Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #48299

ADV-MITIGATION STRATEGIES OF FALSE DATA INJECTION ATTACKS ON LOAD FLOW-SMART GRIDS VIA THE BLOCKCHAIN

Dr. Mojeed Olamide Bello, Morgan State University

Mojeed Olamide Bello received his Ph.D. in Computer and Electrical Systems Engineering from Morgan State University, Baltimore, MD, in May 2024. He earned his M.Eng. degree in Electrical and Computer Engineering and a Post Baccalaureate Certificate in Cybersecurity, Network Information, and Embedded Systems from Morgan State University in 2017. In January 2024, he completed the FEMA EMI Basic Academy, and in March 2024, he obtained teaching certifications from the Association of College and University Educators (ACUE).

ADV-MITIGATION STRATEGIES OF FALSE DATA INJECTION ATTACKS ON LOAD FLOW-SMART GRIDS VIA THE BLOCKCHAIN

Abstract

In this research, Cyber-physical attacks on power grid networks, particularly false data injection attacks (FDIAs), have increased, leading to power outages and significant economic losses. These attacks pose a serious threat to smart grid load flow monitoring systems. This research explores advanced approaches using machine learning models and simulation case studies focused on mitigating FDIAs in smart grids. The study emphasizes resilience, traceability, and mitigation of these attacks through innovations in power load flow monitoring. The methodology involves advanced simulations with minimal programming technologies to decompose multi-node bus power grid generation and address false data load flow issues. A core objective is to standardize effective mitigation strategies to prevent power load flow disruptions, enhance resilience in critical data protection, and embedded blockchain technology for secure transaction management templates within the grid. A virtual platform for smart contracts is developed, facilitating load flow transactions securely. Additionally, a machine learning model is integrated to analyze, train, test, and forecast load flow data, enabling future predictions and improving the smart grid's resilience mechanisms against FDIAs.

Keyword: Load Flow, Machine Learning, Mitigation, Resilience, and Blockchain

ADV-MITIGATION STRATEGIES OF FALSE DATA INJECTION ATTACKS ON LOAD FLOW-SMART GRIDS VIA THE BLOCKCHAIN

1. Introduction

This study focuses on applying machine learning concepts to enhance power flow analysis in smart grid networks, emphasizing the smart integration between data communication and energy distribution systems. The contribution of this research is directed toward the development of a sustainable, secure, and reliable grid infrastructure. A Python-based simulation approach is proposed, highlighting the fundamental role that renewable energy sources can play. Additionally, the modernization of energy infrastructure through smart grid load flow modeling involves the integrated use of advanced machine learning algorithms and virtual networking technologies for energy transportation. These systems enable next-generation distributed energy management protocols, whereby nodes collaboratively determine essential operational parameters, such as electricity output and security metrics, using consensus algorithms to optimize overall performance. Prominent research areas in multi-agent control and distributed systems have explored consensus protocols for securing virtual platforms within smart grids. However, significant challenges remain unresolved, leaving smart grids particularly vulnerable to false data injection (FDI) attacks. FDI attacks involve malicious actors injecting deceptive data into the network, jeopardizing the grid's integrity, stability, and functionality. Accordingly, this study proposes intrusion detection strategies on virtual platforms and mitigation methods for FDI attacks. By utilizing machine learning and blockchain technologies, these approaches aim to enhance resilience and reliability in smart grid operations, ensuring the security and efficiency of energy distribution.

2. Objective

This study contributes to Electrical and Computer Engineering (ECE) education by aligning with the American Society for Engineering Education (ASEE) objectives of curriculum enhancement and student collaboration through laboratory-based research. The findings of this study can be incorporated into the ASEE-ECE curriculum through course syllabi in areas such as machine learning, cybersecurity, power system engineering, and STEM-focused technical electives, as well as through integration into laboratory modules and student-led capstone projects.

The research addresses mitigation strategies and vulnerability analysis of smart grid networks against load-flow false data injection (FDI) attacks. It explores advanced detection methods, resilience mechanisms, and mitigation strategies, thereby contributing to the development of more robust machine learning models and secure smart grid infrastructures. This research-based methodology provides instructional content and serves as a practical framework for addressing real-world challenges in data analysis, machine learning, and load-flow smart grid engineering.

By incorporating this research into standard methodology courses within ECE and STEM programs—particularly capstone design projects—students gain hands-on experience with emerging technologies and power grid infrastructure protection. The study supports the development of skills in data analytics, system modeling, and cybersecurity, ultimately enhancing students' technical expertise and problem-solving abilities in a rapidly evolving engineering landscape.

Specifically, the research focuses on investigating the vulnerabilities of smart grid networks to false load-flow data injection, and discusses improvements in detection and mitigation strategies to strengthen grid resilience. The study contributes to critical aspects of security, monitoring, and predictive analytics for load-flow systems through the application of machine learning and blockchain technologies.

This study addresses the following specific areas:

- Mitigation of Smart Grid Load-Flow Data Vulnerabilities: Based on the virtual template for load-flow bus-generator (BUS-GEN) model reinforcement, this study proposes improved mitigation strategies (refer to Fig. 1).

- Countermeasures for Overall Grid Resilience Enhancement: Countermeasures are proposed to address cyber-physical threats, aiming to enhance the resilience of smart grid load-flow networks.

- Threat Landscape Mapping: An in-depth analysis of various threats is provided, along with corresponding countermeasures, establishing a detailed research framework for mitigating critical vulnerabilities, as illustrated in Fig. 1.

- Blockchain for Security: Blockchain technology is proposed for securing load-flow data transactions to ensure integrity and reliability within smart grid load-flow networks.

Through these contributions, the study advances the development of a resilient smart grid infrastructure capable of real-time monitoring, predictive analytics, and faster detection of intrusion attempts related to false data injection.

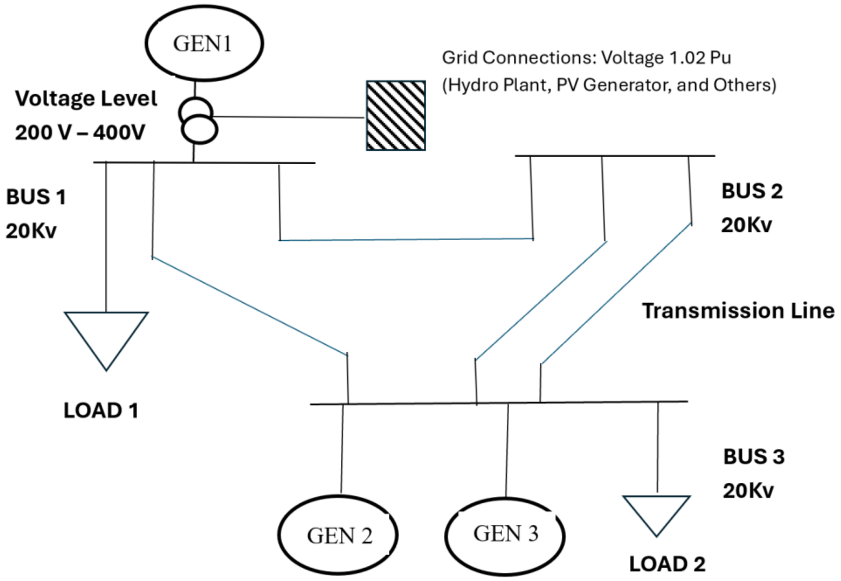


Fig. 1. Load-flow model virtual template

3. Literature Review

The results are represented by trends in the aggregated values of load_q, sgen_p, bus_p, and line_q. These results demonstrate the dynamic machine learning mitigation model for load flow data over time series and provide validation for the reliability of the predictive load flow false data injection (FDI) model (see Eq. 3). In this study, load flow data injection attacks are identified as one of the most threatening cyber incidents within power grids, having attracted significant attention from both researchers and practitioners. This work reviews recent developments related to FDI attacks, focusing on adversarial models, attack targets, and their impacts on smart grid infrastructure. The review covers key cybersecurity threats to smart grids based on both theoretical and practical literature. Specifically, three aspects are pursued: (1) how FDI attacks can be constructed, (2) their impact on demand response market operations, and (3) corresponding defense strategies. This study discusses adversarial approaches, the consequences of market disruptions, and countermeasures from the perspective of system operators, while also identifying future research directions aimed at strengthening defense mechanisms against FDI attacks [1].

FDI attacks targeting critical virtual network electrical equipment can cause system frequency abnormalities, cascading failures, and large-scale blackouts. One proposed solution is a tri-level defense model, as seen in LREPS, which advocates collaboration between defenders, attackers, and operators in decision-making to mitigate the rate of change of frequency (RoCoF) and withstand cyberattacks [2]. This approach also includes pre-event risk analyses and post-event strategies to enhance system functionality during future disruptions. The resilience of such systems is evaluated in terms of their resistance, restabilization, rebuilding, and reconfiguration capabilities after disruptive events [3].

State estimation is a fundamental function of energy management systems that rely on redundant measurements and network topology. FDI attacks can successfully evade traditional bad data detection (BDD) algorithms by injecting manipulated data vectors, thereby controlling state estimation outcomes. Machine learning has been widely adopted to overcome the limitations of traditional residual-based BDD methods, improving both detection speed and accuracy [4]. In smart grids, major themes in cyberattack detection include data integrity and reliability. Some proposals feature agent-based modeling of data integrity and decentralized security frameworks. For instance, cyberattacks have been detected with an accuracy of 98.19% using an artificial feedforward neural network [5]. Cybersecurity remains the primary challenge for smart grids, necessitating the development of new and efficient detection techniques that account for topological changes and other uncertainties arising from the intermittent nature of renewable energy sources. Among the promising techniques, long short-term memory (LSTM) recurrent neural networks (RNNs) have demonstrated the ability to effectively distinguish between natural changes in the grid and real-time cyberattacks, achieving high accuracy in system dynamics modeling [6]. Recent studies have also highlighted that adversaries can easily bypass existing BDD schemes, posing serious threats to grid stability. Researchers have thus focused on optimal attack strategy identification and defense mechanism development, including both protection- and detection-based approaches [7]. Blockchain technology has emerged as a resilient solution to secure communication within smart grids, mitigate data vulnerabilities, and enhance cyber-resilience [8].

Smart grids represent a seamless integration of digital communication networks, control technologies, and power systems that collectively ensure reliability and sustainability. Nevertheless, false data injections can result in disruptions, load shedding, and power theft. Most current robust FDI attack strategies rely on comprehensive knowledge of the grid network topology. To address this vulnerability, three topology-independent detection techniques have been proposed: linear regression, linear regression with timestamps, and delta threshold-based methods. These techniques improve the detection of injected false data by filling in missing real-time measurements [9].

The growth of cybersecurity concerns has been particularly evident with the integration of distributed energy resources (DERs) such as solar and wind power. New challenges related to communication and monitoring have emerged, and various studies have proposed blockchain-based resilient schemes for securing the monitoring and control of DERs within wireless sensor networks (WSNs) [21]. Additionally, interoperability and cyber-resiliency are ensured for renewable smart microgrids by securing the underlying communication infrastructure, protocols, and intelligent electrical devices [22]. Moreover, comprehensive security solutions addressing vulnerabilities in key grid components have been presented [23].

Machine-learning-based frameworks have been tested to detect sensor FDI attacks on industrial control systems through simulation models and hybrid testbeds [24]. Different machine learning models utilizing Internet of Things (IoT) datasets for a 10 kV solar photovoltaic (PV) system have demonstrated their performance in detecting FDIA attacks [25]. These efforts are closely related to the increasing number of cyberattacks targeting power systems, emphasizing the need for fault-tolerant systems capable of adapting to and compensating for attacks to ensure reliable power delivery [26].

This study provides a state-of-the-art review that highlights the extensive research still required for the detection, mitigation, and prevention of FDI attacks on smart grids. Addressing critical cybersecurity vulnerabilities in the growing number of smart devices and DERs is essential for maintaining the resilience and stability of future power systems.

4. Methodology and Analyses

This study investigates the implementation of a multi–machine-learning-based smart grid load flow data injection model, which is crucial for the integration of the next generation of microgrids. The model interacts with a hybrid power generation system through a smart virtual testbed (BUS-GEN model) to provide critical services that support grid operations. While performing various ancillary services and monitoring through the virtual model, the research further elaborates on the Virtual Testbed BUS-GEN model acquisition, which can be simulated accordingly. Specifically, a scalable smart grid system simulates neural network strategies within key design configurations, focusing on customized software configurations, testing, and maintenance. Additionally, modern communication protocol innovations, including master-slave and grid operation systems, are introduced. This virtual intrusion model of load flow data within a smart grid is essential for ensuring the efficient transmission and distribution of power. When embedded within the system, this approach leads to greater efficiency, reducing both energy and financial losses. Furthermore, its robustness against cyber-physical disruptions and cyberattacks ensures rapid recovery from outages, thereby improving the restoration time series and overall security of the smart grid framework.

4.1. Data Resources

Data resources leverage various datasets and computational tools to enhance forecasting processes and system analysis. The datasets used include PandaPower, Pandas, and Simbench, which were integrated into machine-learning models within a blockchain-enabled virtual testbed. Advanced simulation capabilities were supported by a Python-based virtual environment utilizing machine-learning libraries such as *sktime*, *scikit-learn (sklearn)*, and linear regression techniques, while graphical visualizations were produced using tools such as *Matplotlib* and *NumPy*. The blockchain framework was supported by resources including Web3, Infura, Ganache, and Ethereum, enabling secure and decentralized simulation workflows. This holistic integration of datasets and tools forms the foundation for accurate modeling and reliable evaluation of system performance.

4.2. Architecture Framework Mitigation Strategies

This research targets the development of architectural framework mitigation strategies designed to model smart grid load flow, supplemented with enhanced security capabilities and blockchain integration. The study was conducted in three phases. The initial phase focused on creating the structural framework and simulation platform for the smart grid load flow. This model consists of generic templates and virtual BUS elements that support a standard load flow simulation. Additionally, an intrusion detection system (IDS) was implemented on this platform to detect and flag data anomalies (see Fig. 2).

In the second phase, the model was refined to address root-level intrusions by redetecting cyber threats to ensure secure data acquisition. This step involved integrating blockchain technology into the simulation. Spurious data were intentionally introduced into the load flow model as part of the testing process to apply a blockchain-based mitigation framework. The performance of the overall system in identifying and resolving data inaccuracies was subsequently evaluated. Preliminary results indicate that the blockchain framework reliably identifies and validates false data in load flow simulations, demonstrating strong capabilities in maintaining cybersecurity standards.

The final phase of the research focused on the validation, tracing, and feedback of load flow data using the blockchain-based mitigation framework. Both manipulated and normal simulation data were considered at this stage to verify the reliability of blockchain in tracking and securing data. Therefore, this study comprehensively addresses the improvement of data accuracy and cybersecurity to ensure grid stability, thereby contributing to the resilience of smart grid systems, as illustrated in Fig. 2.

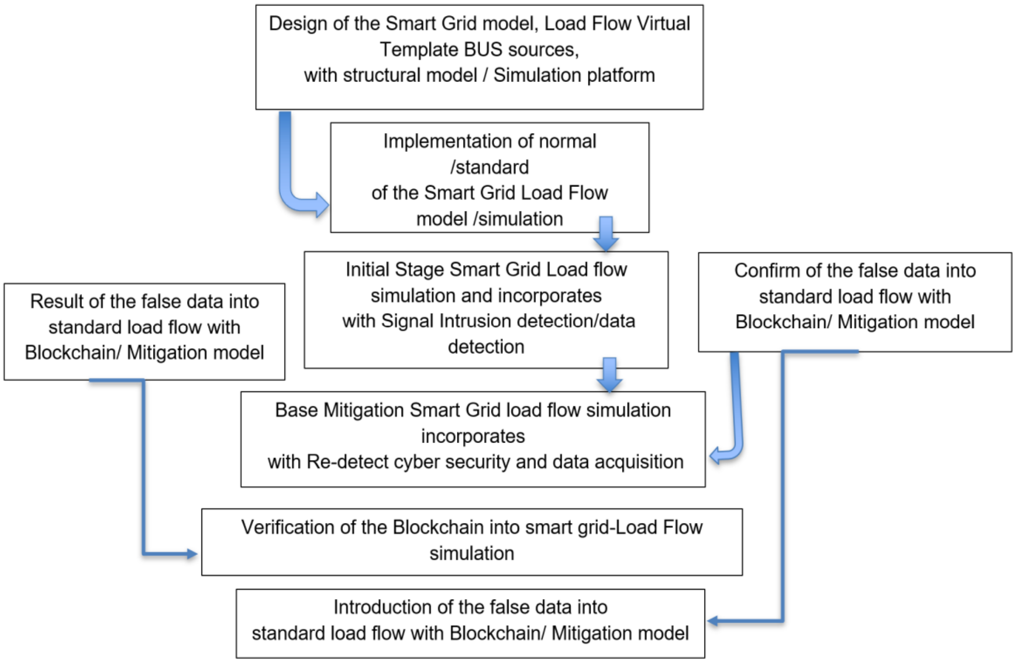

Design of the Smart Grid model, Load Flow Virtual Template BUS sources, with structural model / Simulation platform
Implementation of normal /standard of the Smart Grid Load Flow model /simulation
Initial Stage Smart Grid Load flow simulation and incorporates with Signal Intrusion detection/data detection
Result of the false data into standard load flow with Blockchain/ Mitigation model
Confirm of the false data into standard load flow with Blockchain/ Mitigation model
Base Mitigation Smart Grid load flow simulation incorporates with Re-detect cyber security and data acquisition
Verification of the Blockchain into smart grid-Load Flow simulation
Introduction of the false data into standard load flow with Blockchain/ Mitigation model

Fig. 2: Architecture framework mitigation strategies

4.3. Load-Flow Analysis and Countermeasures

This research establishes partial foundations for fundamental principles, including load flow analysis, optimization methodologies, and scalability criteria, in the design of smart grid systems. In this respect, it highlights the dynamic adaptability of smart grids through advanced models of smart grid load flow, addressing the challenges of evolving systems with specific attention to minimizing risks associated with false data in virtual load flow models.

The study focuses on developing a smart grid that is more resilient to false data injection (FDI) attacks by integrating cybersecurity strategies, including mitigation mechanisms, resilience frameworks, and false data detection algorithms. Furthermore, the methodology incorporates the integration of blockchain technology into the smart grid infrastructure. Blockchain, with its decentralized and tamper-resistant architecture, provides a more robust means of safeguarding load flow data and associated transactions. In this study, blockchain is utilized to introduce an additional layer of protection that ensures data integrity and enhances the reliability and operational stability of smart grid systems.

4.4. Simulation of Mitigation Re-Tracking Model

This study developed mitigation strategies within machine learning models by examining the impacts of false data injection attacks on load flow simulations, utilizing blockchain technology for data integrity retracking, confirmation, and verification. The steps developed for the simulation process are outlined below. First, blockchain technology was employed to enhance data integrity by retracking and confirming the validity of the load flow simulation. A blockchain-based verification mechanism was initially implemented to verify the authenticity of the load flow data injections corresponding to GEN 1 and BUS 1. Subsequently, a similar verification process was performed for the data corresponding to BUS 2, where validation and confirmation were integrated through blockchain technology into the load flow simulation. Furthermore, LOAD 1 served as a template for conducting load flow model data injection simulations. Finally, the smart grid load flow data injection framework integrated GEN 2, GEN 3, and LOAD 2 data into the blockchain for authenticity and coherence. This method is designed to ensure that smart grid load flow simulations remain secure against false data injection attacks, thereby maintaining their dependability. The simulation framework is illustrated in Fig. 3.

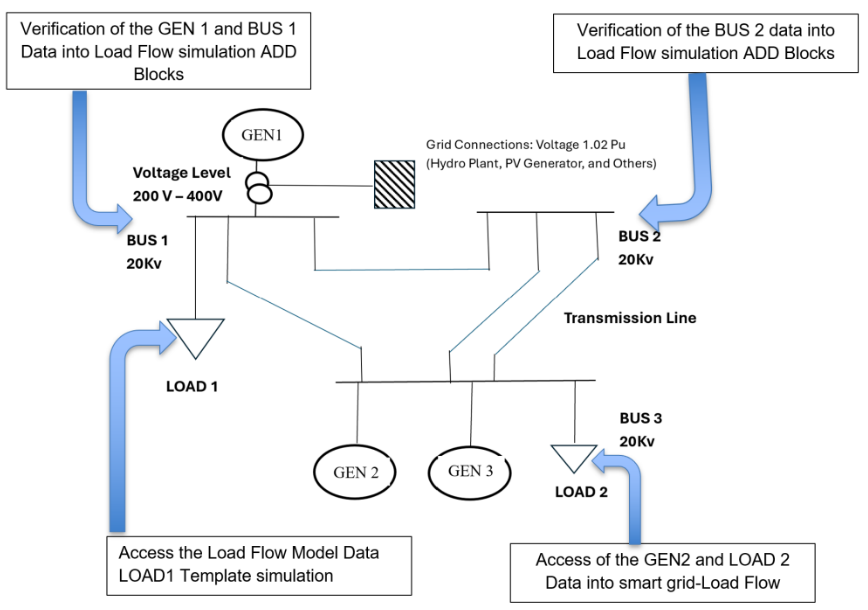

Verification of the GEN 1 and BUS 1 Data into Load Flow simulation ADD Blocks
Verification of the BUS 2 data into Load Flow simulation ADD Blocks
GEN1
Grid Connections: Voltage 1.02 Pu
(Hydro Plant, PV Generator, and Others)
Voltage Level
200 V – 400V
BUS 1
20Kv
BUS 2
20Kv
Transmission Line
LOAD 1
BUS 3
20Kv
GEN 2
GEN 3
LOAD 2
Access the Load Flow Model Data LOAD1 Template simulation
Access of the GEN2 and LOAD 2 Data into smart grid-Load Flow

Fig. 3. Mitigation re-track model simulation

5. Results and Discussion

This project focuses on developing mitigation strategies for load flow false data injection (FDI) testbeds by emulating various smart grid scenarios, using machine learning techniques to acquire data and generate functions aimed at minimizing the impact of such attacks. Accordingly, most investigations in this research concentrated on reducing the risk of false data injection attacks (FDIA) by analyzing load flow data injected using different interval-based tools, such as PandaPower, Pandas, and SimBench, for forecasting purposes. These tools were integrated with machine learning models within blockchain-enhanced virtual testbeds. Simulations were conducted using the Python-based Virtual Testbed BUS-GEN model, which enabled the construction of a scalable power grid architecture. Python provided flexibility for precise modeling, simulation, and analysis, thereby increasing the system's efficiency, accuracy, and security against potential FDIA attacks. Blockchain technology was integrated into the smart grid infrastructure to enhance system security by ensuring the integrity of load flow data and safeguarding transactions against manipulation. The proposed integration of machine learning and blockchain technologies was tailored to meet the demands of hybrid systems, supporting robust data integrity within dynamic energy networks composed of conventional power lines, smart meters, and advanced communication technologies.

FDIA mitigation was thus incorporated into the processes of tracking and verifying the authenticity of load flow data during simulation. The major steps included:

- Mitigation by retracking: Blockchain retracked load flow simulations to ensure data integrity.

- Verification of GEN 1 and BUS 1 load flow injection data: Blockchain verified the precision and coherence of data blocks generated for GEN 1 and BUS 1.

- Re-verification of BUS 2 data: Blockchain maintained the integrity of simulation data associated with BUS 2.

- Simulation training and prediction: Load flow models were simulated and predicted using the LOAD1 template.

- Data integration for GEN 2 and LOAD 2: Real and false data injections were administered using blockchain tools such as Ganache, Ethereum, and Web3.

Machine learning models were subsequently applied to analyze the impacts of false data injections on load flow simulations, enhancing the mitigation, resilience, and security of smart grid networks. This integrated approach of blockchain and machine learning provides a comprehensive framework for mitigating FDIA risks and strengthening smart grid infrastructure.

5.1. Mitigation Strategies and Stages

The mitigation strategy employed a three-stage methodology to prepare and analyze the load flow data injection attack simulation model, as follows:

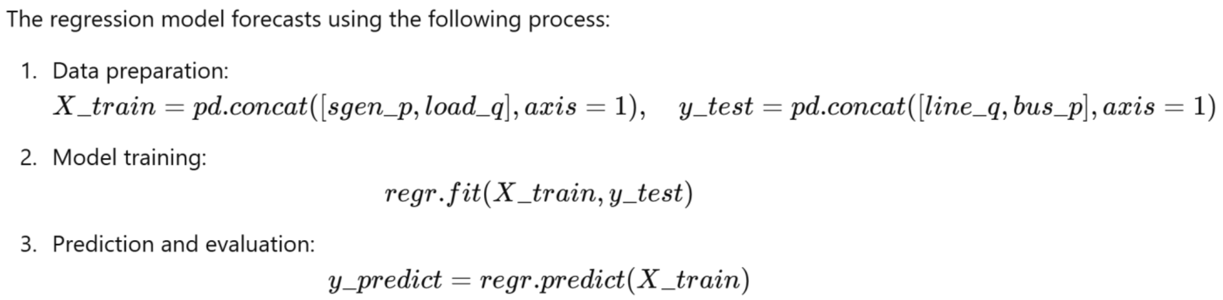
- Initial Stage: Mitigation retracking was performed on a specified data frame, which involved the creation of load flow data profiles, including but not limited to, active generator power, active load power, and reactive load power of lines (see Fig. A and Fig. 4).
- Mid-Stage: Retracking at specific time intervals provided insights into the dynamics that may prevail within the grid (see Fig. B and Fig. 5).
- Final Stage: Refinement of the load flow data injection network model resilience was achieved through mitigation retracking by implementing percentage adjustments (see Fig. C and Fig. 6).

Injecting the results of the load flow data into the virtual testbed emulated each stage virtually. Intrusion detection mechanisms were implemented to simulate false data injections, with consistency and authenticity of the data guaranteed by blockchain technologies, such as Ganache, Ethereum, Infura, and Web3. Enlightening conclusions regarding system responses under FDIA threat conditions were drawn through active and reactive power parameter analyses conducted during these stages.

5.1.1. Stage 1. Initial-Level Simulation Model: Mitigation Re-Tracking Through Data-Range Simulation

The initial phase of the simulation involved training and testing datasets to predict load flow data for different scenarios, including interruptions and normal load flow conditions injected into the network. The dataset ranged from 20 to 100 data frames, with specific data sets processed sequentially. The training data were divided into X_train, X_text, y_train, and y_test, while the testing data covered training sizes ranging from 10 to 100 data points (see Eq. 1). A linear regression model was employed to predict load flow data by isolating sequential data frame proportions within the ranges of 10, 20, 40, 60, 80, and 100 frames (see Fig. A).

Eq.1



The regression model forecasts using the following process:

1. Data preparation:
   $$X\_train = pd.concat([sgen\_p, load\_q], axis = 1), \quad y\_test = pd.concat([line\_q, bus\_p], axis = 1)$$
2. Model training:
   $$regr.fit(X\_train, y\_test)$$
3. Prediction and evaluation:
   $$y\_predict = regr.predict(X\_train)$$

The initial setup of the mitigation retracking simulation model was evaluated using the mean squared error (MSE) metric, and its time efficiency was assessed by analyzing prediction latency. First, profile data were concatenated along two axes, the x- and y-axes, incorporating generator power and line reactive power parameters (sgen_p, line_q, load_q, and line_q) to ensure a comprehensive representation of the input data. The entire dataset was divided into frames ranging from 20 to 100 frames, corresponding to different time intervals. The simulation results, shown in Fig. A, validated the effectiveness of the model.

In the initial stage, the interception of load flow false injection attacks was simulated using data frames containing ranges from 0 to 20, processed in three iterations. Each sample was processed and sent to the blockchain model for validation and analysis (see Fig. A).

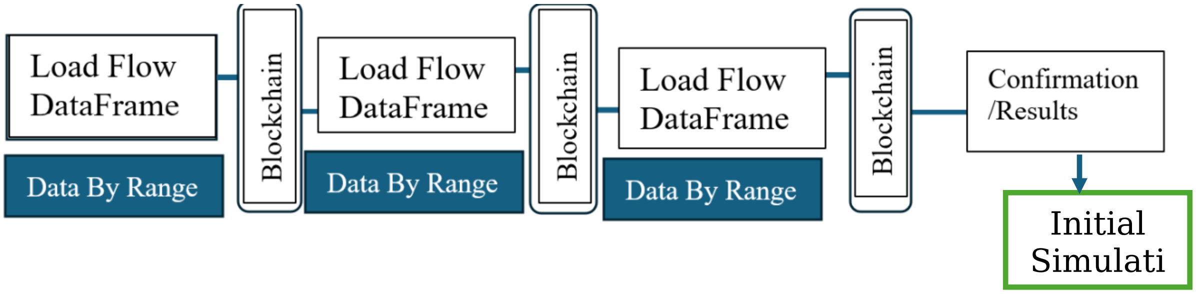


Fig. A. Mitigation re-tracking by data-range

Mitigation strategies for false load flow data injection use time series data to enhance the accuracy and reliability of intrusion detection simulations. The proposed Load Flow Injection Data serve as a critical component in combining training datasets and predicted values, forming a robust foundation for these simulations. LOAD1 is a predicted load flow dataset designed for integration into mitigation models. Its training included both datasets from opposite conditions—normal operation and false data injection—to ensure robust grounds for simulation and analysis.

This mitigation process aligns with an extensive data verification approach. The integrity of the initial data set was ensured by first simulating GEN 1 and BUS 1 in the Load Flow simulation before further validating and incorporating data for BUS 2. Additional simulations were then conducted by integrating GEN 2 and LOAD 2 data using the LOAD1 template. This structured and methodical approach significantly enhances smart grid modeling and strengthens system reliability against potential threats from data injection. An overview of the simulation framework is presented in Fig. 4.

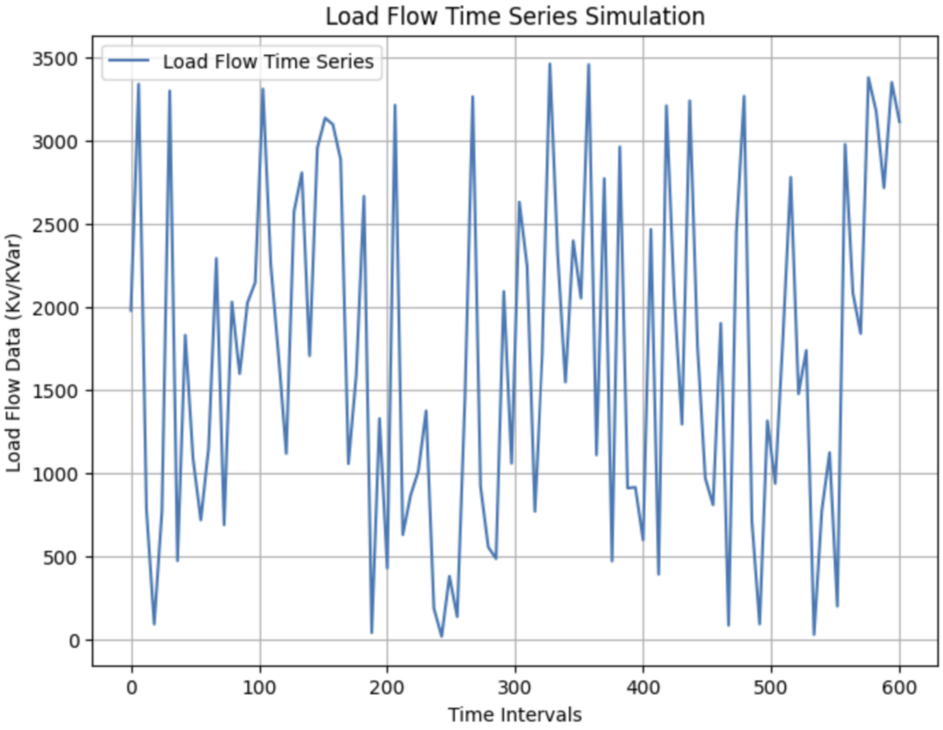


Fig. 4. Mitigation load-flow normal time series

Simulations of the load flow data injection parameters, ranging from 0 to 3500 kV/kVAR, were also conducted at time intervals between 0 and 600 seconds. Realistic load-flow data were extracted from the training datasets to closely represent real-world operational scenarios. The proposed simulation framework incorporates the use of training data with predictive analytics to improve intrusion detection capabilities. Both real and simulated virtual testbed platforms contribute to the FDIA framework, while

LOAD1 is used as the predicted dataset for simulating mitigation strategies. LOAD1 is trained under both normal operating conditions and under false data injection scenarios to ensure the effectiveness of the mitigation strategies against various types of threats.

The model development process employs secure blockchain mechanisms that enable progressive improvements in data mitigation, resilience, integrity, and traceability during simulations. Specifically, the model was developed by verifying GEN 1 and BUS 1, with blockchain integration extended to validate BUS 2 data within the simulation framework. A predefined template for LOAD1 facilitated the performance of load flow simulations more efficiently. Finally, GEN 2 and LOAD 2 data were integrated to study and validate the load flow behavior of the smart grid under different scenarios. This methodology ensures that both actual and forecasted load flow scenarios are robustly evaluated, as shown in Fig. 5.

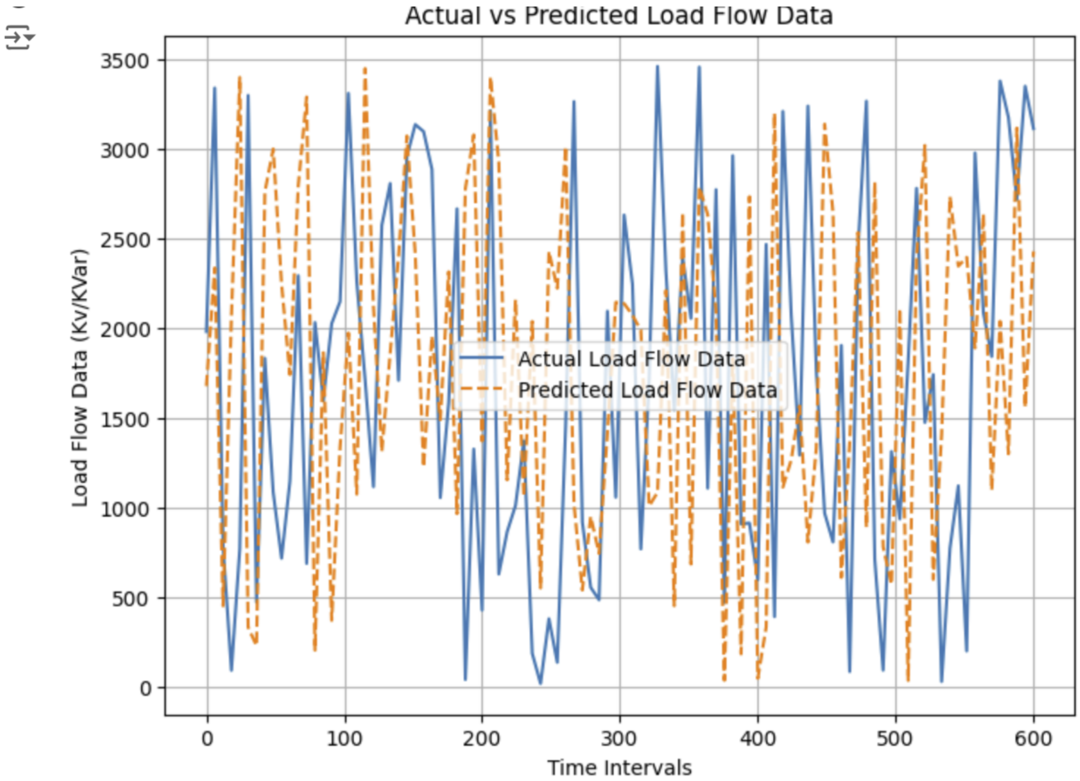


Fig. 5. Actual and predicted load-flow mitigation

5.1.2. Stage 2. Mid-level Simulation Model: Mitigation Re-Tracking by Time Interval

The mitigation retracking model for load flow false data injection was developed using profile data concatenated along two axes. The dataset integrates active and reactive smart grid parameters as the x-axis, while the y-axis includes active and reactive power. This dataset spans data frames recorded at time intervals of 5, 10, and 15–50 seconds. Training and testing splits were performed using sgen_p.sum, line_p.sum, and load_p.sum sets, with 20% of the data allocated for training (refer to Eq. 2). In this experiment, a linear regression model was applied to predict the load flow data and to analyze data sequences proportionally from 10 to 100 data frames. The model's performance at different time intervals is presented in Fig. B.

Eq.2

$$X = pd.concat([sgen\_p, line\_q], axis = 1), \quad y = pd.concat([bus\_p, load\_q], axis = 1)$$

Mid Stage: In the second phase of the load flow false data injection attack simulation, data frames were intercepted at specific time intervals, such as 5–10 seconds, and so on. This process was repeated three times, with each data set sent to the blockchain model for validation (see Fig. B).

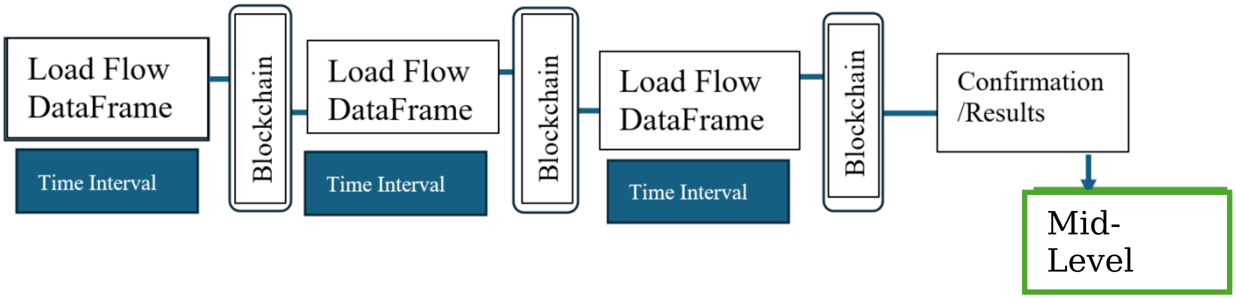


Fig. B. Mitigation re-tracking by time interval

5.1.3. Stage 3. Final-Level Simulation Model: Mitigation of Load-Flow Data via Percentages

The final-level virtual simulations for load flow data mitigation combined training and testing datasets to simulate and predict load flow behavior under varying conditions, including normal operations and interruptions. The dataset ranged from 20% to 100%, incrementally segmented, with specific data frames corresponding to each percentage range. The dataset was divided into a training set comprising 20% of the overall data, with the remaining data used for testing (X_test and y_test). A linear regression model was utilized to predict the load flow data by modeling sequences of data frames, with proportions incrementally increasing from 10% to 100%. The results are shown in Fig. C.

Final Stage: In the final phase, the simulation intercepted load flow data frames based on varying percentages, from 10% to 80%, incrementally. Each interception was repeated three times, and the data were processed and transmitted to the blockchain model for further validation (see Fig. C).

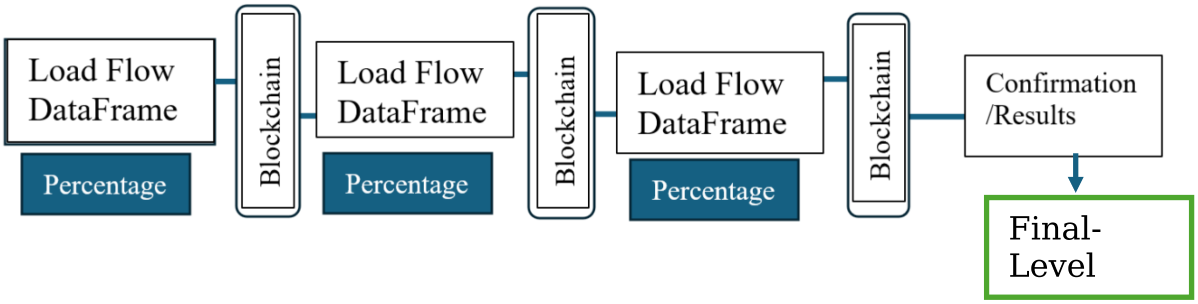


Fig. C. Mitigation re-tracking by percentage

Load flow simulations were performed with parameters ranging from 0 to 3500 kV/kVAR and time percentages varying from 0 to 400 (Ohm_per_Km_%). These simulations generated load flow data percentages by combining training datasets with predictive modeling techniques, ensuring alignment with actual operational conditions. Load Flow Model Data (LOAD) integrates training data with predictive modeling to enhance the simulation of intrusion detection. Additionally, the predicted dataset (LOAD1) was specifically developed for mitigation model simulations, trained under both normal operating conditions and false data injection scenarios. This dual training methodology provides a robust foundation for implementing effective mitigation strategies, as illustrated in Fig. 6.

The simulation framework verified the integrity and transparency of the load flow data at each stage. Verification began with GEN 1 and BUS 1, simulating the initial load flow data injection, and integrating results into corresponding blockchain blocks to maintain an immutable and secure record. Subsequently, BUS 2 data were incorporated into the simulation framework for validation. A pre-developed template for LOAD1 was used to ensure consistency and operational efficiency during load flow model simulations. Finally, GEN 2 and LOAD 2 data were integrated to simulate and validate the load flow behavior of the smart grid. This comprehensive approach enables testing under both real and predicted load flow data injection conditions, providing a thorough assessment of system performance, as shown in Fig. 6.

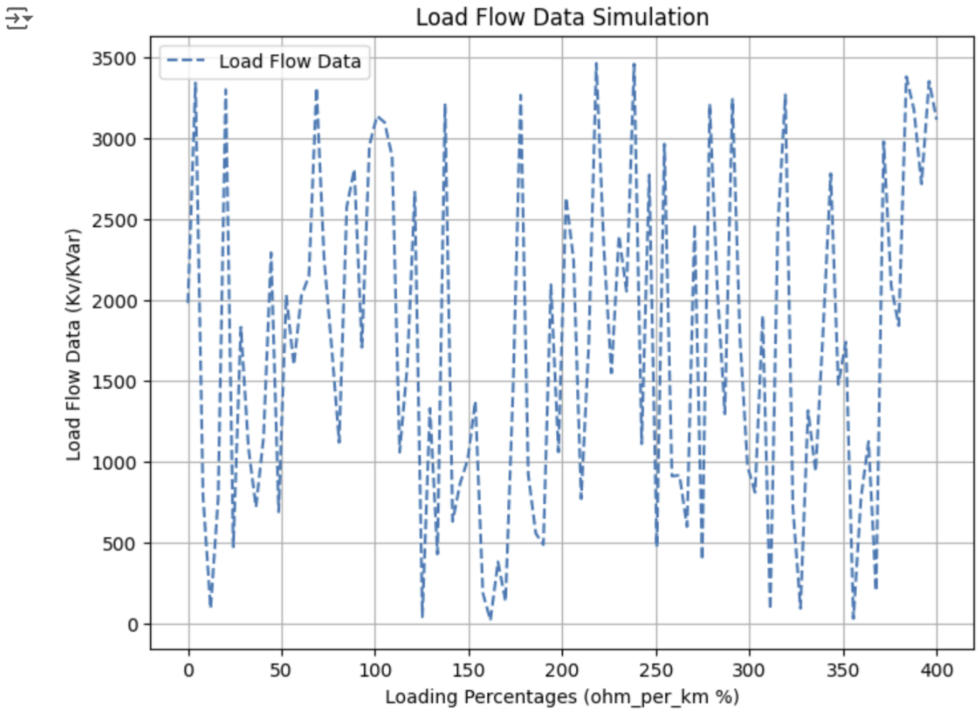


Fig. 6. Mitigation load-flow percentages

The results are represented by trends in the aggregated values of load_q.sum, sgen_p.sum, bus_p.sum, and line_q.sum. These results reflect the dynamic machine learning mitigation model for load flow data using time series analysis and validate the reliability of the predictive model for detecting load flow false-data injections (refer to Eq. 3).

Eq.3.

$$load\_q.sum(axis = 1).plot(label = "load"), \quad sgen\_p.sum(axis = 1).plot(label = "sgen")$$

$$bus\_p.sum(axis = 1).plot(label = "bus"), \quad line\_q.sum(axis = 1).plot(label = "line")$$

5.2. Virtual Simulation Lab

The proposed research implemented a mitigation strategy against load flow data injection attacks in a virtual simulation lab, structured across three stages: initial, middle, and final. Each phase of the load flow data injection model was transmitted to Ethereum or Ganache platforms via Web3 and Infura integration. The simulation was conducted in three successive steps, each designed to address a different attack scenario, as illustrated in Figures 3, 4, and 5, and further detailed in Figures A, B, and C.

The simulations were performed on a virtual platform testbed incorporating machine learning techniques for data generation and acquisition to effectively mitigate false data injection attacks within smart grid infrastructure. Overall, the proposed framework models and predicts load flow data by integrating the virtual testbed environment for FDIA (False Data Injection Attack) with machine learning algorithms. Linear regression was applied, generating highly accurate power flow predictions across various scenarios. The approach demonstrated scalability and efficiency, making its integration into advanced smart grid networks noteworthy.

6. Conclusion

This study presented mitigation strategies against load-flow false data attacks by analyzing major load-flow equations and implementing a virtual testbed platform. A conceptual framework was developed to analyze the impact of virtual simulation and false data injection within load-flow systems. This framework was constructed through a step-by-step integration of mitigation strategies, employing machine learning models for data prediction, training, and forecasting.

Moreover, the integration of blockchain technology ensures data integrity and enhances security, reducing vulnerability to attacks. This research captured data from the virtual testbed platform and applied it within a machine learning context using Pandapower Simbench, processing and manipulating time-series data with libraries such as pandas, sktime, and sklearn.

Consequently, the study proposes an advanced, secure smart grid network capable of neutralizing risks based on threat vectors from an attacker's perspective, leveraging the FDIA framework. The virtual testbed BUS-GEN model and advanced programming methods proposed here offer enhanced network resilience for smart grid protection.

A. Educational Engineering Benefits

This research serves as a testbed for various fields of study, adopting an interdisciplinary approach that supports engineering education in STEM disciplines. By integrating diverse knowledge areas, it establishes a comprehensive foundation for scholars to develop mitigation strategies in science, technology, engineering, and mathematics.

The research methodology followed an architectural approach, incorporating elements of machine learning, blockchain data science, mitigation strategies, and resilience analysis. Specifically, it focuses on identifying and addressing load-flow smart grid attacks and false data injections while contributing to advancements in laboratory research and engineering education.

B. ASEE-ECE Education Connection

This research aligns well with the ASEE-ECE curriculum through its relevance to courses and syllabi in machine learning, cybersecurity, and STEM-focused electives, as well as through laboratory studies and student project discussions. It serves both as a template project and a research resource consistent with ASEE's goals for advancing education.

As a standard methodology component within core Electrical and Computer Engineering programs, it is particularly suitable for capstone projects. Incorporating this research into coursework, laboratory exercises, group discussions, and team-based initiatives provides students with hands-on experience, supporting the development of advanced data engineering skills and enhancing both technical competencies and real-world problem-solving abilities.

References

1. R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, Apr. 2017, doi: 10.1109/TII.2016.2614396.

2. R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, Apr. 2017, doi: 10.1109/TII.2016.2614396.

3. Z. Zhao, Y. Shang, B. Qi, Y. Wang, Y. Sun, and Q. Zhang, "Research on Defense Strategies for Power System Frequency Stability Under False Data Injection Attacks," *Applied Energy*, vol. 371, p. 123711, 2024.

4. P. Gasser et al., "A Review on Resilience Assessment of Energy Systems," *Sustainable and Resilient Infrastructure*, vol. 6, no. 5, pp. 273-299, 2021.

5. A. Sayghe et al., "Survey of Machine Learning Methods for Detecting False Data Injection Attacks in Power Systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581-595, 2020.

6. H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive Survey and Taxonomies of False Data Injection Attacks in Smart Grids: Attack Models, Targets, and Impacts," *Renewable and Sustainable Energy Reviews*, vol. 163, p. 112423, 2022.

7. Z. H. Pang, L. Z. Fan, J. Sun, K. Liu, and G. P. Liu, "Detection of Stealthy False Data Injection Attacks Against Networked Control Systems via Active Data Modification," *Information Sciences*, vol. 546, pp. 192-205, 2021.

8. Z. Pang, Y. Fu, H. Guo, and J. Sun, "Analysis of Stealthy False Data Injection Attacks Against Networked Control Systems: Three Case Studies," *Journal of Systems Science and Complexity*, vol. 36, no. 4, pp. 1407-1422, 2023.

9. R. Nawaz, R. Akhtar, M. A. Shahid, I. M. Qureshi, and M. H. Mahmood, "Machine Learning-Based False Data Injection in Smart Grid," *International Journal of Electrical Power & Energy Systems*, vol. 130, p. 106819, 2021.

10. M. Mohammadpourfard, A. Khalili, I. Genc, and C. Konstantinou, "Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids," *Sustainable Cities and Society*, vol. 75, p. 103116, 2021.

11. J. Yan, Y. Tang, B. Tang, H. He, and Y. Sun, "Power Grid Resilience Against False Data Injection Attacks," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 2016, pp. 1-5, doi: 10.1109/PESGM.2016.7741618.

12. Q. Yang et al., "On False Data-Injection Attacks Against Power System State Estimation: Modeling and Countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717-729, Mar. 2014, doi: 10.1109/TPDS.2013.92.

13. J. Dai, J. Yang, Y. Wang, and Y. Xu, "Blockchain-Enabled Cyber-Resilience Enhancement Framework of Microgrid Distributed Secondary Control Against False Data Injection Attacks," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 2226-2236, Mar. 2024, doi: 10.1109/TSG.2023.3328383.

14. L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, "Detecting False Data Attacks Using Machine Learning Techniques in Smart Grid: A Survey," *Journal of Network and Computer Applications*, vol. 170, p. 102808, 2020.

15. M. Faheem, M. A. Al-Khasawneh, A. A. Khan, and S. H. H. Madni, "Cyberattack Patterns in Blockchain-Based Communication Networks for Distributed Renewable Energy Systems: A Study on Big Datasets," *Data in Brief*, vol. 110212, 2024.

16. O. O. Tooki and O. M. Popoola, "A Critical Review on Intelligent-Based Techniques for Detection and Mitigation of Cyberthreats and Cascaded Failures in Cyber-Physical Power Systems," *Renewable Energy Focus*, vol. 100628, 2024.

17. D. Annavaram, S. Mishra, and D. Pullaguram, "Resilient Event-Driven Distributed Control for DC Microgrids Against False Data Injection Attacks," *IEEE Transactions on Smart Grid*, vol. 15, no. 6, pp. 5358-5372, Nov. 2024, doi: 10.1109/TSG.2024.3419141.

18. A. Althobaiti, A. Jindal, A. K. Marnerides, and U. Roedig, "Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods," *IEEE Access*, vol. 9, pp. 159291-159312, 2021, doi: 10.1109/ACCESS.2021.3131220.

19. S. Das, "Modeling and Mitigating Power Grid Vulnerabilities: A Comprehensive Analysis of Renewable Energy Integration, Cascading Failures, and Microgrid Resilience," 2024.

20. M. Faheem, B. Raza, M. S. Bhutta, and S. H. H. Madni, "A Blockchain-Based Resilient and Secure Framework for Events Monitoring and Control in Distributed Renewable Energy Systems," *IET Blockchain*, 2024.

21. S. H. Rouhani, C. L. Su, S. Mobayen, N. Razmjooy, and M. Elsisi, "Cyber Resilience in Renewable Microgrids: A Review of Standards, Challenges, and Solutions," *Energy*, vol. 133081, 2024.

22. M. Elnour et al., "A Machine Learning Based Framework for Real-Time Detection and Mitigation of Sensor False Data Injection Cyber-Physical Attacks in Industrial Control Systems," *IEEE Access*, vol. 11, pp. 86977-86998, 2023, doi: 10.1109/ACCESS.2023.3303015.

23. M. J. Abudin, S. Thokchom, R. T. Naayagi, and G. Panda, "Detecting False Data Injection Attacks Using Machine Learning-Based Approaches for Smart Grid Networks," *Applied Sciences*, vol. 14, no. 11, p. 4764, 2024.

24. M. Elnour, M. Noorizadeh, M. Shakerpour, N. Meskin, K. Khan, and R. Jain, "A machine learning based framework for real-time detection and mitigation of sensor false data injection cyber-physical attacks in industrial control systems," *IEEE Access*, 2023.

25. M. J. Abudin, S. Thokchom, R. T. Naayagi, and G. Panda, "Detecting false data injection attacks using machine learning-based approaches for smart grid networks," *Applied Sciences*, vol. 14, no. 11, p. 4764, 2024.

26. O. O. Tooki and O. M. Popoola, "A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems," *Renewable Energy Focus*, p. 100628, 2024.