ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun622

Random Forest Approach for Enhancing Resilience Against False Data Injection in Power Distribution Systems

Sony Venugopal[1]; Yogini S.[2]; Sameeksha M. V.[3]

[1;2;3]RNS Institute of Technology

Publication Date: 2026/06/20

Abstract: False Data Injection (FDI) attacks represent a critical cyber-security threat to modern smart grids, as they deliberately manipulate measurement data used for system monitoring and control while remaining difficult to detect using conventional techniques. This paper presents a machine learning-based framework for the detection and localization of FDI attacks in power distribution systems. An IEEE 5-Bus test system is modeled and simulated in the MATLAB/Simulink environment to generate voltage measurements under normal operating conditions. FDI attack scenarios are created by selectively altering bus voltage data to emulate compromised measurement states without disturbing the physical dynamics of the system. Voltage magnitude features extracted from the simulation data are used to train a Random Forest classifier for identifying abnormal operating conditions and localizing the attacked bus. Simulation results demonstrate that the proposed approach effectively detectsThe results highlight the potential of integrating power system simulation with datadriven machine learning techniques to enhance cyber-security and situational awareness in smart grid applications.

Keywords: *False Data Injection Attack, Smart Grid Cyber Security, IEEE 5-Bus System, Machine Learning, Random Forest, Attack Detection and Localization.*

How to Cite: Sony Venugopal; Yogini S.; Sameeksha M. V. (2026) Random Forest Approach for Enhancing Resilience Against False Data Injection in Power Distribution Systems. *International Journal of Innovative Science and Research Technology*, 11(6), 683-689. https://doi.org/10.38124/ijisrt/26jun622

I. INTRODUCTION

The evolution of conventional power grids into smart grids has significantly enhanced the efficiency, reliability, and flexibility of power system operation. Through the integration of advanced sensing, communication, and automation technologies, smart grids enable real-time monitoring, bidirectional information flow, and intelligent control of generation, transmission, and distribution networks.These advancements support the large-scale integration of renewable energy sources, electric vehicles, and dynamic load management

Despite these benefits, the increasing dependence on digital communication and data-driven decision-making has expanded the cyber-attack surface of modern power systems.(1),(5),(9).Measurement data obtained from sensors, smart meters, and supervisory control and data acquisition

(SCADA) systems play a crucial role in state estimation, protection, and control. Any compromise in data integrity can result in incorrect operational decisions, degraded reliability, or large-scale system failures.

Among various cyber threats, False Data Injection (FDI) attacks are particularly dangerous due to their stealthy nature(2),(3). In an FDI attack, an adversary deliberately alters measurement data to misrepresent the actual system state while bypassing conventional bad data detection schemes. In power systems, carefully crafted false voltage or power measurements can mislead state estimation algorithms, leading to voltage instability, line overloading, or cascading outages.

To address these challenges, machine learning–based techniques have gained increasing attention for cyber-attack detection in smart grids(1),(4),(10). Unlike traditional rulebased methods, machine learning algorithms can learn complex and nonlinear relationships directly from data. In this paper, a Random Forest–based approach is proposed for detecting and localizing FDI attacks using voltage magnitude measurements obtained from an IEEE 5-Bus power system modeled in MATLAB/Simulink(7).

II. SYSTEM DESCRIPTION

The proposed framework is evaluated using a standard IEEE 5-Bus power system modeled and simulated in the MATLAB/Simulink environment.

The IEEE 5-Bus system is widely used as a benchmark network for power system analysis and cyber-security research

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun622

due to its simplicity, computational efficiency, and ability to represent essential grid operating characteristics.

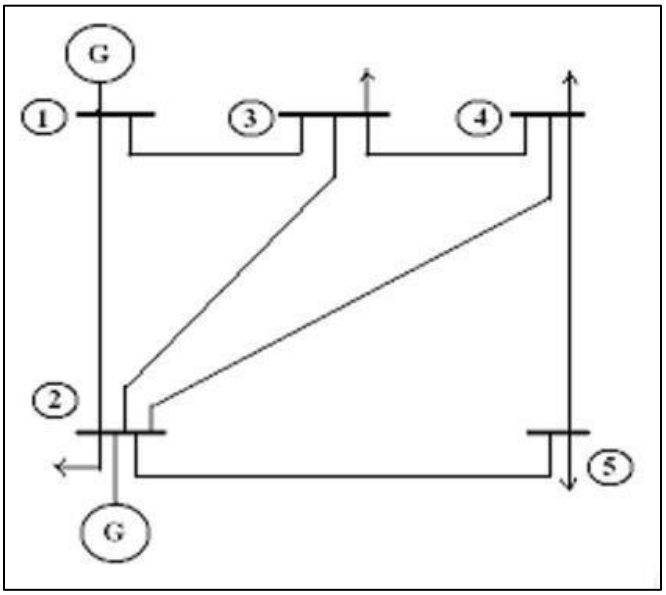

Fig 1 Single Line Diagram of 1EEE 5 Bus System

The system consists of five interconnected buses operating at a base voltage of 10 kV. Two generating units are connected at Bus 1 and Bus 2. Bus 1 functions as the swing (slack) bus, maintaining system power balance by providing a fixed voltage magnitude and reference phase angle. Bus 2 operates as a PV bus, where active power output and voltage magnitude are specified, and reactive power is adjusted to maintain voltage regulation. Buses 3, 4, and 5 are modeled as PQ buses representing load buses with predefined real and reactive power demands.

All buses are interconnected through three-phase transmission lines forming a meshed network topology. Multiple power flow paths enhance operational flexibility and improve system reliability under abnormal conditions. Distributed three-phase loads are placed at Buses 2, 3, 4, and 5 to represent realistic demand distribution. System parameters are expressed using the per-unit system to simplify analysis and ensure numerical stability.

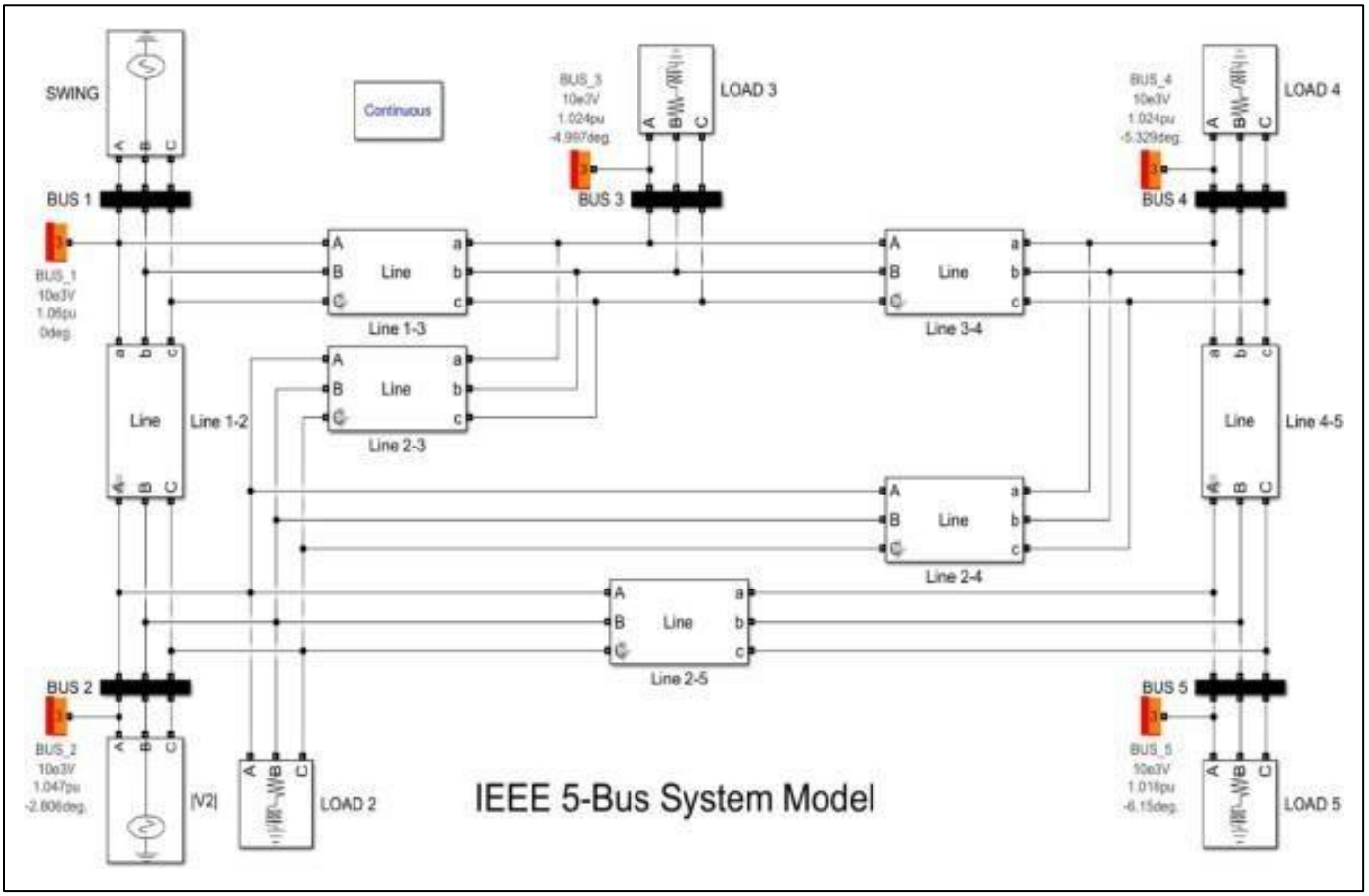

Fig 2 IEEE 5 Bus Model

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun622

Voltage measurement blocks are installed at each bus to continuously record three-phase voltages. These measurements form the primary dataset used for normal operation analysis and FDI attack detection.

III. METHODOLOGY

The proposed methodology integrates power system simulation with machine learning–based analysis for the detection and localization of False Data Injection attacks. The overall framework consists of four stages: power system modeling and data acquisition, FDI attack simulation, feature extraction and dataset preparation, and machine learning-based detection and localization.

Under normal operating conditions, the IEEE 5-Bus system is simulated in MATLAB/Simulink as a three-phase network using Simscape Electrical components. Voltage measurements for all three phases are obtained at each bus using V-I measurement blocks and exported to the MATLAB workspace using *To Workspace* blocks. These measurements form the baseline dataset representing healthy system operation.

FDI attack scenarios are generated by deliberately modifying voltage measurements at one bus at a time while keeping the remaining measurements unchanged. This approach accurately reflects the stealthy nature of real FDI attacks, which target data integrity without disturbing physical system dynamics. Multiple attack cases are generated to create a labeled dataset consisting of normal and compromised operating states.

Voltage magnitude is selected as the primary feature for analysis to reduce computational complexity while preserving essential system information. The extracted features are used to train a Random Forest classifier.

During testing, the trained model detects the presence of an FDI attack and identifies the specific bus under attack.

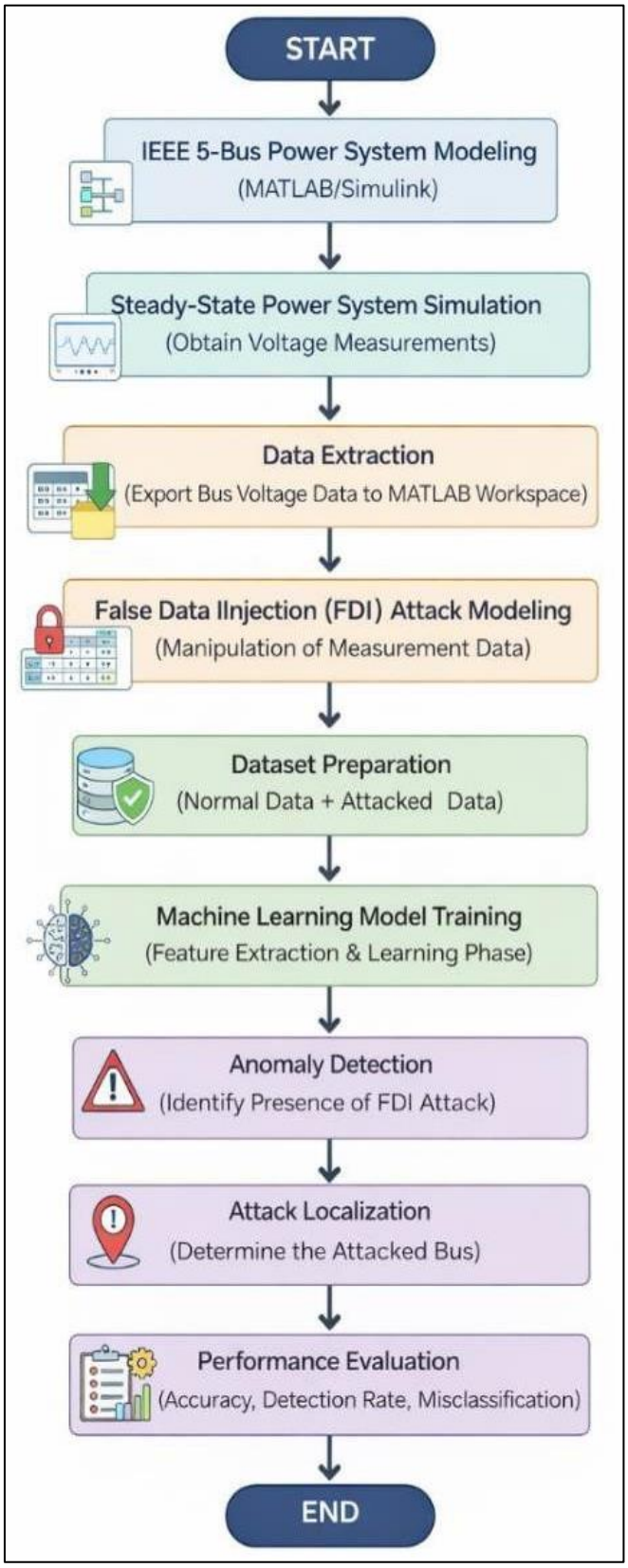

Fig 3 FDI Attack Detection Flow Chart

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun622

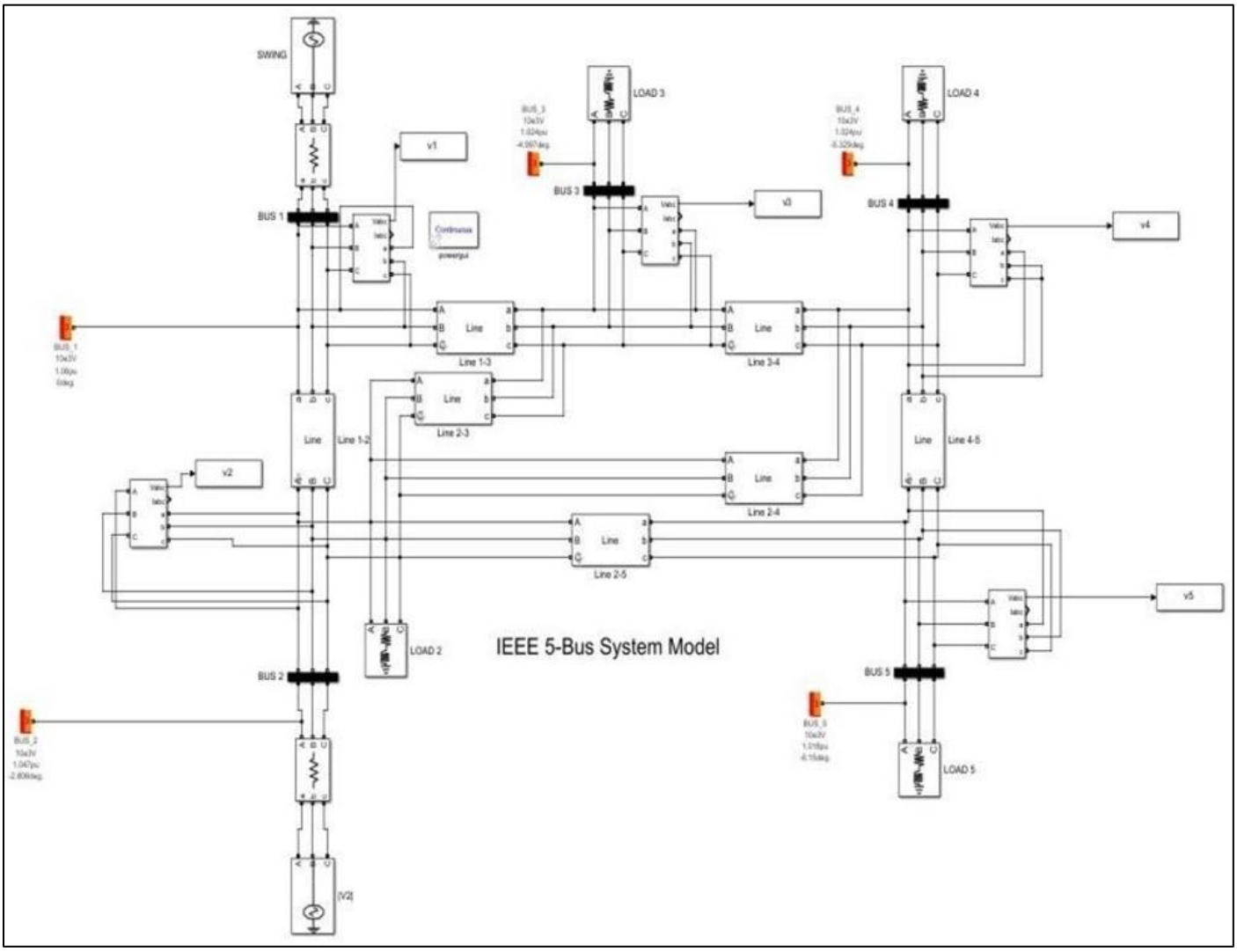

Fig 4 MATLAB Simulation Model

IV. RESULT AND DISCUSSION

The effectiveness of the proposed False Data Injection (FDI) attack detection framework is evaluated using voltage magnitude data obtained from simulation of the IEEE 5-Bus system. The analysis is carried out under normal operating conditions and under intentionally injected FDI attack scenarios. The results are presented using graphical representations to clearly illustrate system behavior and the performance of the machine learning model.

➢ *Voltage Profile Under Normal Operating Conditions:*

The bar graph represents steady-state voltage magnitudes measured at each bus. As expected, Bus 1 and Bus 2 exhibit comparatively higher voltage magnitudes since they are directly connected to generator units and are responsible for voltage regulation.

In contrast, Buses 3 and 4 show relatively lower voltage magnitudes due to their location as load buses and the presence of power flow through transmission lines, which introduces voltage drops. Bus 5 exhibits an intermediate voltage level influenced by both network topology and load distribution.

All bus voltages remain within acceptable operating limits, indicating stable and balanced system operation.

This voltage profile serves as a reference baseline against which deviations caused by FDI attacks are identified and analyzed.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun622

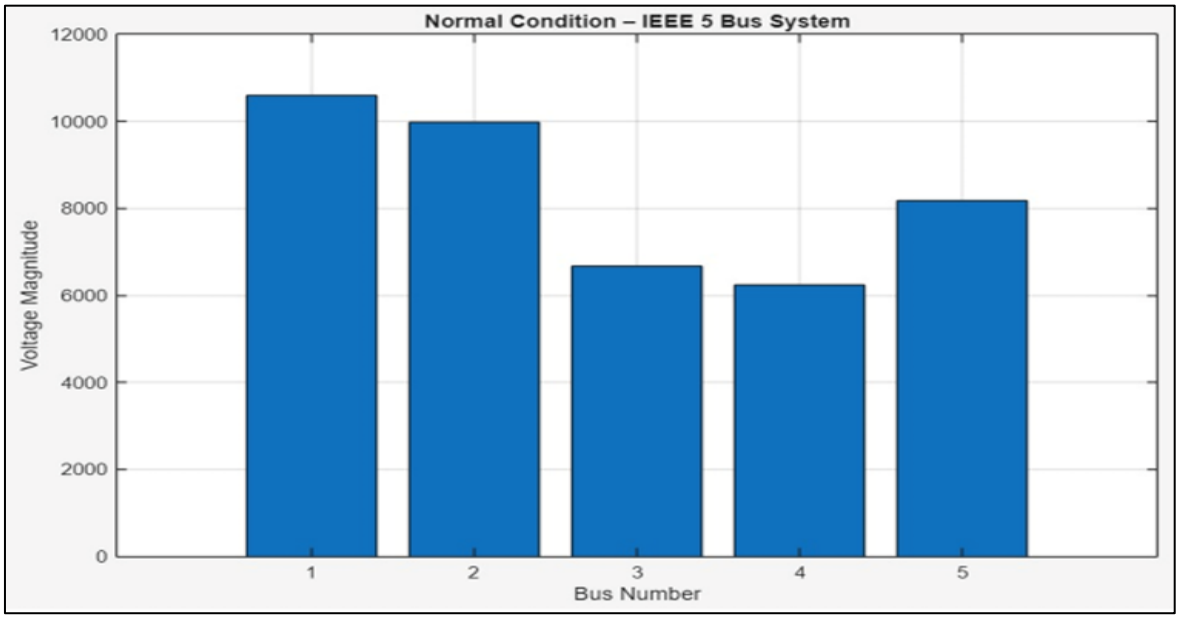

Fig 5 Output of the System Under Normal Condition

➢ *Impact of False Data Injection Attack on Voltage Measurements:*

To analyze the impact of an FDI attack, voltage measurements at Bus 3 are deliberately altered while keeping the remaining bus measurements unchanged. The resulting voltage magnitude distribution is shown in Fig. 6. Compared to the normal operating profile, a clear and intentional deviation is observed at Bus 3, where the voltage magnitude significantly departs from its expected value. The voltage magnitudes at the other buses remain nearly identical to those observed under normal conditions. This result highlights a key characteristic of FDI attacks: their ability to selectively compromise measurement data at a specific location without causing noticeable changes in the overall system behavior. Since the physical system remains stable and only the measurement data are manipulated, conventional protection and fault detection schemes may fail to identify such attacks. The localized voltage anomaly introduced at Bus 3 provides a distinctive signature that can be exploited by data-driven detection techniques.

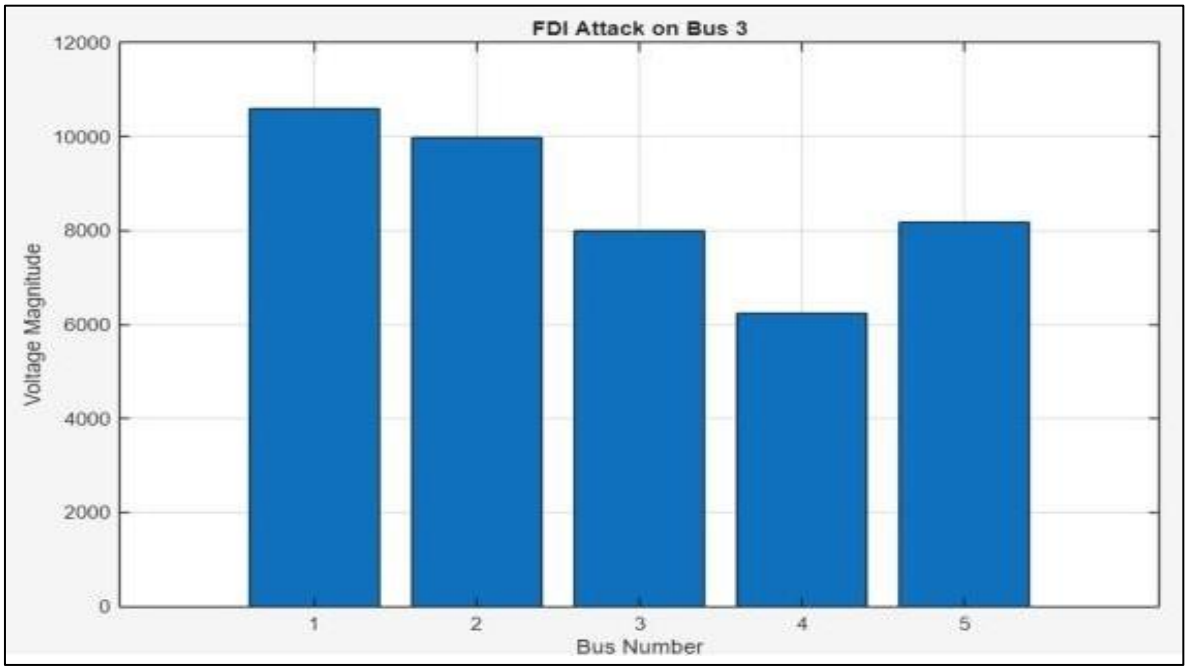

Fig 6 Output after Attack on Bus 3

➢ *FDI Attack Detection and Localization Using Random Forest:*

The voltage magnitude data obtained under normal and attacked conditions are used to train a Random Forest classifier for FDI attack detection and localization. Fig. 7 illustrates the output of the trained model for the attack scenario targeting Bus 3. The bar graph represents the number of classification outcomes corresponding to each bus.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun622

A dominant peak is observed at Bus 3, indicating that the classifier consistently identifies this bus as the compromised location. The absence of significant classification outputs at other buses demonstrates that the model does not misclassify the attack location.

This confirms the ability of the Random Forest classifier to learn characteristic voltage patterns associated with FDI attacks and accurately localize the affected bus.

The results validate that even subtle, localized measurement manipulations introduced by FDI attacks can be effectively detected and localized using voltage magnitude features and ensemble-based machine learning techniques.

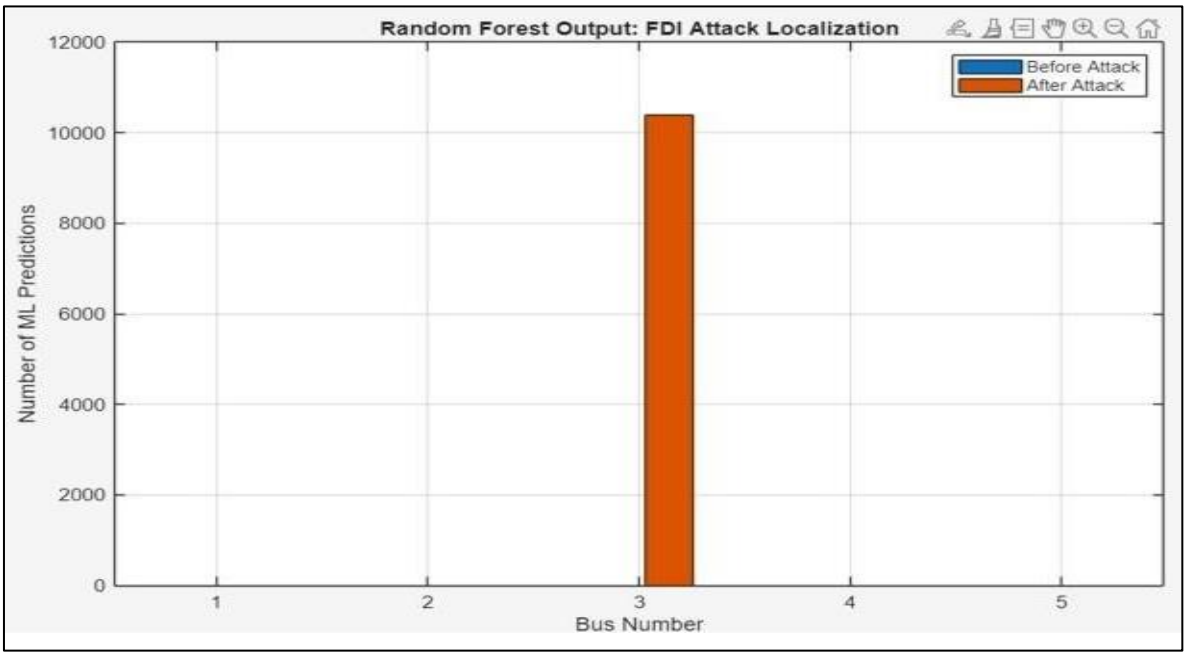

Fig 7 FDI Attack Localisation

V. CONCLUSION

This paper presented a machine learning–based framework for the detection and localization of False Data Injection attacks in power distribution systems. An IEEE 5-Bus test system was modeled in the MATLAB/Simulink environment to generate realistic voltage measurement data under normal operating conditions. FDI attack scenarios were created by selectively manipulating bus voltage measurements, enabling realistic representation of cyberattacks without disturbing the physical dynamics of the system.

Voltage magnitude was employed as the primary feature for analysis, offering an effective balance between computational efficiency and detection capability. A Random Forest classifier was trained using datasets representing both normal and attacked operating conditions. The results demonstrated that the proposed approach can reliably detect FDI attacks and accurately localize the compromised bus. Overall, the integration of power system simulation with data-driven machine learning techniques provides a practical and scalable solution for enhancing cyber-security in modern smart grids. Future work may focus on extending the proposed framework to larger power networks, incorporating additional measurement types, and implementing real-time detection strategies to further improve resilience against coordinated and multi-point cyber-attacks.

REFERENCES

[1]. P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, “A detailed investigation and analysis of using machine learning techniques for intrusion detection,” IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 686–713, First Quarter 2019, doi: 10.1109/COMST.2018.2847722.

[2]. S. Osken, G. Karatas, and L. Cuhaci, “Intrusion detection systems with deep learning: A systematic mapping study,” in Proceedings of the 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), 2019, pp. 1–6.

[3]. Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 955–965, September 2011, doi: 10.1109/TIFS.2011.2127968.

[4]. L. Xie, Y. Mo, and B. Sinopoli, “Integrity data attacks in power market operations,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 659–666, December 2011, doi: 10.1109/TSG.2011.2162965.

[5]. M. Ozay, I. Esnaola, F. Vural, S. Kulkarni, and H. Poor, “Machine learning methods for attack detection in the smart grid,” IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773–1786, August 2016, doi: 10.1109/TNNLS.2015.2404803.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun622

[6]. H. He and J. Yan, “Cyber-physical attacks and defenses in the smart grid: A survey,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 164–172, Third Quarter 2016, doi: 10.1109/COMST.2016.2545094.

[7]. G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine blackout: Implications for false data injection attacks,” IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317–3318, July 2017, doi: 10.1109/TPWRS.2016.2631891.

[8]. J. Zhang and Z. Yang, “Random forest-based cyber-attack detection in smart grids,” IEEE Access, vol. 6, pp. 74829–74838, 2018, doi: 10.1109/ACCESS.2018.2883683.

[9]. Y. Chakhchoukh, V. Vittal, and G. T. Heydt, “PMU-based state estimation for electric power systems under cyber attacks,” IEEE Transactions on Power Systems, vol. 29, no. 2, pp. 659–666, March 2014, doi: 10.1109/TPWRS.2013.2285097.

[10]. W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” Computer Networks, vol. 57, no. 5, pp. 1344–1371, April 2013, doi: 10.1016/j.comnet.2012.12.017.

[11]. A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, D. Dutta, and Y. Jin, “Machine learning-based false data injection attack detection in power systems,” in Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761445.