Cyber-Attack Detection of Power Converters in Isladed Microgrids using Deep Learning Approaches

Nanthaluxsan E.
Department of Electrical Engineering,
University of Moratuwa,
Colombo, Sri Lanka
nanthaluxsane.19@uom.lk

Jalini S.
Department of Electrical Engineering,
University of Moratuwa,
Colombo, Sri Lanka
jalinis.19@uom.lk

Kopikanth K.
Department of Electrical Engineering,
University of Moratuwa,
Colombo, Sri Lanka
kopikanthk.19@uom.lk

Dr.V.Logeeshan
Department of Electrical Engineering
University of Moratuwa
Colombo, Sri Lanka
logeeshanv@uom.lk

Prof.Sisil Kumarawadu
Department of Electrical Engineering
University of Moratuwa,
Colombo, Sri Lanka
sisil@uom.lk

***Abstract*— Islanded microgrids have emerged as essential components in enhancing the sustainability and efficiency of electricity distribution in modern power systems. They play a vital role in advancing renewable energy adoption and reducing transmission losses. However, as communication and control technologies in microgrids evolve, the susceptibility to cyber threats targeting power converters has increased. This study introduces a deep learning-based model designed to detect and classify cyber-attacks, specifically focusing on False Data Injection (FDI) and Denial of Service (DOS) attacks targeting solar inverters, battery inverters, and DC to DC boost converters. The proposed model employs deep learning techniques to analyze real-time data and identify anomalies indicative of cyber-attacks. To validate the effectiveness of the approach, real-time tests are conducted using MATLAB, simulating various attack scenarios over time. This deep learning-based solution provides a scalable and dependable method for safeguarding the electrical infrastructure of islanded microgrids, addressing a critical need in the sector.**

Keywords— Islanded Microgrid, power converter, cyber-attack, False Data Injection (FDI), Denial of Service (DoS)

I. Introduction

In the evolving landscape of modern energy systems, islanded microgrids have become pivotal for delivering reliable and sustainable power, especially in remote or isolated areas. These microgrids operate independently from the main power grid, integrating various renewable energy sources and advanced power converters. However, their increasing reliance on digital control systems makes them susceptible to cyber-attacks. This project, titled "Cyber-Attack Detection of Power Converters in Islanded Microgrid Using Deep Learning Approaches," aims to enhance the security and resilience of islanded microgrids against cyber threats. By developing a robust detection system using deep learning methodologies, specifically Artificial Neural Networks (ANNs), the project focuses on identifying and mitigating Denial of Service (DoS) and False Data Injection (FDI) attacks. Through detailed modeling and simulation in MATLAB, this study seeks to provide comprehensive strategies for safeguarding microgrid infrastructures from evolving cyber threats, ensuring reliable energy delivery and system integrity.

II. Islanded Microgrid

An islanded microgrid refers to a microgrid that is operating independently from the main grid. A remote village uses solar panels and a wind turbine with battery storage to supply its power needs. Although the UOM microgrid is grid-connected, we are using it as a reference to model an islanded microgrid. Our project also assesses the feasibility and value of operating a microgrid in islanded mode [7]. Microgrids offer a compelling answer to the global energy crisis by reducing transmission and distribution losses, promoting renewable energy sources, cutting carbon emissions, reducing costs, and minimizing large land use.

Islanded microgrids provide vital power solutions for various applications. They enhance living standards in remote and rural areas, support military base operations with secure power, and ensure connectivity for telecommunications during disasters. In agriculture, power irrigation and greenhouses, promoting sustainability. Mining operations in distant locations and islands benefit from reliable, renewable energy. Advancements in technology and investments promise a bright future for microgrids, fostering a sustainable energy landscape.

A. *Microgrid model in Matlab*

Our microgrid design draws inspiration from the UOM microgrid, utilizing its load profiles for various facilities.
Our design includes as load a new administration building requiring 100 kW of power, a canteen with a power demand of 50 kW, the Sumanadasa building, which has a load requirement of 200 kW.

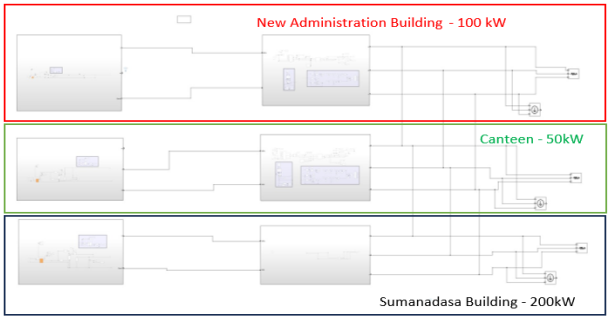

Fig. 1. Microgrid model design showing load in UOM

Our project focuses on exploring cyber-attacks targeting power converters, specifically solar inverters, battery inverters, and DC to DC Boost Converters.

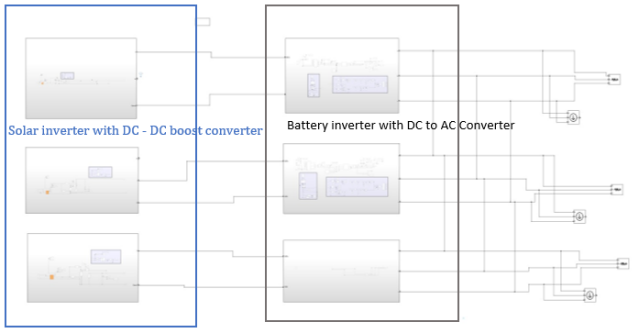

Fig. 2. Microgrid model design showing power converters

B. Solar inverter

Equipped with multiple DC inputs, they optimize efficiency through maximum power point tracking. Inverters connect to PV AC combiner panels, distributing power to buildings. Communication via RS485 lines with the DHYBRID platform enables monitoring and control, regulating power setpoints to prevent battery overcharging, especially in islanded mode scenarios. [4]

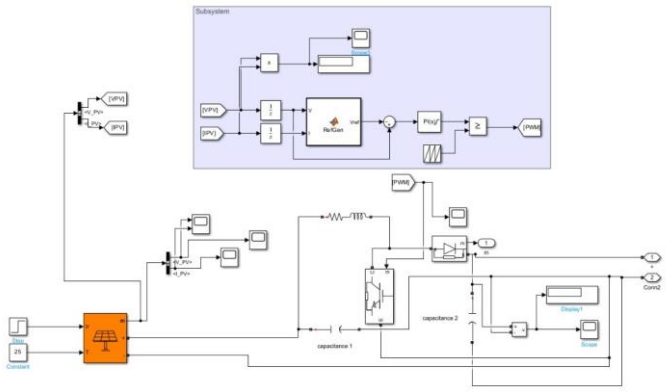

Fig. 3. Designed Solar inverter with DC-to-DC boost converter in MATLAB

C. Battery inverter

The battery inverter is vital in islanded microgrids, converting DC power from batteries to AC and vice versa. It operates bidirectionally, providing active and reactive power. In grid mode, it syncs with the grid; off-grid, it acts as a virtual synchronous generator, controlling voltage and frequency. It adjusts output frequency based on load and PV production, managing reactive power to regulate voltage.

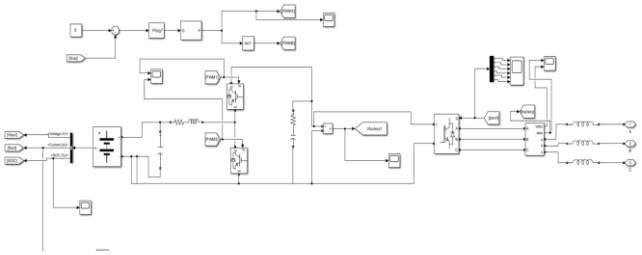

Fig. 4. Designed Battery inverter in MATLAB

D. DC to AC converter

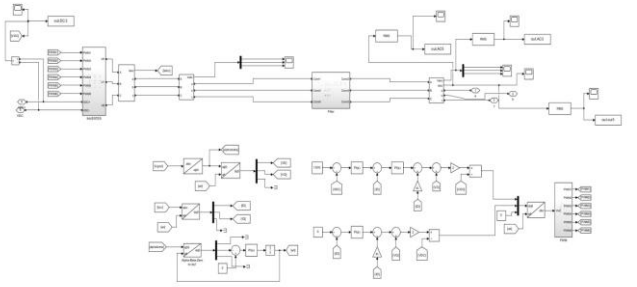

Fig. 5. Designed DC to AC Converter in MATLAB

III. Cyber-attacks

Cyber-attacks pose significant threats to microgrids, especially in sensitive areas requiring reliable electricity. These attacks can disrupt energy generation, distribution, and storage. Protecting microgrids is essential for maintaining secure power supplies. Despite their advantages, the centralization of monitoring and control systems in a cloud environment increases the risk of cyber-attacks, making it crucial to address these vulnerabilities to ensure the security and reliability of microgrid operations.[1]

A. Historical Cyber-Attacks on Power Systems

Recent decades have seen numerous cyber-attacks targeting the energy sector, causing significant disruptions. Notable incidents include the Mumbai power outage, the 2015 Kyiv blackout, and the 2021 Natanz nuclear facility attack. These events highlight the vulnerabilities of urban energy systems and national infrastructure to cyber threats. The May 2021 ransomware attack on U.S. oil pipelines further underscores the economic and logistical impacts. These incidents emphasize the urgent need for robust cybersecurity measures to protect the energy sector and ensure the reliability of essential services.

B. cyber-attacks classification in microgrid

1) Attacks on Data Integrity

These attacks can corrupt measurements or command signals within the communication network, leading to malfunctions in the microgrid and affecting its control systems. A notable example of an attack compromising data integrity is the False Data Injection (FDI) attack. FDI attacks are among the most challenging threats for microgrids, and their impacts on modern power grids can be severe and unacceptable. [3]

FDI attack Mathematical model

$$Y_F(t) = \alpha * Y_O(t) + \beta \quad (1)$$

- $\alpha \neq 0$, $\beta = 0$, this attack manipulates the real measurement by α
- $\alpha = 0$, $\beta \neq 0$, this attack replaces the real measurement by β
- $\alpha = 1$, $\beta = 0$, there is no attack in controller.

From this model we classified FDI attack in our project as 3 cases,

- FDI Case1 - $\alpha \neq 1, \beta > 0$
- FDI Case2 - $\alpha \neq 1, \beta = 0$
- FDI Case3 – $\alpha = 1, \beta > 0$

2) Attacks on Data Availability

The cybersecurity system must ensure timely and accessible data, which is essential for controlling power electronics converters in smart microgrids, particularly in islanded mode and during transient events. Attacks aimed at obstructing or delaying data communications are known as attacks on data availability which is commonly referred to Denial of service (DoS). DOS attack model used as $\alpha = 0$, $\beta = 0$ in the equation (1). Attackers can employ DoS attacks targeting the communication links while FDI attack targeting controller.[5]

3) Attacks on Data Confidentiality

Cyber-attacks that breach confidentiality enable hackers to eavesdrop on the communication network, gaining access to sensitive information about customers and microgrid operation and control strategies. While these attacks may not immediately disrupt microgrid operations, they pose significant privacy and security risks.[6] In our project, we employ False Data Injection (FDI) attacks in three distinct cases, along with Denial of Service (DoS) attacks, which has more impact on microgrid and attacker commonly willing to use these types.

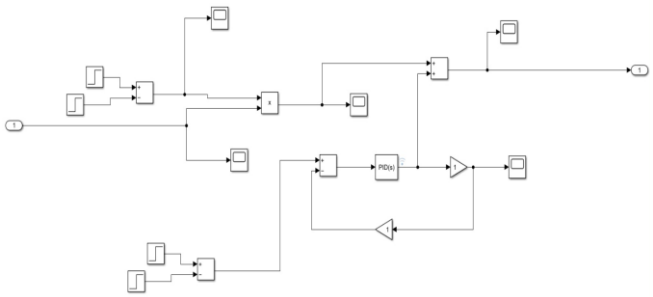

Figure 6. Cyber-attack model

Our project investigates cyber-attacks on power converters, identifying potential vulnerabilities and exploring their implications. Attack areas can vary within power converters and are analyzed using matrix equations.

Equation (1),

$$\begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

In our project, we adjust matrix values for alpha (a11, a22) and beta (b1, b2) to optimize accuracy in detecting and classifying cyber-attacks on power converters. We prioritize minimal threshold values, informed by potential cyber attackers' strategies, objectives, and anticipated system impact. We consider that in all our scenarios, the cyber-attack occurs within 2 to 4 seconds. We observe how it impacts the system and how the values differ before, during, and after the attack. When we increase the values of α and β, we observe a significant increase in the difference. Cyber-attacks on a battery inverter requires higher α and β values than a solar inverter to cause significant variations due to its primary role as a storage device.

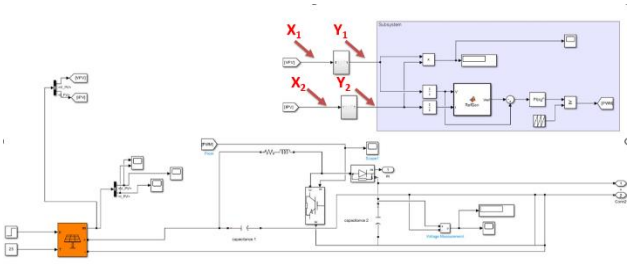

Fig. 7. Solar inverter with DC - DC boost converter with Attack

IV. RESULTS

A. FDI Case1

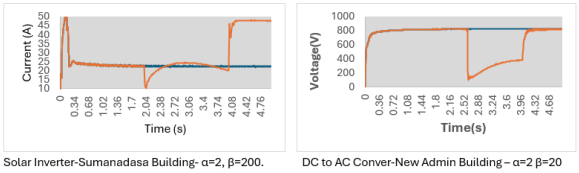

Fig. 8. Solar inverter-FDI Case 1, current and DC voltage respectively

B. FDI Case2

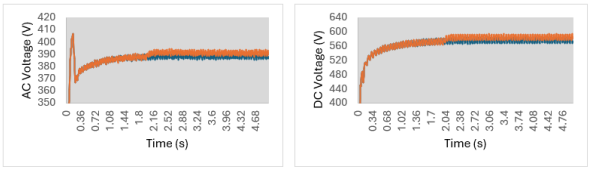

Fig. 9. Battery Inverter-Canteen α=50, β=0

C. FDI Case 3

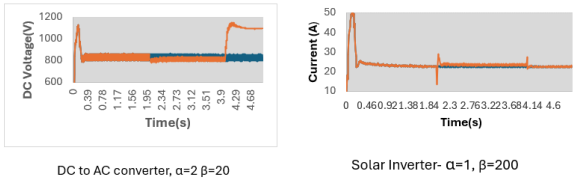

Fig. 10. Solar Inverter-Sumanadasa building, α=1, β=200

D. DOS attack

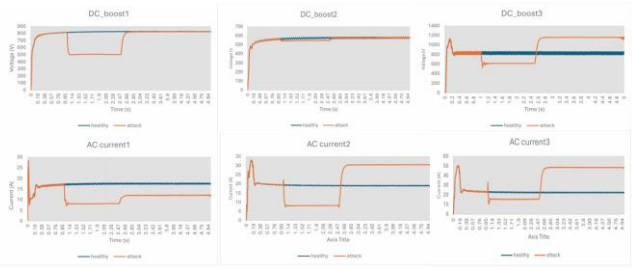

Fig. 11. DoS attack of DC Voltage and AC current in Solar Inverter

----healthy -----Attack

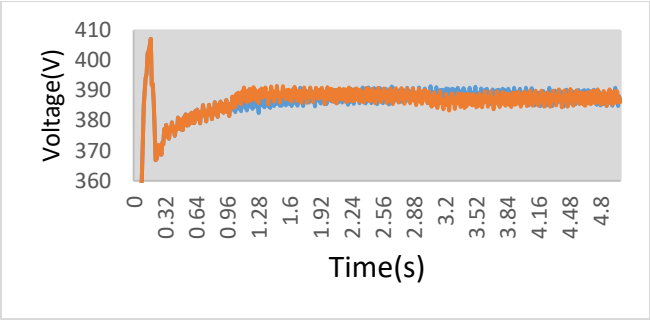

Fig. 12. AC Voltage-DOS Attack-Battery Inverter

V. EXPERIMENT AND EVALUATION

Proposed data-driven evaluation approach method directly applied to the output of the Islanded microgrid MATLAB model. Applied cyber-attacks in the time intervals to model. record the output data and label it. Based on the label data, applied the data processing methods. After that start to train the data-driven methods. Under evaluation of methods consider precision, f1-score, recall, accuracy, MSE (Mean Squared Error), MAE (Mean Absolute Error), and validation loss. Also, consider the ROC (Receiver Operating Characteristic curve)[2]

$$\text{MSE} = \frac{1}{n}\sum(\bar{y} - y)^2 \quad (2)$$

$$\text{MAE} = \frac{1}{n}\sum|\bar{y} - y| \quad (3)$$

$$\text{Accuracy} = \frac{TN+TP}{TN+TP+TN\pm FP+FN} \quad (4)$$

$$\text{Precision} = \frac{TP}{TP+TN} \quad (5)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (6)$$

$$\text{f1-score} = \frac{2\times TP}{2\times TP+TN\pm FP+FN} \quad (7)$$

$\bar{y}$ is predicted output, y is actual output, and n is the number of data points True Positive (TP) is a correct positive prediction, while True Negative (TN) is a correct negative prediction. False Positive (FP), or Type I Error, occurs when a positive prediction is incorrect, and False Negative (FN), or Type II Error, occurs when a negative prediction is incorrect.

A. Data Preprocessing

The basic step is data analysis to understand how the relationships between variables and data are distributed. Data cleaning focuses on handling missing values and detecting and removing outliers. Data transformation involves normalization, removing duplicates, encoding categories, and discretization. Feature engineering is used to select relevant features and create new features from existing ones to identify patterns. Data integration involves combining data from different sources and resolving inconsistencies, while data reduction aims to simplify the dataset.

In data processing, the input data window size is (10,9) each window is assigned a label based on the maximum frequency of outputs within those 10 rows. 10 rows and 9 features are combined into a matrix. To address this, the ANN and LSTM models were designed to accept two-dimensional input with a window size of 10 rows and 9 features. The process involves sliding the window from the 1st to the 10th row, then from the 2nd to the 11th row, and so on.

B. Model training

1) FNN model for detection

Implementing a hyperparameter tuning process for an ANN model using a grid search technique. the model has three hidden layers with 128, 64, and 32 neurons, respectively, activated by ReLU. The input layer accepts 2D input, and the output layer uses the sigmoid activation function. Using grid search, we determined the optimal configuration, including dropout rates, to enhance performance. early stopping is also used to measure validation loss that value is 0.01. it monitors 10 epochs tIt waits for 10 epochs to check the validation loss's change. If the change is not significant, it stops the training. This method stops training when the validation performance gets worse, preventing overfitting and keeping the best weight. The defined epoch is 50 and the batch size is 20. The model is trained using the training data set.

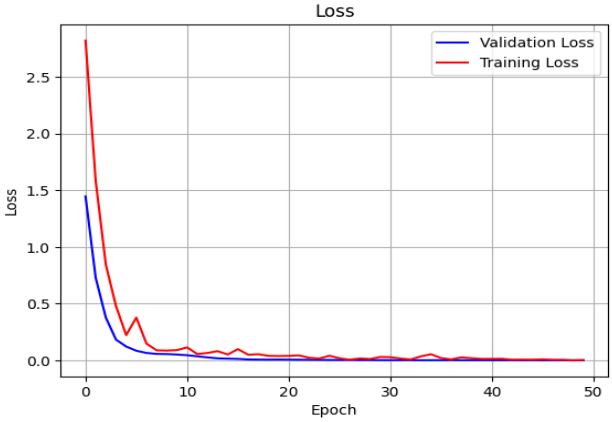

Fig. 13. Loss curve of training and validation loss of FNN model for detection

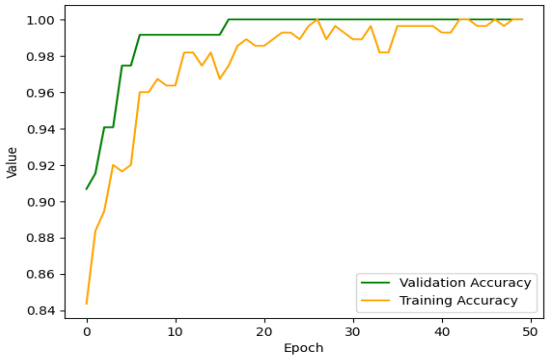

Fig. 14. Accuracy curve of training and validation of FNN model for detection

2) LSTM model for detection

The LSTM model consists of four LSTM layers, each with 50 units of neutrons, which process sequential data by maintaining 50-dimensional hidden states. After each LSTM layer, a dropout rate of 0.2 is applied to reduce overfitting. The final Dense layer with a sigmoid activation outputs a binary classification. under the training.

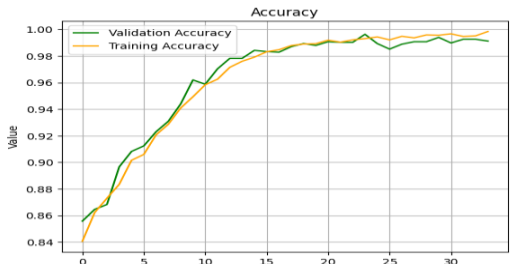

Fig. 15. Accuracy curve of training and validation of LSTM model for detection

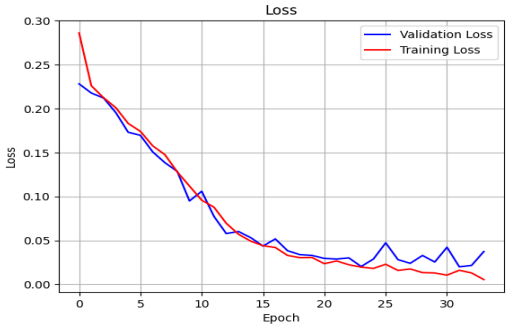

Fig. 16. Loss curve of training and validation loss of LSTM model for detection

3) FNN model for classification

Grid search algorithm to identify the number of neutrons in each hidden layer. It gives the best parameters for each data set. want to find the best set of parameters that give the highest performance for most of the inputs. Based on the results of the grid search,128, 64,64, and 32 are the number of neutrons that are contained by hidden layers in order from the input layer. It gives higher performance compared to other sets of parameters. Under the training.

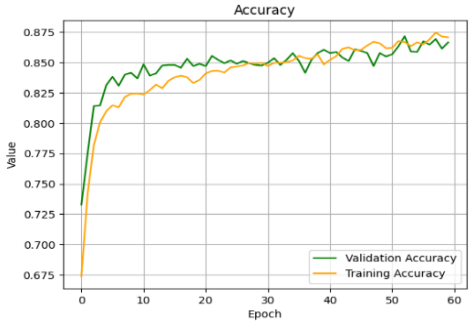

Fig. 17. Accuracy curve of training and validation of FNN model for classification

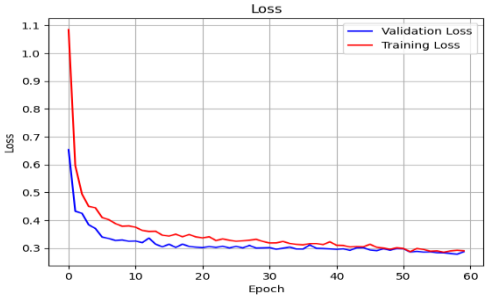

Fig. 18. Accuracy curve of training and validation of FNN model for detection

C. Evaluation of the model

1) FNN model for detection

Based on the testing accuracy of the model is changed. Continuously monitor the values. Took the average value of performance measurement.

Table I. Results of the FNN model for the detection

Binary Cross entropy	0.2782528533975387
Mean Squared Error	0.040759421559616586
Binary Accuracy	0.9532712267504798
Precision	0.9329721497164832
Recall	0.9497611853811476

2) LSTM model for detection

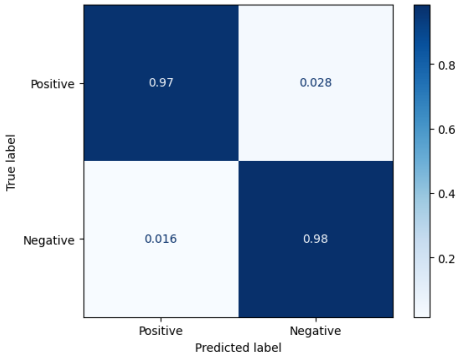

Fig. 19. Confusion matrix of FNN model for detection

Based on the evaluation LSTM model shows high performance in cyber-attack detection. Below average results. LSTM shows superior high memory capacity's has better performance than ANN. It achieves an average accuracy of 96.6%.

Table II. Results of the LSTM model for the detection

Binary Cross entropy	0.171276028606702
Mean Squared Error	0.030489846938673345
Binary Accuracy	0.9660238731991161
Precision	0.9901613593101501
Recall	0.930474888194691

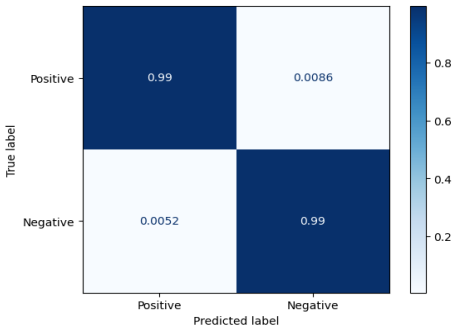

Fig. 20. Confusion matrix of LSTM model for detection

3) FNN model for classification

FDI and DOS classification which is done by FNN Network to identify which attacks happen at a particular time interval. The results are shown below.

Table. III. Results of the FNN model for the classification

Cross-entropy	0.37810681282112807
Mean Squared Error	0.045587739754969686
Mean Absolute Error	0.08357285286407344
Accuracy	0.9014673943702991
Precision	0.9014555009511801
Recall	0.9010788935881394
F1_score	0.924886943388293

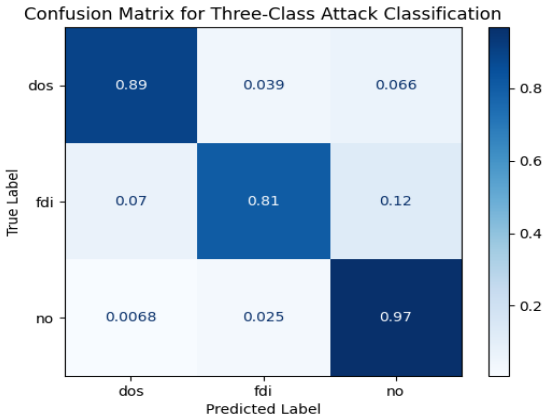

Fig. 21. Confusion matrix of FNN model for classification

VI. Conclusions

Numerous graphs were generated to train a cyber-attack detection and classification model, identifying high-impact attacks on power converters. DoS attacks have a relatively low impact compared to three FDI cases, with FDI Case 1 having the highest impact. DC to AC converters are particularly vulnerable due to their integration into grid systems and reliance on digital communication, while battery inverters are the least vulnerable. The ANN model achieves a detection accuracy of 0.9533, the LSTM model achieves 0.9660 and ANN model achieves a classification accuracy of 0.901. Future work includes fine-tuning these models and hardware implementation.

Acknowledgment

The successful completion of this project required significant guidance and support from many individuals. Gratitude is extended to project supervisors, Senior Prof. Sisil Kumarawadu and Dr. V. Logeeshan, for their invaluable support and encouragement, which were instrumental in the project's success.

References

[1] Gupta, K., Sahoo, S., Panigrahi, B. K., Blaabjerg, F., & Popovski, P. (2021). On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids. *Energies*, *14*(16), 4941. doi: 10.3390/en14164941

[2] Q. Li, F. Li, J. Zhang, J. Ye, W. Song and A. Mantooth, "Data-driven Cyberattack Detection for Photovoltaic (PV) Systems through Analyzing Micro-PMU Data," *2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, Detroit, MI, USA, 2020, pp. 431-436, doi: 10.1109/ECCE44975.2020.9236274.

[3] A. S. Musleh, G. Chen and Z. Y. Dong, "A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids," vol. 11, no. 3, pp. 2218-2234, May 2020, doi: 10.1109/TSG.2019.2949998.

[4] J. Poon, P. Jain, I. C. Konstantakopoulos, C. Spanos, S. K. Panda and S. R. Sanders, "Model-Based Fault Detection and Identification for Switching Power Converters," vol. 32, no. 2, pp. 1419-1430, Feb. 2017, doi: 10.1109/TPEL.2016.2541342.

[5] Barua, A., & Faruque, M. a. A. (2020). Hall Spoofing: A Non-Invasive DOS attack on Grid-Tied solar inverter. *USENIX Security Symposium*, 1273–1290. doi: 10.5555/3489212.3489284.

[6] Nejabatkhah, F., Li, Y. W., Liang, H., & Ahrabi, R. R. (2020). Cyber-Security of smart microgrids: A survey. *Energies*, *14*(1), 27. doi: 10.3390/en14010027

[7] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li and J. Zhang, "A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids," in *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929-1938, May 2021, doi: 10.1109/TSG.2020.3047949.