Parallel CNN Deep Learning Model for Security Monitoring and Fault Prediction in Electrical Systems

Jaouhar Fattahi[1] ; Mohamed Mejri[1] ; Ridha Ghayoula[2]
Laila Boumlik[1] ; Feriel Sghaier[3] and Marwa Ziadia[1]

***Abstract*— Electrical systems keep things running in modern life, but they often run into problems like imbalances, short circuits, ground faults, and overloading, which can cause equipment to break down, fires to break out, and even large-scale blackouts. To make matters worse, acts of sabotage, physical damage, or cyberattacks on systems like SCADA can mess up operations, throw grids off balance, and set off cascading failures. To avoid these risks, there is a growing need for smarter tools that can keep track of system performance and flag potential issues before they get out of hand. In this paper, we suggest a deep learning model built on the inception architecture, designed to monitor electrical systems, call out potential security faults, and spot malicious actions. Taking advantage of deep learning, our approach helps increase fault prediction accuracy and keep operations on track.**

***Index Terms*— Electrical systems, Fault, Detection, Deep Learning, Inception, Forensics, Cybersecurity.**

I. Introduction

Power systems face many threats that can severely damage equipment and disrupt everyday life [1]–[3]. Short circuits harm equipment, cause power outages, and even start fires or trigger explosions. Ground faults wear out insulation and increase the risk of electric shock or fire. Overloading puts strain on transformers and generators, making them overheat, break down faster, or trip protective devices, which cuts off power and leads to blackouts. Voltage imbalances make equipment run inefficiently, heat up, and wear out earlier than expected. Cyberattacks on SCADA systems [4], [5], for example, let hackers take over operations, shut down grids, destabilize systems, or steal and corrupt important data. Physical sabotage or vandalism breaks or destroys critical infrastructure like substations and transformers, leaving entire regions without power for long periods. Aging infrastructure adds to these risks, as old components break down more easily, causing outages, driving up maintenance costs, and creating safety hazards. Cascading failures, often triggered by grid instability, quickly snowball into regional or even nationwide blackouts, which disrupt critical services and daily routines. Insider threats, who are generally authorized personnel, can misuse their access to harm equipment or cause long-term security problems. Together, these threats show how vulnerable electrical systems are and why it is so important to protect and monitor them to avoid large-scale damage. Finding electrical problems early makes life a lot easier and safer. It helps stop small issues from turning into big, expensive ones, saving money on repairs and avoiding the hassle of replacing damaged equipment. We can plan maintenance ahead of time instead of dealing with sudden breakdowns, which keeps things running without unexpected delays. Fixing these problems early also brings down maintenance costs and makes sure everything stays in good shape. On top of that, it helps prevent dangerous situations like fires, short circuits, or electric shocks, which keeps everyone safe. When we sort out issues like overheating or voltage problems quickly, our equipment works better, uses less energy, and does not drive up electricity bills. In addition, taking care of small faults helps equipment last longer, so we do not have to replace it as often. Early detection also prevents power outages from disrupting work or daily life by keeping the system stable and reliable. That also allows to stay on the right side of safety rules, avoiding fines and making sure that operations stay legal. In the end, catching electrical problems early saves us time, money, and stress while making sure everything runs smoothly and safely. Deep learning brings plenty of advantages when it comes to strengthening physical security for electrical systems. First, it helps us identify threats on-time, like someone acting suspicious, so that we can manage the problem. Second, it reduces false alarms by learning the difference between normal activity and real risks, saving us time and effort. Third, it lets us predict potential problems by spotting patterns and warning us about issues before they happen. Fourth, it monitors everything around the clock, so we don't need someone constantly watching over it. This gives us peace of mind knowing the system is always on guard. Fifth, it boosts access control with tools like facial recognition or other checks to ensure only authorized people can get in. Sixth, it helps us identify insider threats, flagging unusual or risky behavior from people who are supposed to have access. Seventh, it speeds up response time by highlighting what needs immediate attention and giving us clear steps to resolve it. Eighth, it scales easily as systems grow, handling more data and infrastructure. Ninth, it adapts to new threats, continuously learning and improving to stay ahead of evolving risks. Finally, it works with what we already have, so we can upgrade security [6] without

[1] Jaouhar Fattahi and Mohamed Mejri and Laila Boumlik and Marwa Ziadia are with the Department of Computer Science and Software Engineering, Laval University, Quebec, Canada. Jaouhar.Fattahi.1@ulaval.ca; Mohamed.Mejri@ift.ulaval.ca; Laila.Boumlik.1@ulaval.ca and Marwa.Ziadia.1@ulaval.ca

[2] Ridha Ghayoula is with the Faculty of Engineering, University of Moncton, New Brunswick, Canada. Ridha.Ghayoula@umoncton.ca

[3] Feriel Sghaier is with the Carthage National Engineering School, Carthage University, Tunis, Tunisia. Feriel.Sghaier@enicar.ucar.tn

overhauling the entire setup. In short, deep learning makes protecting electrical systems easier, faster, and more reliable, giving us the tools we need to stay safe and secure. In this paper, we explore an inception-based deep learning model [7], [8] to predict faults in electrical systems. Inception models stand out because of their parallel architecture, where multiple convolutional filters of different sizes run side by side in the same layer. This setup allows the model to pick up on both fine details and broader patterns at the same time, making it highly effective at capturing complex features in data. These models have already proven their worth in other fields, such as image classification, medical diagnosis, and object detection, where they have achieved remarkable accuracy and reliability. When it comes to securing electrical plants and systems, inception models can act by spotting problems early and flagging them before they escalate into major problems. They can help us stay ahead of faults, ensuring that problems are fixed on time to avoid costly downtime or safety risks. Their ability to handle complex data and adapt to different situations makes them a valuable tool for keeping critical infrastructure safe and reliable. By applying this powerful deep learning approach, we aim to improve fault prediction and strengthen the overall security of electrical systems.

II. Experiment

A. Dataset

Our dataset is a subset of the dataset described in [9]. The dataset focuses on transmission lines, which transfer alternating current (AC) or direct current (DC) over long distances to connect power plants to substations or deliver electricity to various users. It includes details about different types of lines—overhead, underground, and submarine—and highlights key design factors such as voltage, current capacity, and insulation to ensure reliable performance. The dataset is designed to identify and classify faults in the system, with five possible fault types:

- **Class 0**: No Fault
- **Class 1**: Fault between Phase A and Ground
- **Class 2**: Fault between Phase A and Phase B
- **Class 3**: Fault Phases A,B and Ground
- **Class 4**: Fault between three Phases: A, B, and Ground

The dataset supports the development of models to monitor systems, spot faults quickly, and ensure safe and efficient power delivery. The dataset contains 6728 entries with 11 features, 5382 out of the entries are used for training and 1346 for tests. Fig. 1 shows the class distribution in the used dataset.

B. Model architecture

Our model is basically a simplified Inception-based neural network with five output classes. It leverages the strengths of the **Inception architecture** by employing parallel convolutional paths within its single Inception block, providing multi-scale feature extraction capabilities. Below is a detailed breakdown of the model:

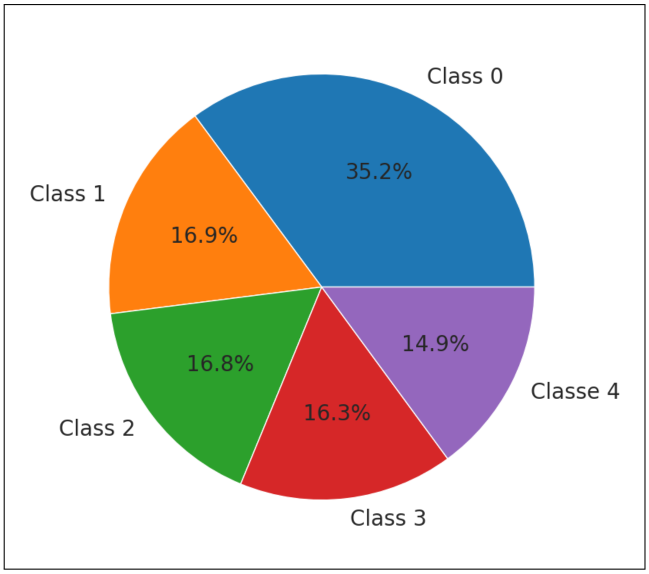


Fig. 1: Class distribution in the dataset

- **Input Layer:**
  - Accepts reshaped input data of shape $(\text{input\_dim}, 1)$, where `input_dim` represents the sequence length, and 1 is the number of channels (e.g., for 1D data like time-series or audio).
- **Inception Block:**
  - A single block processes the input using **four parallel paths**:
    - **Path 1:** A 1×1 convolutional layer to extract fine-grained features.
    - **Path 2:** A 1×1 convolution followed by a 3×3 convolution to capture medium-scale features.
    - **Path 3:** A 1×1 convolution followed by a 5×5 convolution to capture larger-scale patterns.
    - **Path 4:** A 3×3 max-pooling layer followed by a 1×1 convolution to focus on local and contextual features.
  - The outputs of these four paths are concatenated along the feature axis, resulting in a rich representation of multi-scale features.
- **Max Pooling:**
  - After the Inception block, a `MaxPooling1D` layer with a pool size of 2 reduces the spatial dimensions, capturing dominant features and lowering computational complexity.
- **Flatten Layer:**
  - Flattens the feature map into a one-dimensional vector to prepare it for the dense layers.
- **Dropout:**
  - A dropout layer with a rate of 0.3 helps prevent overfitting by randomly deactivating 30% of neurons during training.
- **Dense Layer:**

- A fully connected layer with 128 neurons and ReLU activation extracts high-level patterns from the flattened features.

- **Output Layer:**
  - The final dense layer with 5 neurons (corresponding to the number of classes) and softmax activation outputs probabilities for each class.
- **Optimizer:** Adam optimizer ensures efficient convergence with adaptive learning rates.
- **Loss Function:** Sparse Categorical Crossentropy is used for multi-class classification.
- **Metrics:** Accuracy is tracked during training and validation.
- **Training Setup:**
  - Batch size: 20
  - Epochs: 100
  - Validation split: 20% of the training data is used for validation.

Figure 2 illustrates the architecture of our model.

C. Used metrics

In our experiment, we used the following metrics.

1) Accuracy: Accuracy measures the proportion of correctly classified instances among the total instances. It is a general measure of how often the model makes the correct prediction.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

- TP: True Positives
- TN: True Negatives
- FP: False Positives
- FN: False Negatives

2) Precision: Precision measures the proportion of true positive predictions out of all positive predictions made by the model. It reflects how precise the model is in identifying the positive class.

$$\text{Precision} = \frac{TP}{TP + FP}$$

3) Recall: Recall, also known as sensitivity or true positive rate, measures the proportion of true positive predictions out of all actual positive instances. It shows how well the model identifies the positive class.

$$\text{Recall} = \frac{TP}{TP + FN}$$

4) F1-Score: The F1-score is the harmonic mean of Precision and Recall. It provides a single score that balances the trade-off between precision and recall, especially useful when the dataset is imbalanced.

$$\text{F1-Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

III. Results

Fig. 3 shows the training progression over epochs of the accuracy and loss.

Fig. 4 shows the overall confusion matrix.

Fig. 5 displays the confusion matrices for each class in the dataset (Class 0 to Class 4). Each matrix shows the performance of the model in distinguishing one class versus all others.

Fig. 6 shows the accuracy rate for each class.

Fig. 7 shows the precision rate for each class.

Fig. 8 shows the recall rate for each class.

Fig. 9 shows the F1-score rate for each class.

As we can see it through the four last figures, for all classes, the accuracy rate is above 92.90%, reaching 100.00% for Class 0. The precision rate is always above 91.02%, reaching 100.00% for Class 4 and 99.31% for Class 0. The recall rate is always above 93.32%, reaching 99.65% for Class 1. The F1-score is always above 93.25%, reaching 99.65% for Class 0. These outcomes confirm the effectiveness of the proposed model.

IV. Related work, discussion and future directions

Many studies showcase the powerful role of AI and deep learning in solving complex problems across diverse fields. Pereira et al. [10] use Transformers and LSTMs with a recursive multi-step forecasting approach to predict influent conductivity in wastewater treatment plants, achieving high accuracy and enabling proactive water salinity management. Yao et al. [11] propose a hybrid model combining a 1D-CNN and LSTM (SLSTM-TCNN) to analyze plant electrical signals under salt stress, coupled with a salt tolerance classification model, improving the efficiency of identifying salt-tolerant crops. Chen et al. [12] develop a physics-guided multi-agent reinforcement learning algorithm (PG-MA2TD3) for active voltage control in power grids, integrating global voltage sensitivity to coordinate PV inverters, achieving robust performance in minimizing voltage fluctuations. Mohammadi et al. [13] utilize transfer learning with the GoogleNet architecture to detect high-impedance faults in electrical systems by converting harmonic data into images using the Wigner–Ville distribution, enabling fault detection with minimal training data. Carratù et al. [14] apply convolutional autoencoders to detect anomalies in industrial electrical systems using only current intensity data from one phase, reducing false positives and improving fault detection efficiency. Lastly, El-Telbany [15] employs LSTMs for short-term electrical load forecasting, demonstrating improved accuracy by capturing temporal dependencies in smart meter data, aiding smarter energy management. Together, these studies highlight how deep learning models, tailored to specific challenges, provide robust, data-driven solutions across industries. In this study, we propose an effective Inception-based deep learning model to monitor electrical systems, detect faults in real time, and identify security anomalies. The model leverages Inception's parallel convolutional layers [16]–[18] to capture both fine details and

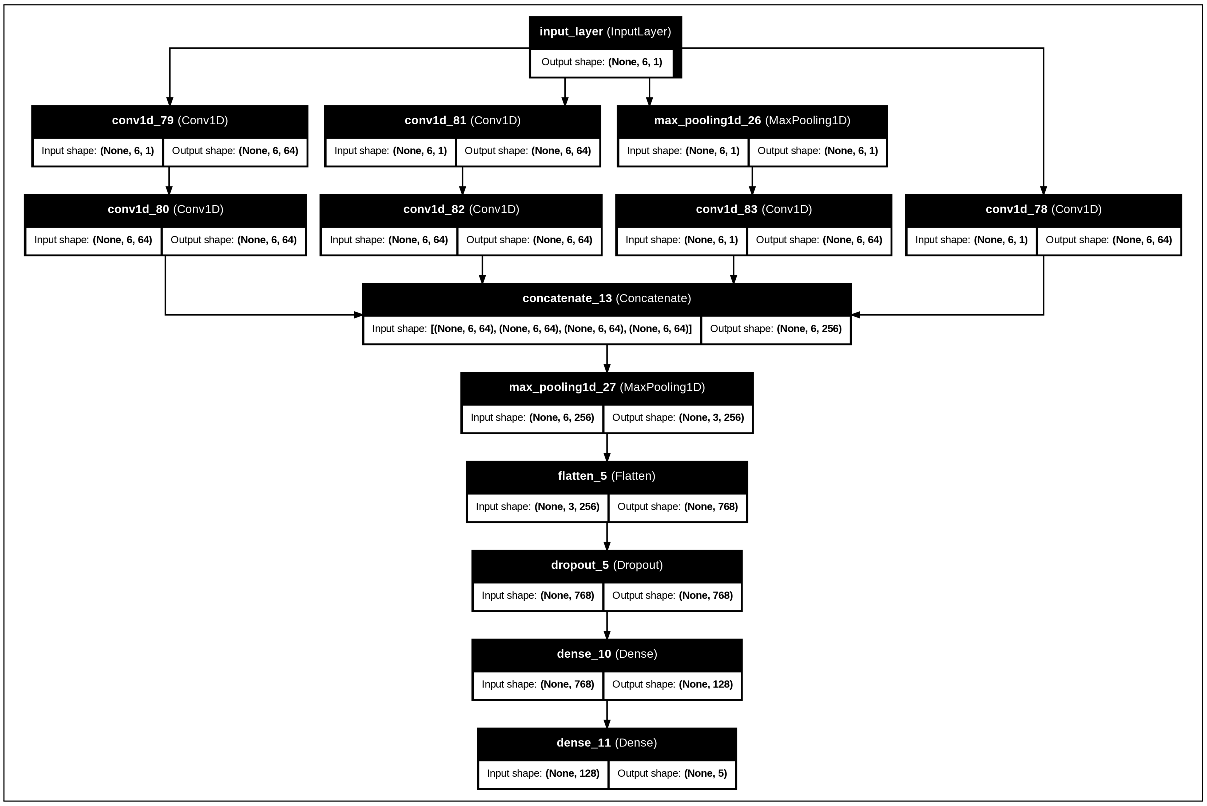

input_layer (InputLayer)
Output shape: (None, 6, 1)
conv1d_79 (Conv1D)
Input shape: (None, 6, 1)
Output shape: (None, 6, 64)
conv1d_81 (Conv1D)
Input shape: (None, 6, 1)
Output shape: (None, 6, 64)
max_pooling1d_26 (MaxPooling1D)
Input shape: (None, 6, 1)
Output shape: (None, 6, 1)
conv1d_80 (Conv1D)
Input shape: (None, 6, 64)
Output shape: (None, 6, 64)
conv1d_82 (Conv1D)
Input shape: (None, 6, 64)
Output shape: (None, 6, 64)
conv1d_83 (Conv1D)
Input shape: (None, 6, 1)
Output shape: (None, 6, 64)
conv1d_78 (Conv1D)
Input shape: (None, 6, 1)
Output shape: (None, 6, 64)
concatenate_13 (Concatenate)
Input shape: [(None, 6, 64), (None, 6, 64), (None, 6, 64), (None, 6, 64)]
Output shape: (None, 6, 256)
max_pooling1d_27 (MaxPooling1D)
Input shape: (None, 6, 256)
Output shape: (None, 3, 256)
flatten_5 (Flatten)
Input shape: (None, 3, 256)
Output shape: (None, 768)
dropout_5 (Dropout)
Input shape: (None, 768)
Output shape: (None, 768)
dense_10 (Dense)
Input shape: (None, 768)
Output shape: (None, 128)
dense_11 (Dense)
Input shape: (None, 128)
Output shape: (None, 5)

Fig. 2: Model Architecture

broader patterns, making it well-suited for complex electrical signals. Our approach addresses critical challenges like timely fault detection and anomaly identification, ensuring small issues do not escalate into major failures. It reduces false alarms, focuses on real risks, and scales effectively to handle large datasets. By combining deep learning with Inception's advanced feature extraction, this model enhances the reliability, efficiency, and security of electrical systems. Moving forward, this model could be integrated with real-time monitoring systems to enable continuous, autonomous operation. Expanding the training dataset to include more diverse fault scenarios and environmental conditions could further enhance its robustness. Additionally, incorporating explainable AI (XAI) techniques [19]–[21] could provide deeper insights into model predictions, making it easier for operators to trust and act on its outputs. Finally, applying this approach to other critical infrastructure, such as water or transportation systems, could broaden its impact and utility.

V. Conclusion

To sum up, our inception-based deep learning model has shown that it can reliably predict faults in electrical systems, helping us tackle problems before they get out of hand. Thanks to its parallel architecture, the model can pick up both fine details and big-picture patterns, making it an adequate tool for identifying and preventing potential issues. This study shows that deep learning is a practical and powerful solution to keep electrical systems secure, to fix problems on time, and to make operations more efficient in general. Future work will include integrating the model with real-time monitoring, expanding the dataset for diverse fault scenarios, applying transfer learning to other infrastructure domains, and using explainable AI to improve transparency and trust in predictions.

References

[1] M. Ibrahim and R. Elhafiz, "Security assessment of industrial control system applying reinforcement learning," *Processes*, vol. 12, no. 4, 2024.

[2] M. Ibrahim, A. Alsheikh, F. M. Awaysheh, and M. D. Alshehri, "Machine learning schemes for anomaly detection in solar power plants," *Energies*, vol. 15, no. 3, 2022.

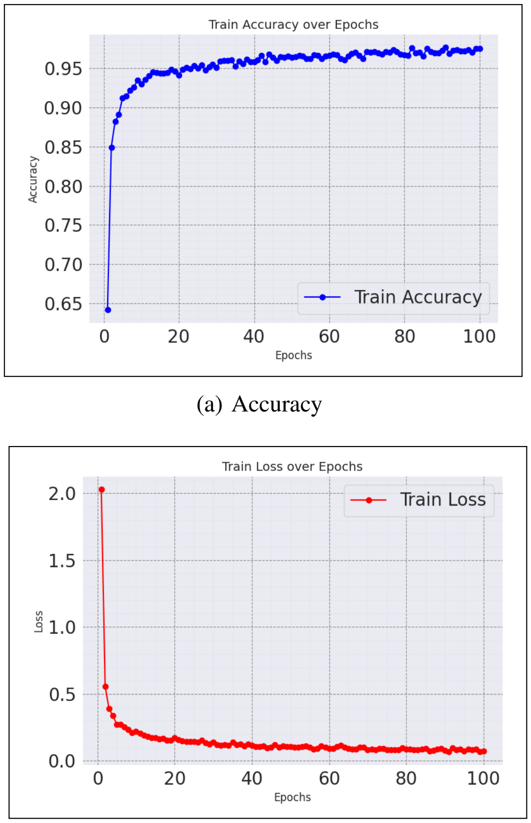
[3] M. Ibrahim, A. Alsheikh, and R. Elhafiz, "Resiliency assessment of power systems using deep reinforcement learning," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 2017366, 2022.

[4] S. F. Mihalache, E. Pricop, and J. Fattahi, *Resilience Enhancement of Cyber-Physical Systems: A Review*, pp. 269–287. Cham: Springer International Publishing, 2019.

[5] E. Pricop, J. Fattahi, N. Dutta, and M. Ibrahim, eds., *Recent Developments on Industrial Control Systems Resilience*, vol. 233 of *Studies in Systems, Decision and Control*. Springer Cham, 1 ed., 2020. Published: 05 October 2019 (eBook), 17 October 2019 (Hardcover), 17 October 2020 (Softcover). Copyright Springer Nature Switzerland AG 2020.

[6] J. Fattahi, "Machine Learning and Deep Learning Techniques used in Cybersecurity and Digital Forensics: a Review," *arXiv e-prints*, p. arXiv:2501.03250, Dec. 2024. https://ui.adsabs.harvard.edu/abs/2025arXiv250103250F.

[7] A. Aljuaid, M. Almohaya, and M. Anwar, "An early detection of oral epithelial dysplasia based on googlenet inception-v3," in *IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2022, Arlington, VA, USA, November 17-19, 2022*, pp. 172–173, IEEE, 2022.



(a) Accuracy

(b) Loss

Fig. 3: Training progression over epochs

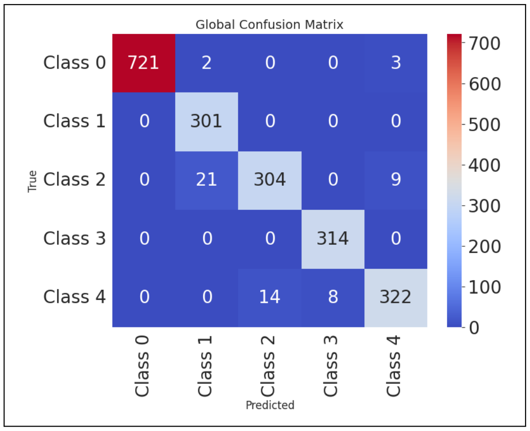
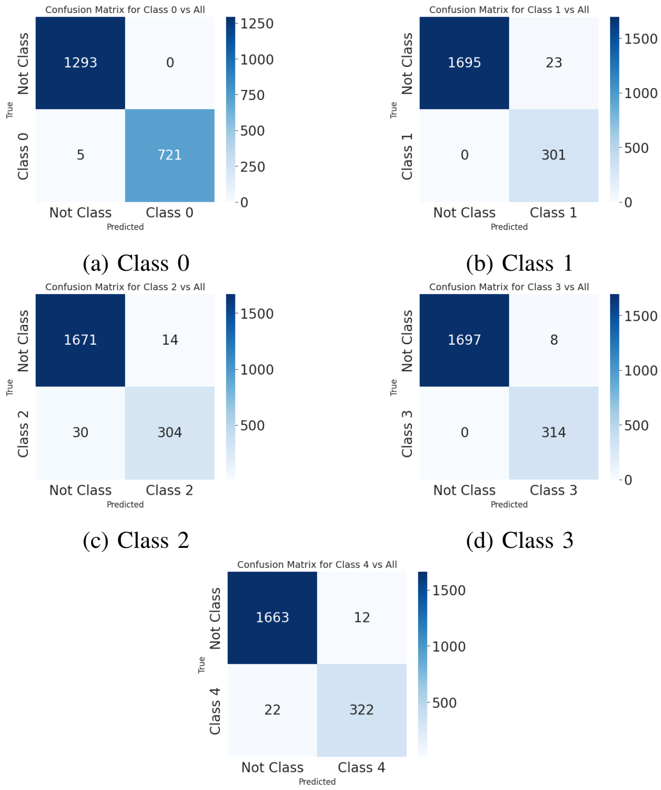


Fig. 4: Overall confusion matrix



(a) Class 0

(b) Class 1

(c) Class 2

(d) Class 3

(e) Class 4

Fig. 5: Confusion matrices for each class against all

[8] X. Wang, M. Zhong, H. Cheng, J. Xie, Y. Zhou, J. Ren, and M. Liu, "Spikegoogle: Spiking neural networks with googlenet-like inception module," *CAAI Trans. Intell. Technol.*, vol. 7, no. 3, pp. 492–502, 2022.

[9] Kaggle.com, "Electrical fault detection and classification: A collection of line currents and voltages for different fault conditions." https://www.kaggle.com/code/harshsingh2209/electrical-faults-analysis-classification/, n.d. Released under the Apache 2.0 open source license. Last accessed: January 15, 2025.

[10] J. Pereira, P. Oliveira, M. S. Duarte, G. Martins, and P. Novais, "Using deep learning models to predict the electrical conductivity of the influent in a wastewater treatment plant," in *Intelligent Data Engineering and Automated Learning - IDEAL 2023 - 24th International Conference, Évora, Portugal, November 22-24, 2023, Proceedings* (P. Quaresma, D. Camacho, H. Yin, T. Gonçalves, V. Julián, and A. J. Tallón-Ballesteros, eds.), vol. 14404 of *Lecture Notes in Computer Science*, pp. 130–141, Springer, 2023.

[11] J. Yao, Z. Wang, R. F. de Oliveira, Z. Wang, and L. Huang, "A deep learning method for the long-term prediction of plant electrical signals under salt stress to identify salt tolerance," *Comput. Electron. Agric.*, vol. 190, p. 106435, 2021.

[12] P. Chen, S. Liu, X. Wang, and I. Kamwa, "Physics-guided multi-agent deep reinforcement learning for robust active voltage control in electrical distribution systems," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 71, no. 2, pp. 922–933, 2024.

[13] A. Mohammadi, M. Jannati, and M. Shams, "Using deep transfer learning technique to protect electrical distribution systems against high-impedance faults," *IEEE Syst. J.*, vol. 17, no. 2, pp. 3160–3171, 2023.

[14] M. Carratù, V. Gallo, A. Pietrosanto, P. Sommella, G. Patrizi, A. Bartolini, L. Ciani, M. Catelani, and F. Grasso, "Anomaly detection on industrial electrical systems using deep learning," in *IEEE International Instrumentation and Measurement Technology Conference, I2MTC 2023, Kuala Lumpur, Malaysia, May 22-25, 2023*, pp. 1–6, IEEE, 2023.

[15] M. E. El-Telbany, "Prediction of the electrical load for egyptian energy management systems: Deep learning approach," in *Proceedings of the International Conference on Artificial Intelligence and Computer Vision, AICV 2020, Cairo, Egypt, 8-10 April, 2020* (A. E. Hassanien, A. T. Azar, T. Gaber, D. Oliva, and M. F. Tolba, eds.), vol. 1153 of *Advances in Intelligent Systems and Computing*, pp. 237–246, Springer, 2020.

[16] J. Fattahi, B. E. Lakdher, M. Mejri, R. Ghayoula, F. Sghaier, and L. Boumlik, "The good and bad seeds of CNN parallelization in forensic facial recognition," in *10th International Conference on Control, Decision and Information Technologies, CoDIT 2024, Vallette, Malta, July 1-4, 2024*, pp. 1719–1724, IEEE, 2024.

[17] J. Fattahi, F. Sghaier, M. Mejri, S. Bahroun, R. Ghayoula, and E. Manai, "Cyberbullying detection using bag-of-words, tf-idf, par-

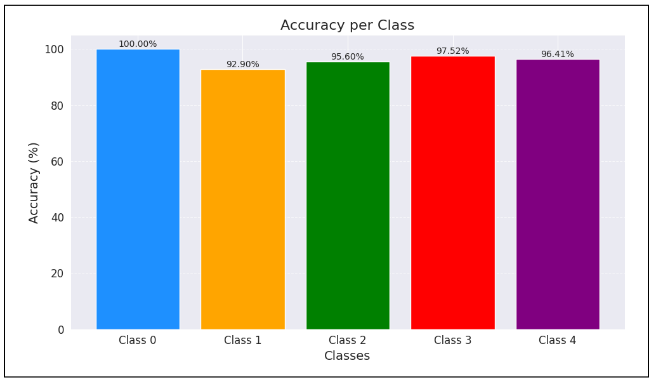


Fig. 6: Model accuracy

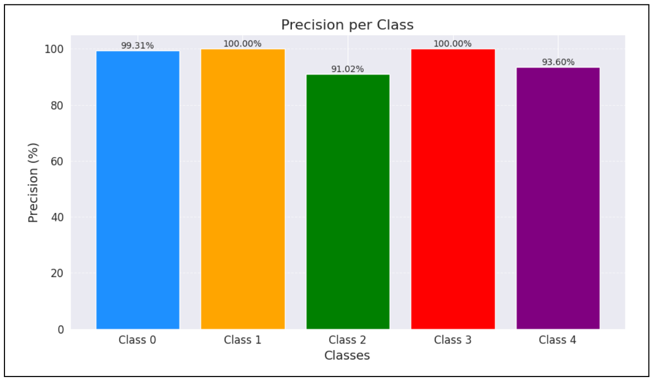


Fig. 7: Model precision

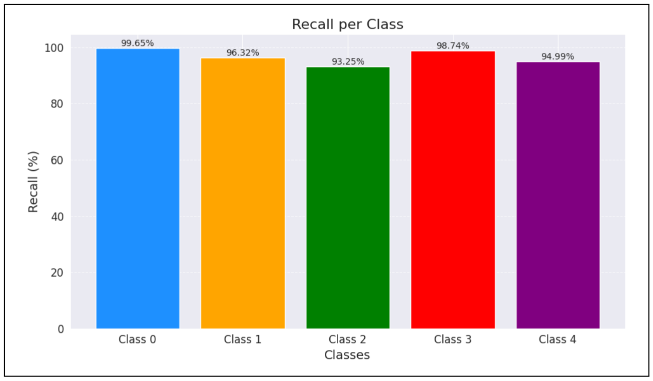


Fig. 8: Model recall

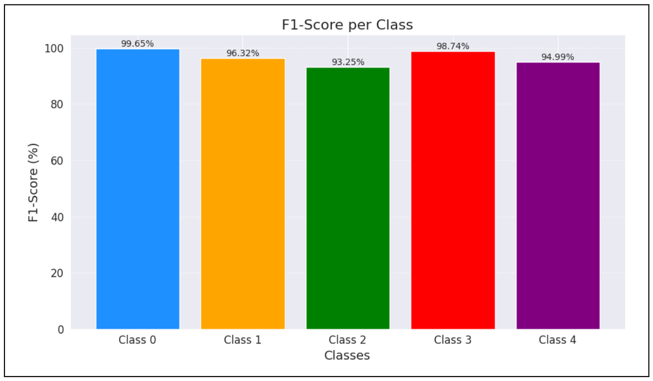


Fig. 9: Model F1-score

allel cnns and bilstm neural networks," in *New Trends in Intelligent Software Methodologies, Tools and Techniques - Proceedings of the 23rd International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT_24), Cancun, Mexico, September 24-26, 2024* (H. Fujita, H. M. P. Meana, and A. Hernandez-Matamoros, eds.), vol. 389 of *Frontiers in Artificial Intelligence and Applications*, pp. 72–84, IOS Press, 2024.

[18] J. Fattahi, F. Sghaier, M. Mejri, R. Ghayoula, E. Pricop, and B. E. Lakdher, "Handwritten signature recognition using parallel cnns and transfer learning for forensics," in *10th International Conference on Control, Decision and Information Technologies, CoDIT 2024, Vallette, Malta, July 1-4, 2024*, pp. 1697–1702, IEEE, 2024.

[19] E. Manai, M. Mejri, and J. Fattahi, "Helping cnas generate cvss scores faster and more confidently using xai," *Applied Sciences*, vol. 14, no. 20, 2024.

[20] E. Manai, M. Mejri, and J. Fattahi, "Fingerprint fraud explainability using grad-cam for forensic procedures," in *New Trends in Intelligent Software Methodologies, Tools and Techniques - Proceedings of the 23rd International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT_24), Cancun, Mexico, September 24-26, 2024* (H. Fujita, H. M. P. Meana, and A. Hernandez-Matamoros, eds.), vol. 389 of *Frontiers in Artificial Intelligence and Applications*, pp. 457–470, IOS Press, 2024.

[21] E. Manai, M. Mejri, and J. Fattahi, "Minimizing model misclassification using regularized loss interpretability," in *16th IIAI International Congress on Advanced Applied Informatics, IIAI-AAI 2024, Takamatsu, Japan, July 6-12, 2024*, pp. 231–236, IEEE, 2024.