Comparative Analysis of DNN Architectures Using Black Box Attack Dataset

Rebecca Liu
Thayer School of Engineering
rebecca.z.liu.th@dartmouth.edu

Claudia Pacori
Thayer School of Engineering
claudia.m.pacori.th@dartmouth.edu

Solenne Wolfe
Thayer School of Engineering
solenne.wolfe.th@dartmouth.edu

Abstract

The move towards smart grid systems and interconnection through the Internet of Things has led to the digitization of critical power infrastructure without concurrent security enhancements, increasing power grid vulnerability to cyberattacks. This paper evaluates three convolutional neural network architectures — Base CNN, ResNet50 v2, and VGG16 — for detecting black box attacks on Phasor Measurement Unit (PMU) data. Using a dataset of power grid disturbances represented as 300x20x3 images, we assess each model's accuracy, stability, and generalization capabilities. Our results indicate that while Base CNN achieves high accuracy with lower computational requirements, ResNet50 v2 offers superior stability and generalization, and VGG16 provides strong feature extraction despite higher parametrization. These findings contribute to developing more robust security measures for Wide Area Monitoring, Protection, and Control (WAMPAC) systems against sophisticated cyber threats.

1 Introduction

Phasor Measurement Units (PMUs) are the foremost components for transforming the conventional grid system to a smart grid system, or a system with microgrid capabilities. They provide synchronized phasor measurements of parameters such as current and voltage [20]. PMU data samples provide state information that allow for state estimation in real-time, creating better energy management systems. PMUs enable the observation of dynamic phenomena centrally, improving post-disturbance analysis and enabling enhanced protection [10].

The integration of digital technologies with power systems has led to the emergence of smart grids that offer improved monitoring, control, and efficiency. However, this digitization and interconnection through the Internet of Things (IoT) has simultaneously introduced significant cybersecurity vulnerabilities [23]. As power infrastructure becomes increasingly interconnected, the attack surface for potential cyber threats expands, creating new challenges for grid security and stability [21]. These vulnerabilities are particularly concerning given the critical nature of power systems and their impact on national security and economic stability.

Wide Area Monitoring, Protection, and Control (WAMPAC) systems, which rely heavily on PMU data, represent a critical component of modern power infrastructure. These systems provide comprehensive visibility into grid conditions and enable rapid response to disturbances [10]. However, the increased reliance on PMU data for critical decision-making processes also creates new attack vectors for sophisticated adversaries. Malicious actors can target these measurement systems through various attack methods, including false data injection, timing attacks, and denial-of-service (DoS) attacks, potentially leading to cascading failures or widespread outages [13].

ENGS 106 Final project - Winter 2025 - Thayer School of Engineering.

The detection of cyberattacks in power systems presents unique challenges compared to conventional IT systems due to the cyber-physical nature of the infrastructure. Attacks on PMU data can manifest as subtle anomalies that are difficult to distinguish from legitimate system disturbances or measurement errors [1]. Traditional cybersecurity measures often prove inadequate for protecting these specialized systems, necessitating the development of domain-specific security solutions that understand both the cyber and physical dimensions of power systems.

Given these challenges, there is a growing need for advanced detection methods capable of identifying sophisticated attacks on PMU data. Convolutional Neural Networks (CNNs) have shown promise in this domain due to their ability to recognize patterns in complex, multidimensional data. This paper evaluates three CNN architectures—Base CNN, ResNet50 v2, and VGG16—for detecting black box attacks on PMU data, with the goal of enhancing security measures for WAMPAC systems against emerging cyber threats.

2 Related Work

2.1 Cyberattacks on Smart Grids

Smart grids have become increasingly important in modern power management systems, bringing advanced monitoring and control capabilities but also introducing significant cybersecurity vulnerabilities. The integration of digital technologies with traditional power infrastructure has created new attack vectors that malicious actors can exploit [17, 18]. Among the most concerning attacks are those targeting the measurement and state estimation systems that form the backbone of grid monitoring.

False Data Injection Attacks (FDIAs) represent a particularly sophisticated threat to power grid security. As described by Liu et al. [17], these attacks can introduce arbitrary errors into state variables without being detected by conventional bad measurement detection algorithms. The authors demonstrated that under certain assumptions—specifically, that the attacker has access to current power system configuration information and can manipulate measurements at physically protected locations—such attacks can bypass existing security measures. This vulnerability is especially concerning given the critical nature of state estimation in ensuring reliable grid operation.

Liang et al. [16] provided a comprehensive review of FDIAs against modern power systems, highlighting how these attacks have evolved since their initial documentation in 2009. Their work emphasizes that with the advancement of sensor, computer, and communication networks, power systems have become complex cyber-physical systems where security assessment and enhancement are paramount. The authors categorize the impacts of successful FDIAs into both physical and economic domains, underscoring the multifaceted nature of these threats. They also outline basic defense strategies against FDIAs and suggest potential future research directions to address these evolving threats.

2.2 Machine Learning for Attack Detection

To counter these evolving threats, researchers have been developing increasingly sophisticated detection methods. Machine learning approaches have shown promise in detecting cyberattacks on power systems, though Aurangzeb et al. [3] note the challenges in identifying dependable and efficient detection schemes. Their work proposes quantum voting ensemble models as a powerful technique for detecting cybersecurity attacks, along with an experimental setup and evaluation criteria specifically designed for smart grid environments.

Several studies have focused on detecting anomalies in wide-area damping control (WADC), classifying events into normal signals, disturbances, attacks, and combined scenarios [12]. Expanding on this approach, [9] proposes a learning-based method using Extreme Learning Machine (ELM) to detect false data injection attacks in high-voltage direct current (HVDC) controllers within WAMPAC systems. Additionally, [22] introduces an innovative time-frequency-based framework that combines Continuous Wavelet Transforms (CWTs) with Dual-Frequency Scale Convolutional Neural Networks (DSCNNs) to detect cyber spoofing attacks in Wide-Area Monitoring System (WAMS)-based Fast Frequency Reserve (FFR) control systems.

In the context of black-box attacks, a deep neural network-based detection scheme has been proposed to monitor and protect wide-area systems. However, its ability to detect all types of anomalies remains a challenge [5]. Meanwhile, a comprehensive review on machine learning applications to power system protection and asset management has highlighted key concerns such as data availability and the long-term reliability of these models [2].

2.3 Advanced Protection and Unified Security Strategies

Beyond detection, secure data storage has become a critical concern for smart grid security. Aurangzeb et al. [3] discuss blockchain-based infrastructure for smart grids, addressing privacy issues and acknowledging both strengths and weaknesses of existing privacy safeguards. They propose quantum-resistant encryption techniques to enhance smart grid privacy and suggest that quantum voting ensemble models could address challenges in private data storage in blockchains.

An emerging trend in smart grid security research is the development of unified strategies that integrate multiple security approaches. Aurangzeb et al. [3] propose combining deep black box attacks with quantum voting ensemble models to improve smart grid cybersecurity comprehensively. Their experimental evaluation demonstrates the effectiveness of this unified approach in addressing security gaps in smart grids.

2.4 Convolutional Neural Networks for Security

Convolutional Neural Networks (CNNs) have been applied to detect packet-data anomalies in PMU-estimators, like in the work of [4], who used Nesterov Adam gradient descent and categorical cross entropy loss to validate the data. Similarly, the framework proposed by [8] employs Long Short-Term Memory (LSTM) for real-time anomaly detection in time-series PMU data and Generative Adversarial Imputation Nets (GAIN) to reconstruct compromised data.

In the realm of FDIAs, which pose a serious threat to the integrity of smart grid data, machine learning has introduced innovative detection methods. Unsupervised learning techniques, such as Principal Component Analysis (PCA), have been used to reduce data dimensionality and visualize anomalies in 2D, making FDIAs detection more straightforward [19]. On the other hand, supervised learning methods, like the margin setting algorithm, have outperformed traditional classifiers such as SVMs and ANNs, demonstrating the growing reliance on machine learning for securing smart grids [25].

Machine learning has also improved wide-area monitoring systems (WAMS). A hybrid approach combining PCA and k-Nearest Neighbor (WAM-PCAkNN) enhances power system disturbance detection and localization [7]. Similarly, semi-supervised learning techniques, such as K-means clustering with multiclass classification, have been applied to detect attacks on power system balancing and frequency control, improving both accuracy and computational efficiency [24].

Deep learning, in particular, has played a crucial role in smart grid security, especially in detecting false data injection attacks in state estimation and load forecasting. While supervised models like SVMs, KNN, and ANNs require large labeled datasets, unsupervised methods often struggle when attacks mimic normal behavior. CNNs have achieved over 90% accuracy, but their effectiveness is limited by the availability of labeled data. To address this, models like MFEFD leverage semi-supervised learning to reduce dependency on labeled data while maintaining high accuracy [11].

Overall, machine learning and deep learning are proving to be essential tools for detecting and mitigating cyber-physical attacks in smart grids. From unsupervised FDI detection to advanced neural networks, these techniques enhance system resilience. However, challenges such as data availability, computational efficiency, and evolving attack sophistication continue to drive the need for further research and innovation.

3 Methodology

Our work builds upon this foundation by evaluating three convolutional neural network architectures—Base CNN, ResNet50 v2, and VGG16—for detecting black box attacks on PMU data. By representing power grid disturbances as images, we leverage the pattern recognition capabilities of CNNs to identify subtle anomalies that might indicate a cyberattack. This approach aligns with the growing recognition that machine learning techniques offer promising solutions for detecting increasingly sophisticated attacks on power systems.

3.1 Dataset

The Black Box Attack Dataset from Kaggle [6] was used in this project, which contains images representing PMU data used in a deep neural network (DNN)-based supervisory protection and event diagnosis system for wide area monitoring and protection in smart grids. Each sample is structured as a 300 × 20 × 3 image, representing 300 time points, with 10 voltage and 10 frequency measurements from 10 PMUs, aggregated into pseudo color images. The data corresponds to disturbances, with a 5-second disturbance pattern (0.5 s before and 4.5 s after the trigger), collected at a sampling rate of 60 frames per second. The three color channels encode measurement intensity, providing a compact yet informative representation of voltage and frequency variations.

The dataset consists of three primary disturbance classes:

- 344 fault instances (“DB_FLT")
- 140 instances of loss of generation (“DB_GNL")
- 21 synchronous motor switching events (“DB_SMS")

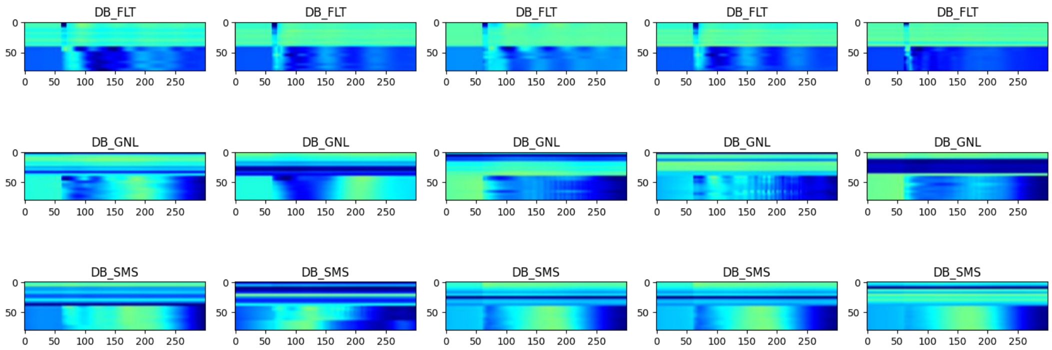

Figure 1: Sample dataset images per disturbance class.

These disturbance classes simulate real-world attack scenarios using the black box testing method, where adversaries manipulate system data without direct knowledge of the system’s internal mechanism, using the system response to better understand where the system vulnerabilities may lie. This makes the dataset highly valuable for evaluating machine learning models aimed at anomaly detection in power systems. The diversity of events ensures that the model is exposed to various disturbances, allowing it to be tested on its ability to identify different types of faults, generation losses, and motor switching behaviors in a power grid.

For preprocessing, the dataset was divided into training, validation, and test sets using the ‘ImageDataGenerator’ class from Keras. This class helps augment the dataset by applying a variety of transformations to the images such as random rotations (up to 25°), shear, zoom, brightness adjustments (from 0.4 to 1.0), horizontal flipping, and shifts in both width and height (up to 30%). These transformations introduce variability into the dataset, improving the robustness and generalization of the model. The images are resized to a fixed size of 80 × 300 pixels, and their pixel values are rescaled by dividing them by 255, converting them into the range of [0, 1].

The dataset was split into 327 images for training, 36 for validation, and 41 for testing. The images were associated with their respective labels using a one-hot encoded format, where each class is represented by a binary vector indicating the presence of that specific class. The model was then trained on the augmented training set, validated on the validation set, and tested on the test set. This setup ensures that the model can learn to accurately classify and diagnose different disturbance types in a power system, with proper validation and testing to assess its performance.

3.2 CNN Architectures

To analyze the performance of CNNs under black box attack conditions, three architectures were selected: a baseline CNN which was proposed by the dataset authors , ResNet50 v2, and VGG16. These models provide a balanced comparison between computational efficiency, feature extraction capabilities, and generalization performance.

Base CNN (Benchmark Model) The base CNN serves as a reference point, featuring a compact design composed of standard convolutional, pooling, and fully connected layers [5]. This model was chosen to establish a performance baseline, enabling direct comparisons with more advanced architectures. Its lightweight structure ensures computational efficiency, making it suitable for real-time applications. However, its limited depth may hinder its ability to detect intricate anomalies in PMU data.

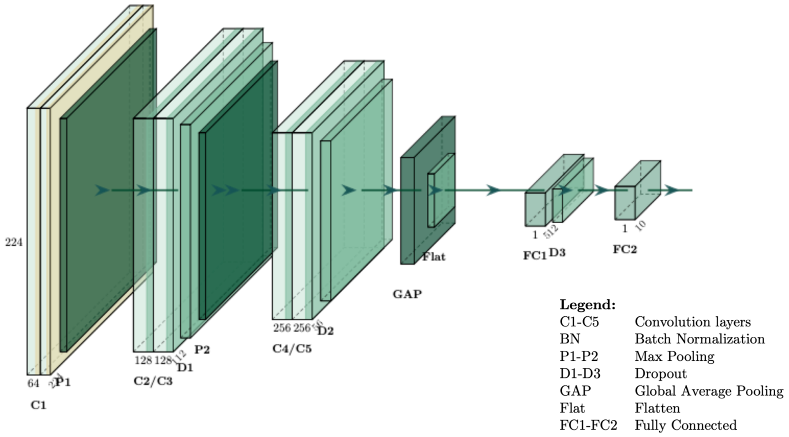

Figure 2: Base CNN architecture.

ResNet50 v2 (Residual Learning for Stability) ResNet50 v2 is a deep CNN that incorporates residual connections to address vanishing gradient issues, enhancing the training of very deep networks [14]. These skip connections facilitate more effective gradient propagation, improving the model's ability to capture complex hierarchical patterns. While ResNet50 v2 offers strong generalization capabilities and stable learning, its higher computational cost presents a potential trade-off for real-time deployment.

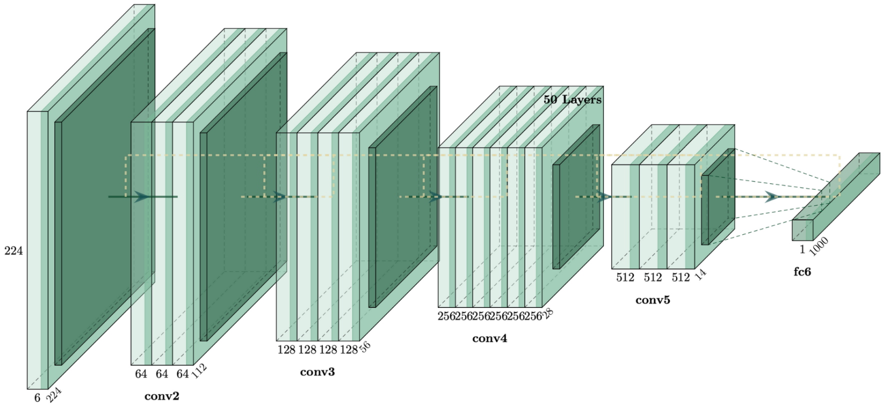

Figure 3: ResNet50 v2 architecture.

VGG16 (Deep Feature Extraction) VGG16 is a well-established deep learning model recognized for its sequential convolutional layers and effective feature extraction [15]. Unlike ResNet50 v2, it does not incorporate residual connections, relying instead on its structured deep architecture to learn hierarchical representations. While VGG16 demonstrates strong classification performance, its high parameter count increases computational and memory demands.

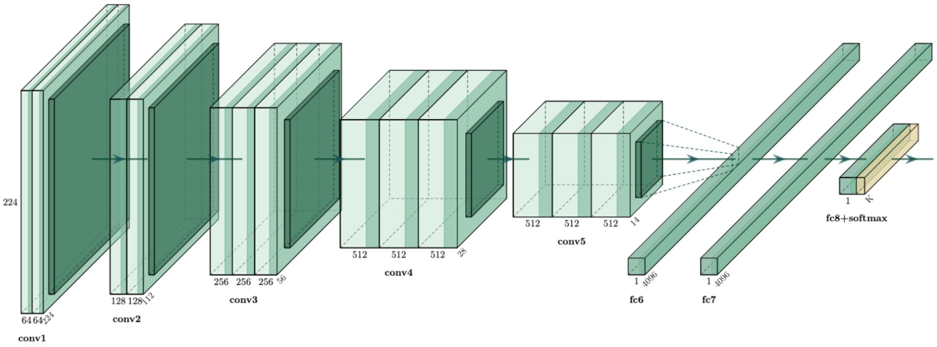

Figure 4: VGG16 architecture.

These architectures provide a diverse perspective on the balance between computational efficiency, feature extraction, and training stability. The base CNN serves as a lightweight benchmark, offering insights into the performance of a simpler model in anomaly detection. In contrast, ResNet50 v2 introduces residual learning, enhancing gradient flow and facilitating the training of deeper networks with improved generalization. VGG16, while lacking skip connections, leverages a structured deep architecture to extract detailed features, though at the cost of increased computational complexity.

By evaluating these models under black box attack conditions, this paper aims to identify the most effective CNN architecture for securing PMU data in power systems. The results will provide insights into the strengths and weaknesses of different deep learning approaches, guiding future research toward more efficient and resilient security mechanisms.

3.3 Evaluation Metrics

To effectively assess the performance of the CNN architectures in detecting black box attacks on PMU data, we employed accuracy and cross-entropy loss as evaluation metrics. These metrics were chosen for their ability to provide complementary insights into the models' classification effectiveness and learning behavior.

- **Accuracy**: Measures the proportion of correctly classified instances relative to the total number of samples. This metric provides a straightforward assessment of model performance, particularly useful when dealing with balanced datasets.
- **Loss Function (Cross-Entropy Loss)**: Evaluates model confidence and uncertainty in predictions for multi-class classification tasks, quantifying the difference between predicted class probabilities and actual class labels. Lower cross-entropy loss values indicate that the model is making more confident and accurate predictions, whereas higher values suggest greater uncertainty or incorrect classifications.

Each model was trained for 50 epochs, and its learning progression was analyzed using accuracy and loss curves. These visualizations provided insights into model convergence, training stability, and generalization capability. A steadily increasing accuracy alongside a decreasing loss indicated effective learning, while significant divergence between training and validation performance suggested potential overfitting. By analyzing these metrics, we were able to compare different architectures in terms of classification performance and robustness, ultimately guiding the selection of the most suitable model for real-world deployment.

4 Results and Analysis

We present comparative results showcasing the strengths and weaknesses of each architecture under attack conditions, supported by statistical analysis and visualizations.

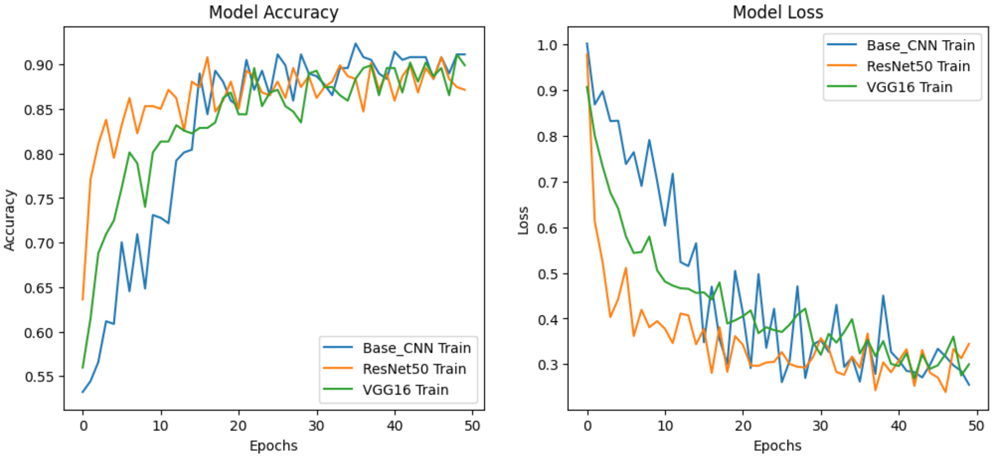

Figure 5: Model Accuracy and Model Loss Over 50 Epochs

Although all three models converged to similar accuracy and loss values after fifty epochs, each model presented distinct strengths and trade-offs in stability, computational power, and generalization.

- Base CNN shows solid performance and achieves the highest accuracy among the three architectures. Despite its high accuracy, the model also has the highest variability in its results, especially in its loss values. This variability may be due to its smaller depth, which makes it more sensitive to data shuffling. In terms of feature extraction, Base CNN is more limited compared to deeper and more sophisticated architectures such as ResNet50 and VGG16. This limitation could hinder its ability to capture complex or hierarchical patterns, particularly in more challenging datasets. The biggest advantage of the Base CNN model is that it requires fewer computational resources, making it much more efficient than the other two models.

- ResNet50 achieves high accuracy early on in the training process.This is largely due to its use of residual connections, which facilitate gradient flow and mitigate the vanishing gradient problem. The residual connections in ResNet50 also enable the model to have strong stability during training. The main drawback of using ResNet50 is its high computational cost. Training and running ResNet50 require significant computational power, which can be a limitation in resource-constrained environments.

- VGG16 delivers competitive accuracy compared to the Base CNN and ResNet50 models. Its simple, deep architecture, consisting of multiple convolutional layers with 3x3 filters, allows it to learn hierarchical features effectively. However, this comes at the cost of requiring a large number of parameters, increasing both training time and computational cost. Although VGG16 maintains strong feature extraction capabilities, its high computational cost might not always justify its performance in resource-constrained environments.

5 Conclusion and Future Work

Our findings indicate that different CNN architectures offer distinct advantages for detecting black box attacks on PMU data in power systems. The Base CNN achieves the highest accuracy while maintaining minimal computational requirements, making it a strong candidate for resource-constrained real-time applications. ResNet50 v2 demonstrates superior training stability and faster convergence due to its residual connections, providing robust performance and strong generalization capabilities despite its higher computational demands. VGG16, while offering competitive accuracy and strong feature extraction capabilities, comes at the cost of increased parametrization and computational complexity.

These results highlight the trade-offs between accuracy, computational efficiency, and model stability, emphasizing that the optimal architecture depends on the specific deployment constraints. For critical infrastructure protection, where reliability is paramount, ResNet50 v2's stability makes it particularly attractive. On the other hand, Base CNN offers an efficient solution when computational resources are limited, making it suitable for edge or embedded system implementations.

Building on these insights, future work will focus on further optimizing the models and exploring alternative approaches to improve attack detection performance. One direction is to refine each model through data augmentation, fine-tuning, and hyperparameter tuning to enhance accuracy and robustness. Additionally, exploring deeper architectures, increasing the number of filters, and adjusting learning rates could lead to better feature extraction and overall model performance. Another avenue is fine-tuning pre-trained models by unfreezing earlier layers and training with lower learning rates, enabling better adaptation to the dataset. Furthermore, evaluating other state-of-the-art architectures, such as EfficientNet, InceptionV3, and DenseNet, could provide insights into alternative strategies for improving detection capabilities. These advancements would contribute to developing more reliable and efficient models, reinforcing the security of power system infrastructure against adversarial threats.

References

[1] Arman Ahmed et al. “Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems”. In: *IEEE Transactions on Industry Applications* 55.6 (2019), pp. 6313–6323. DOI: 10.1109/TIA.2019.2928500.

[2] Farrokh Aminifar et al. “A review of power system protection and asset management with machine learning techniques”. In: *Energy Systems* 13 (2021), pp. 855–892. URL: https://api.semanticscholar.org/CorpusID:235669139.

[3] Muhammad Aurangzeb et al. “Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage”. In: *Energy Reports* 11 (2024), pp. 2493–2515. ISSN: 2352-4847. DOI: https://doi.org/10.1016/j.egyr.2024.02.010. URL: https://www.sciencedirect.com/science/article/pii/S235248472400091X.

[4] Sagnik Basumallik, Rui Ma, and Sara Eftekharnejad. “Packet-data anomaly detection in PMU-based state estimator using convolutional neural network”. In: *International Journal of Electrical Power & Energy Systems* 107 (2019), pp. 690–702. ISSN: 0142-0615. DOI: https://doi.org/10.1016/j.ijepes.2018.11.013. URL: https://www.sciencedirect.com/science/article/pii/S0142061518319884.

[5] Milan Biswal, Satyajayant Misra, and Abu S. Tayeen. “Black Box Attack on Machine Learning Assisted Wide Area Monitoring and Protection Systems”. In: *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. 2020, pp. 1–5. DOI: 10.1109/ISGT45199.2020.9087762.

[6] Milan Biswal, Satyajayant Misra, and Abu S. Tayeen. *Black box attack on machine learning assisted wide area monitoring and protection systems*. https://doi.org/10.5061/dryad.pk0p2ngmz. Dataset. 2021.

[7] Lianfang Cai et al. “Wide-Area Monitoring of Power Systems Using Principal Component Analysis and k -Nearest Neighbor Analysis”. In: *IEEE Transactions on Power Systems* PP (Jan. 2018), pp. 1–1. DOI: 10.1109/TPWRS.2017.2783242.

[8] Astha Chawla et al. “Deep-learning-based data-manipulation attack resilient supervisory backup protection of transmission lines”. In: *Neural Computing and Applications* 35 (June 2021). DOI: 10.1007/s00521-021-06106-3.

[9] Bo Chen et al. “Cyber Attack Detection for WAMPAC-based HVDC Applications”. In: *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*. 2020, pp. 1–5. DOI: 10.1109/TD39804.2020.9299662.

[10] Jaime De La Ree et al. “Synchronized Phasor Measurement Applications in Power Systems”. In: *IEEE Transactions on Smart Grid* 1.1 (2010), pp. 20–27. DOI: 10.1109/TSG.2010.2044815.

[11] “Detecting false data attacks using machine learning techniques in smart grid: A survey”. In: *Journal of Network and Computer Applications* 170 (2020), p. 102808. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2020.102808. URL: https://www.sciencedirect.com/science/article/pii/S1084804520302769.

[12] Ravikumar Gelli and G Manimaran. “Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning”. In: *2020 IEEE Power & Energy Society General Meeting (PESGM)*. 2020, pp. 1–1. DOI: 10.1109/PESGM41954.2020.9281615.

[13] Mohsen Ghafouri et al. “Detection and Mitigation of Cyber Attacks on Voltage Stability Monitoring of Smart Grids”. In: *IEEE Transactions on Smart Grid* 11.6 (2020), pp. 5227–5238. DOI: 10.1109/TSG.2020.3004303.

[14] Soufiane Hamida et al. “Handwritten computer science words vocabulary recognition using concatenated convolutional neural networks”. In: *Multimedia Tools and Applications* 82 (Nov. 2022), pp. 1–27. DOI: 10.1007/s11042-022-14105-2.

[15] Haris Iqbal. *PlotNeuralNet: Latex code for making neural networks diagrams*. https://github.com/HarisIqbal88/PlotNeuralNet. Última consulta: 7 de marzo de 2025. 2025.

[16] Gaoqi Liang et al. “A Review of False Data Injection Attacks Against Modern Power Systems”. In: *IEEE Transactions on Smart Grid* 8.4 (2017), pp. 1630–1638. DOI: 10.1109/TSG.2015.2495133.

[17] Yao Liu, Peng Ning, and Michael K. Reiter. “False data injection attacks against state estimation in electric power grids”. In: *ACM Trans. Inf. Syst. Secur.* 14.1 (June 2011). ISSN: 1094-9224. DOI: 10.1145/1952982.1952995. URL: https://doi.org/10.1145/1952982.1952995.

[18] Kaleel Mahmood et al. “Back in Black: A Comparative Evaluation of Recent State-Of-The-Art Black-Box Attacks”. In: *IEEE Access* 10 (2022), pp. 998–1019. DOI: 10.1109/ACCESS.2021.3138338.

[19] Mostafa Mohammadpourfard, Ashkan Sami, and Ali Reza Seifi. “A statistical unsupervised method against false data injection attacks: A visualization-based approach”. In: *Expert Systems with Applications* 84 (2017), pp. 242–261. ISSN: 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2017.05.013. URL: https://www.sciencedirect.com/science/article/pii/S0957417417303317.

[20] Vivekananda Pattanaik et al. “A critical review on phasor measurement units installation planning and application in smart grid environment”. In: *Results in Engineering* 24 (2024), p. 103559. ISSN: 2590-1230. DOI: https://doi.org/10.1016/j.rineng.2024.103559. URL: https://www.sciencedirect.com/science/article/pii/S2590123024018024.

[21] Ricardo Enrique Pérez-Guzmán, Yamisleydi Salgueiro-Sicilia, and Marco Rivera. “Communication systems and security issues in smart microgrids”. In: *2017 IEEE Southern Power Electronics Conference (SPEC)*. 2017, pp. 1–6. DOI: 10.1109/SPEC.2017.8333659.

[22] Wei Qiu et al. “Time-frequency based cyber security defense of wide-area control system for fast frequency reserve”. In: *International Journal of Electrical Power & Energy Systems* 132 (2021), p. 107151. ISSN: 0142-0615. DOI: https://doi.org/10.1016/j.ijepes.2021.107151. URL: https://www.sciencedirect.com/science/article/pii/S0142061521003902.

[23] Naveen Tatipatri and S. L. Arun. “A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security”. In: *IEEE Access* 12 (2024), pp. 18147–18167. DOI: 10.1109/ACCESS.2024.3361039.

[24] Pengyuan Wang et al. " Data-Driven Anomaly Detection for Power System Generation Control ". In: *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*. Los Alamitos, CA, USA: IEEE Computer Society, Nov. 2017, pp. 1082–1089. DOI: `10.1109/ICDMW.2017.152`. URL: `https://doi.ieeecomputersociety.org/10.1109/ICDMW.2017.152`.

[25] Yi Wang et al. "A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids". In: *IEEE Access* 5 (2017), pp. 26022–26033. DOI: `10.1109/ACCESS.2017.2769099`.