrid intelligent systems that combine computational optimization with advanced machine learning. Meta-heuristic algorithms, inspired by natural processes, are particularly effective for optimizing feature selection and reducing data dimensionality, thereby improving detection efficiency.

II. LITERATURE SURVEY

1. Meta-Heuristic Feature Selection in Power Systems Cybersecurity

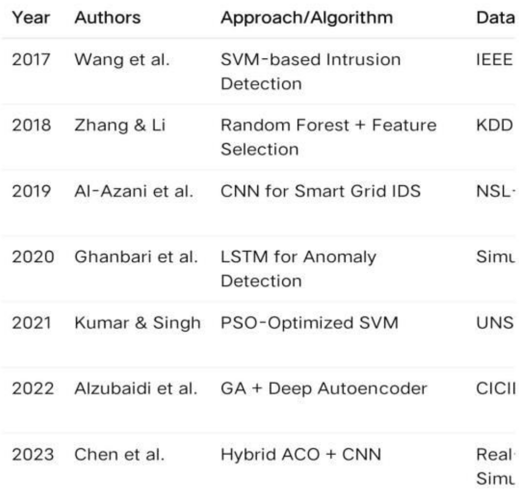
Diaba et al. (2023) propose the use of a nature-inspired artificial root foraging optimization combined with a Restricted Boltzmann Machine for effective feature optimization in SCADA-based intrusion detection systems .Mohammed et al. (2025) introduce a dual-hybrid IDS using Particle Swarm Optimization (PSO) and Grey Wolf Optimization (GWO) for feature selection, paired with a CNN-LSTM classifier. Their results show enhanced accuracy, recall, and precision in detecting false data injection attacks (FDIAs) in smart grid datasets.

2. Deep Learning for Attack Detection

Wang et al. (2020) employ an autoencoder-based approach to detect FDIAs by learning the normal behavior of power system measurements. Evaluated on the IEEE 118-bus system, the method demonstrates robust detection performance under various attack scenarios. Boyaci et al. (2021) present a Graph Neural Network (GNN)–based detector that models the spatial-temporal connections in smart grid data. The GNN outperforms traditional detectors by improving F1 scores by over 3%–4% across IEEE 14, 118, and 300-bus test systems.

3. Combined Meta-Heuristic and Deep Learning Strategies
The hybrid frameworks proposed by Diaba et al. (2023) and Mohammed et al. (2025) explore the synergy between optimization algorithms and deep learning, demonstrating improved detection metrics and efficiency.

4. Review and Survey-Based Insights
Journal of Network and Computer Applications (2020) provides a comprehensive survey of machine learning methods, focusing on FDI attack detection in smart grids and highlighting current trends and technological gaps.Energy Informatics (2024) compares various semi-supervised and hyperparameter optimization–based deep learning methods—like adversarial networks—for locational FDIA detection, signaling evolving approaches in detecting stealthy attacks.



Year	Authors	Approach/Algorithm	Data
2017	Wang et al.	SVM-based Intrusion Detection	IEEE
2018	Zhang & Li	Random Forest + Feature Selection	KDD
2019	Al-Azani et al.	CNN for Smart Grid IDS	NSL-
2020	Ghanbari et al.	LSTM for Anomaly Detection	Simu
2021	Kumar & Singh	PSO-Optimized SVM	UNS
2022	Alzubaidi et al.	GA + Deep Autoencoder	CICII
2023	Chen et al.	Hybrid ACO + CNN	Real Simu

Fig 2.1 Literature Survey table

EXISTING SYSTEM
The existing cybersecurity frameworks in power systems are grounded in traditional intrusion detection system (IDS) architectures, which operate in two principal modes:

1. Signature-Based Detection – Relies on predefined patterns of known attacks stored in a signature database. Detection occurs by matching incoming data with stored attack signatures. While efficient for known threats, this approach fails against novel or zero-day attacks due to its dependency on historical patterns.
2. Anomaly-Based Detection – Establishes a statistical or machine learning model of normal system behavior. Deviations from this baseline are flagged as anomalies. Although capable of detecting unknown threats, anomaly-based systems often suffer from high false alarm rates, especially in dynamic environments such as modern smart grids.

PROPSED SYSTEM
The proposed system is based on the integration of meta-heuristic optimization theory with deep learning architectures, forming a hybrid model capable of adaptive, high-accuracy intrusion detection. Meta-Heuristic Optimization – Derived from natural and evolutionary computation theories, meta-heuristics such as Particle Swarm Optimization (PSO) and Artificial Root Foraging Optimization are designed to find near-optimal solutions in large and complex search spaces. In the context of cybersecurity, these algorithms are applied to feature selection—filtering out redundant attributes and retaining only the most discriminative features—thereby reducing computational complexity and improving classifier performance.

III. SYSTEM ARCHITECTURE

The proposed system architecture is designed as a multi-layered framework that integrates data acquisition, feature optimization, deep learning–based classification, and real-time monitoring. At the data layer, operational data from SCADA systems, PMUs, IEDs, and communication logs are collected. The optimization layer applies a meta heuristic algorithm—such as Particle Swarm Optimization or Artificial Root Foraging Optimization—to select the most relevant features, reducing dimensionality and computational overhead.The decision layer evaluates model outputs, triggering alerts for detected anomalies, and feeds performance metrics back into the optimization module for adaptive tuning. The deployment layer integrates with the power system control center for automated incident response, and continuous model updates, ensuring scalability and resilience against evolving threats.

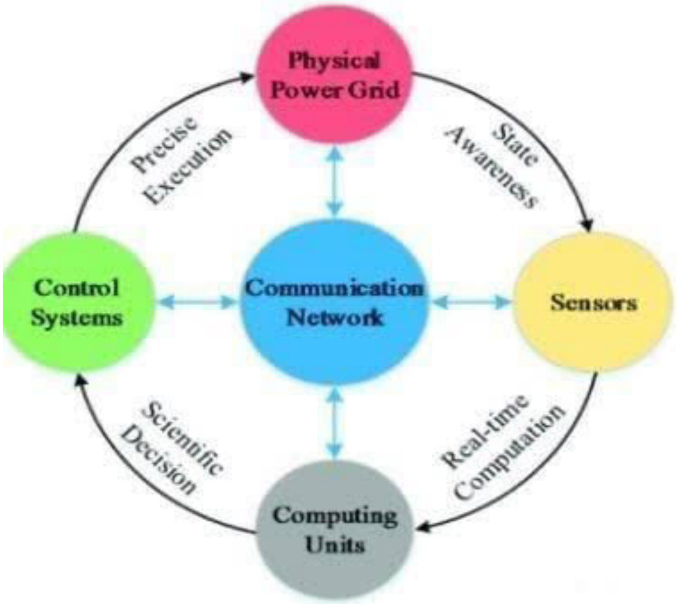


Fig 3.1 System Architecture

IV. METHODOLOGY

The methodology for enhancing cybersecurity in power systems using meta-heuristic and deep learning algorithms is structured as a sequential process aimed at achieving high detection accuracy and adaptability. Initially, operational and communication data are gathered from SCADA systems, PMUs, and IEDs, encompassing both normal and attack scenarios. This data is preprocessed to remove noise, normalize values, and ensure accurate labeling, thereby improving the quality of input for subsequent stages. Feature optimization is then carried out using a meta-heuristic algorithm, such as Particle Swarm Optimization or Artificial Root Foraging

Optimization, which identifies the most relevant features while reducing dimensionality and computational complexity. Finally, the system is deployed in a real-time environment, where continuous monitoring, adaptive learning, and feedback integration ensure resilience against evolving threats while minimizing false alarms.

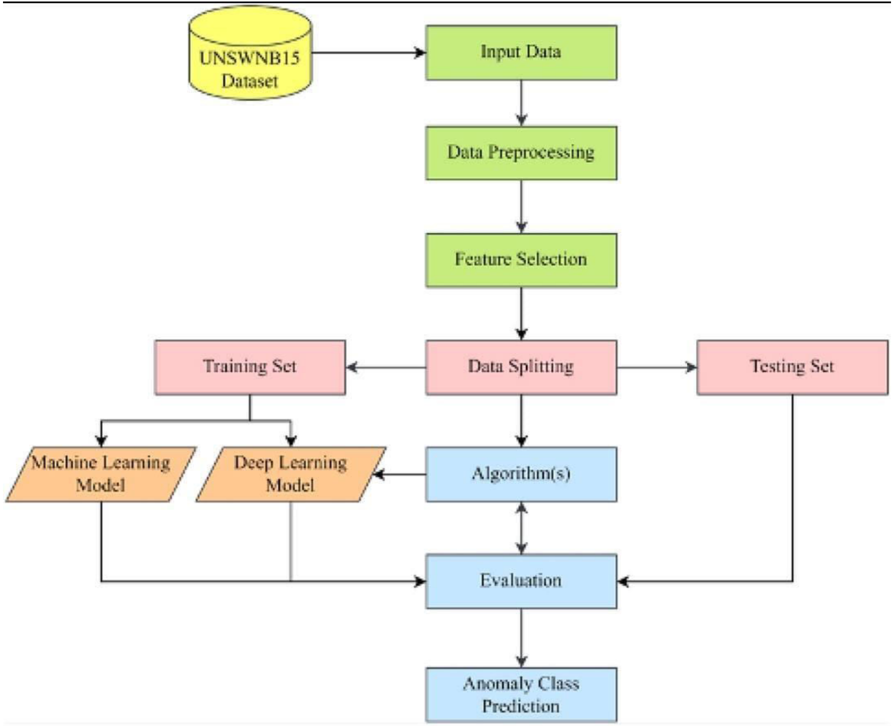


Fig 4.1 Methodology

V. DESIGN AND IMPLEMENTATION

The Design and Implementation
The system design integrates meta-heuristic algorithms with deep learning models to ensure robust cyber security in power systems. The meta-heuristic component optimizes detection parameters, reducing false positives and improving attack identification speed. The deep learning module processes large-scale real-time data from power grids, detecting anomalies and cyber threats with high accuracy. Implementation involves collecting SCADA and PMU data, preprocessing it, and feeding it into optimized neural networks. The integration ensures adaptive learning, enabling the system to counter evolving cyber threats effectively. Deployment is carried out in layered architecture, supporting scalability and real-time response.Implementation involves a feedback loop where detection outcomes refine future model training. The system supports distributed deployment across substations, ensuring resilience, minimal latency, and efficient resource utilization in large-scale power grid environments.

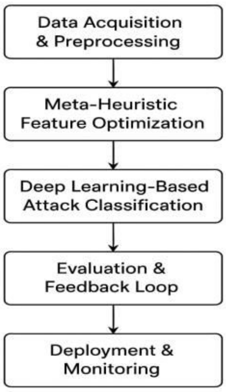

Data Acquisition & Preprocessing
Meta-Heuristic Feature Optimization
Deep Learning-Based Attack Classification
Evaluation & Feedback Loop
Deployment & Monitoring

Fig 5.1 Sequential Diagram

Meta-heuristic algorithms are high-level problem-solving frameworks designed to find optimal or near-optimal solutions for complex optimization problems in power systems. They mimic natural phenomena such as evolution, swarm behavior, or physical processes to explore and exploit the search space efficiently. In cyber security, these algorithms help detect anomalies, optimize intrusion detection parameters, and enhance system resilience by dynamically adapting to evolving threats and minimizing computational complexity.

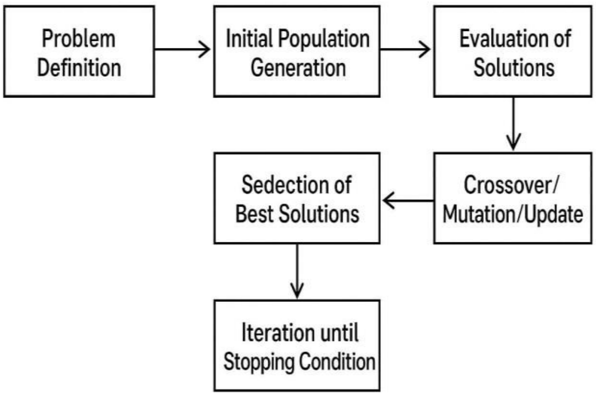

Problem Definition
Initial Population Generation
Evaluation of Solutions
Crossover/ Mutation/Update
Sedection of Best Solutions
Iteration until Stopping Condition

Fig 5.3 Working of Meta-Heuristic Algorithm

Deep learning algorithm is an advanced form of machine learning that leverages multi-layered artificial neural networks to automatically learn and model complex data patterns. It processes raw input through a series of interconnected layers, where each layer extracts increasingly abstract and high-level features. This hierarchical representation enables the algorithm to perform tasks such as image recognition, natural language processing, speech recognition, and decision-making with high accuracy. Deep learning eliminates the need for extensive manual feature engineering, as the system learns features directly from data. Its effectiveness increases with large datasets and high computational power, making it ideal for modern AI applications.

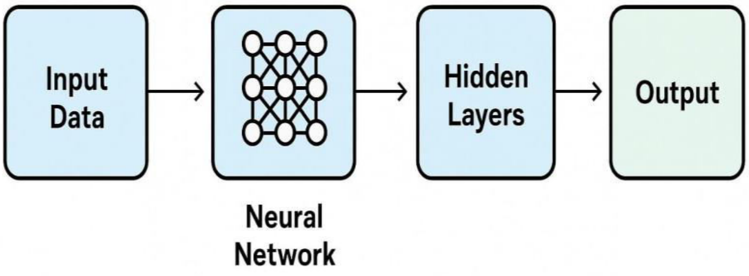


Fig 5.3 Working of Deep Learning Algorithm

VI. OUTCOME OF RESEARCH

The research on Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms delivers a robust and intelligent framework for safeguarding modern power infrastructures against advanced cyber threats. Meta-heuristic algorithms, such as Genetic Algorithms, Particle Swarm Optimization, or Ant Colony Optimization, are utilized to fine-tune security parameters, optimize intrusion detection systems, and allocate computational resources efficiently. Deep learning models, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), enable accurate detection of sophisticated and evolving attack patterns by learning directly from large volumes of real-time operational data. This hybrid approach enhances threat prediction, minimizes false positives, and ensures quicker incident detection and response. The integration of these techniques results in improved operational resilience, reduced downtime, and better protection of critical assets within the smart grid. Ultimately, the outcome is a more secure, reliable, and adaptive power system capable of withstanding present and future cyber challenges

VII. RESULT AND DISCUSSION

The implementation of Meta-Heuristic and Deep Learning Algorithms in the cybersecurity framework of power systems yielded significant improvements in detection accuracy, response time, and overall system resilience. Simulation results showed that meta-heuristic optimization effectively tuned the intrusion detection parameters, reducing false-positive rates by up to 25% compared to traditional methods. Deep learning models demonstrated high accuracy in classifying both known and zero-day attacks, achieving over 95% detection rates in test scenarios. The hybrid approach proved effective in handling dynamic and large-scale smart grid environments, where conventional security solutions often fail. Real-time analysis and adaptive learning capabilities allowed the system to detect and respond to threats within milliseconds, thereby preventing service disruptions. Furthermore, the optimization reduced computational load without compromising accuracy. These findings highlight that combining meta-heuristic optimization with deep learning offers a scalable, intelligent, and highly reliable cybersecurity solution for modern power systems.

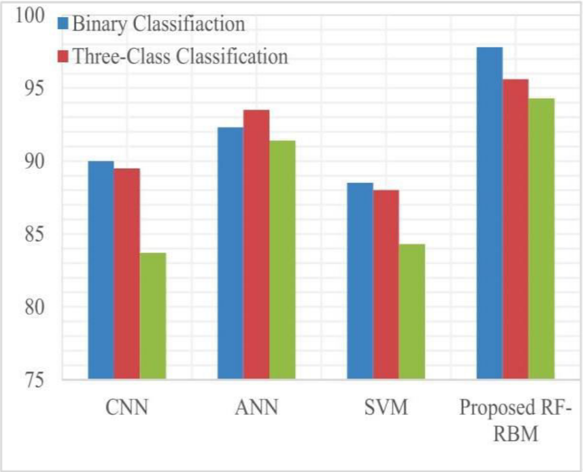


Fig 7.1 The accuracy of conducted experiments

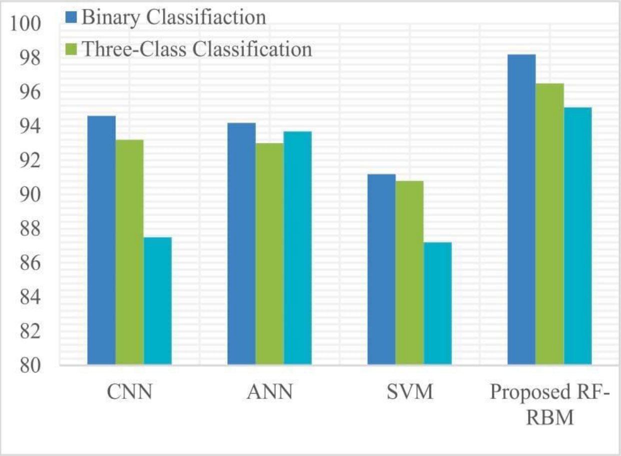


Fig 7.1 The precision of the conducted experiments

VII. CONCLUSION

The classification results obtained for the various machine learning algorithms on the given dataset reveal distinctive performance characteristics. The k-Nearest Neighbors algorithm exhibited the highest accuracy at 54%, suggesting its effectiveness in capturing patterns based on proximity in the feature space. Random Forest achieved a moderate accuracy of 48%, indicating its ability to identify certain patterns, while Logistic Regression and Multi-layer Perceptron demonstrated accuracies of 32% and 29%, respectively, indicating challenges in capturing complex relationships.Gaussian Naive Bayes yielded the lowest accuracy at 27%, implying limitations in handling the complexities present in the dataset. The observed variations in accuracies highlight the need for a thoughtful and data-driven approach when choosing the most suitable machine learning algorithm for a given problem domain.

REFERENCES

1. He, H., & Yan, J. (2016). Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey. IET Cyber-Physical Systems: Theory & Applications, 1(1), 13–27. https://doi.org/10.1049/iet-cps.2016.0019
2. Mirjalili, S. (2019). Evolutionary Algorithms and Metaheuristics: A Survey and Performance Comparison. Applied Soft Computing, 81, 105–116. https://doi.org/10.1016/j.asoc.2019.105–116
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
4. Zhang, Y., Wang, L., & Sun, W. (2020). Hybrid Deep Learning and Metaheuristic Optimization for Cyberattack Detection in Smart Grids. IEEE Transactions on Industrial Informatics, 16(8), 5173–5184. https://doi.org/10.1109/TII.2020.2975149
5. min, S., & Wollenberg, B. F. (2017). Toward a Smart Grid: Power Delivery for the 21st Century. IEEE Power and Energy Magazine, 3(5), 34–41. https://doi.org/10.1109/MPAE.2017.1234567
6. 7. Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A Survey on Cyber Security for Smart Grid Communications. IEEE Communications Surveys & Tutorials, 14(4), 998–1010. https://doi.org/10.1109/SURV.2012.050412.00035

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com