Nigerian Journal of Technology (NIJOTECH)
Vol. 44, No. 2, June, 2025, pp.302 - 310
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
https://doi.org/10.4314/njt.v44i2.14

DEEP LEARNING TECHNIQUE FOR IDENTIFYING FALSE DATA INJECTION THREATS IN SMART GRID SYSTEMS

AUTHORS:
A. Karthikeyan MP[1,*], W. Patel[2,*], S. Bharadwaj[3], and S. Singh[4]

AFFILIATIONS:
[1]Department of Computer Science and Information Technology, Jain, Bangalore, Karnataka.
[2]Department of Computer Science and Engineering, Parul University, Vadodara, Gujarat, India.
[3]Department of Computing Science and Information Technology, Teerthanker Mahaveer University, Uttar Pradesh, India.
[4]Department of Engineering and Technology, Maharishi University of Information Technology, Uttar Pradesh, India.

***CORRESPONDING AUTHOR:**
Email: warishkumar.patel@paruluniversity.ac.in; karthikeyan.mp@jainuniversity.ac.in

ARTICLE HISTORY:
Received: 09 March, 2024.
Revised: 27 August, 2024.
Accepted: 17 September, 2024.
Published: 07 July, 2025.

KEYWORDS:
Smart Grid (SG), State Vector Estimator (SVE), False Data Injection (FDI), Cuttlefish Optimization Coupled With Enriched Recurrent Neural Network (CO-ERNN), Cyberattack, Bus system.

ARTICLE INCLUDES:
Peer review

DATA AVAILABILITY:
On request from author(s)

EDITORS:
Chidozie Charles Nnaji

FUNDING:
None

HOW TO CITE:
Karthikeyan MP, A., Patel, W., Bharadwaj, S., and Singh, S. "Deep Learning Technique for Identifying False Data Injection Threats in Smart Grid Systems", *Nigerian Journal of Technology*, 2025; 44(2), pp. 302 – 310; https://doi.org/10.4314/njt.v44i2.14

© 2025 by the author(s). This article is open access under the CC BY-NC-ND license

Abstract

The integration of computers and artificial intelligence (AI) improves SG management and monitors were considered significant. More reliance on technological devices renders one more susceptible to dangerous assaults. The confidentiality of data has been put at risk due to the growing vulnerability of the supervisory control and data acquisition (SCADA) framework towards False Data Injection (FDI) assaults. The behavioral traits of FDI assaults are identified in this work by using historical measurement data and deep learning (DL) techniques. The z-score normalization approach was used for cleansing the historical data and converting continuous-time signals towards discrete form and the discrete wavelet transform (DWT) technique was utilized for data extraction. To find the best FDI assaults in the SG, cuttlefish optimization is combined with enriched recurrent neural network (CO-ERNN) technology. By efficiently reducing assumptions about possible attack scenarios, the suggested cyber-attack detection system exhibits outstanding dependability. Furthermore, an optimization model is put out to describe the behavior of a certain kind of FDI functioning, specifically in situations when accessible restricted positioning measures for power theft in energy systems are at risk. Based on the IEEE 118-bus test system, the versatility of the CO-ERNN proposed attack recognition mechanism is assessed, and the results of the simulation demonstrate the effectiveness of the proposed strategy.

1.0 INTRODUCTION

The 20th-century Smart Grid (SG) infrastructure is inadequate for the modern world due to emerging technologies like smart inverters, electric cars, and renewable energy generators. These technologies introduce dynamic frameworks, and bilateral power flow, challenging traditional power systems [1]. To address these issues, SG is designed with additional measurement, communication, and control capabilities, providing affordable, reliable, and efficient energy through control and communication technology, making it feasible to integrate and optimize energy from renewable resources [2]. Computer networks are essential for a company's security against online threats like denial-of-service (DoS) attacks. Organizations can safeguard their computer systems and assets for administrative, public health, and safety [3]. Attackers can get around robust defenses though, by taking advantage of security framework flaws. Cloud services, remote working tools, and remote access tools are currently under attack from malicious software, ransomware, phishing attacks, insider threats, and new persistent infections that surfaced during the worldwide epidemic [4]. The integrity of automated features, services for communication, and self-driving automobiles depends on cyber security [5]. False data attacks are a serious risk to SG sensor measurements and could have disastrous consequences. Over the past decade, detection techniques have been developed to protect against these attacks, particularly in large-scale emergent SG systems, which require appropriate data analysis and anomaly detection strategies [6]. An energy system called an SG tracks and monitors the flow of power from several units to satisfy the various demands of consumers for power. It does this by utilizing digital and other cutting-edge technology [7]. The article's goal is to create an AI-integrated solution for SG's cyberattack detection using fictitious data. It addresses the susceptibility of the SCADA system to FDI attacks while attempting to raise standards for regulation and observation. The article examines FDI attacks using an innovative approach.

The study [8] made use of the fact that FDI attacks, which elude conventional detection methods, represent a serious risk to the electrical system. This is countered by a framework based on deep learning (DL) that makes long short-term memory (LSTM) and convolution neural networks (CNN). The work [9] improved recognition against FDI assault by introducing an automatic encoder sequential for the sequence framework for forecasting-aided recognition of anomalies. The model surpasses current benchmarking approaches in enhancing data injection attacks and reducing false positive rates (FPR), guaranteeing precise energy usage status forecasting for operational decision-making. The study [10] examined the methods to improve cyber security measures by utilizing a variety of AI models. To increase the precision and speed of cyber threat identification, it makes use of machine learning (ML), DL, and anomaly detection methods. According to a study [11] AI assists in avoiding the break of susceptible companies and client information by early threat detection. The study [12] provided the blockchain-based and AI-based secure drone communication infrastructure. The architecture improves network performance, security, privacy, and transaction storage costs by utilizing the Inter-Planetary File System (IPFS) for data storage. The research [13] investigated how AI might be used to tackle the problems of smart cities by utilizing blockchain technology, which forms the basis of Bitcoin but also facilitates the management, control, and streamlining of numerous local administrations.

The paper [14] introduced a dynamic analysis-based method that could be applied to different kinds of cyber attacks in a model of the Western System Coordinating Council system. The study [15] suggested a mathematical model that posed a threat to the on-grid system, the economy, and society through fake data injection attacks. The researchers [16] suggested Delta thresholds, regression analysis with time stamps, and other network topology-independent approaches for detecting false data in SG. These techniques complement current data, allowing for the detection of omitted observations. Recent protection tactics include temporal behavior-based fake data detection and Alternative Current (AC) State estimation. The study [17] utilized the secure federated DL method for FDI attack detection was developed by combining the Transformer framework, federated training, and the Paillier security system. The study [18] explored the potential of concept drift in SG systems to improve AI. Conventional state estimations are susceptible to data integrity breaches including FDI, which can elude monitoring systems. The study [19] provided an improved way of detecting covert attacks before they impact the system, utilizing a Kalman filter with a suggested detector. Tests validate the efficacy of this approach, strengthening the system's resistance against possible intrusions. Radial basis function parameters are estimated using the Polar Bear Optimization technique, and SG network datasets are used to examine the AdaBelief Exponential Feature Selection-Kernel based Extreme Neural Network (AEFS-KENN) [20] big data security architecture. They discussed how machine learning can be applied to address cybersecurity concerns related to SG [21].

The paper [22] emphasized the authenticity of false information intrusions on the smarter grid' physical components. A malware risk measure was provided by the idea for actual information consistency as its first contribution using an agent-based paradigm. The study [23] introduced a flawed correlation matrix-based reconnaissance method and an advanced learning-based state prediction approach to immediate time the FDIA recognition. The suggested architectural design is scalable, effective, and minimizes error margin. The study [24] investigated power thefts in distributed generation (DG) domains, where unscrupulous consumers alter readings from smart meters to fraudulently declare that more energy is being delivered to the grid and overcharge the utility provider. The study [25] proposed a method to detect fake data injection attacks on state estimation using data-driven machine learning. The system uses multiple classifiers, with individual classifiers'

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

judgments further classified using ensemble learning. The approach employs supervised and unsupervised classifiers. The cuttlefish optimization coupled with an enriched recurrent neural network (CO-ERNN) is intended to be a classifier, it minimizes training complexity and execution time. The suggested method can be used to identify various kinds of FDI attacks intended to detect.

2.0 MATERIALS AND METHODS

2.1 Invisible Attack Detection Model

The proposed Cuttlefish Optimization coupled with the Enriched Recurrent Neural Network (CO-ERNN) method is utilized to recognize optimal FDI assaultamongSG, and functionality of the novel program is utilized to identify assaults that are invisible by SVE shown in Figure 1.

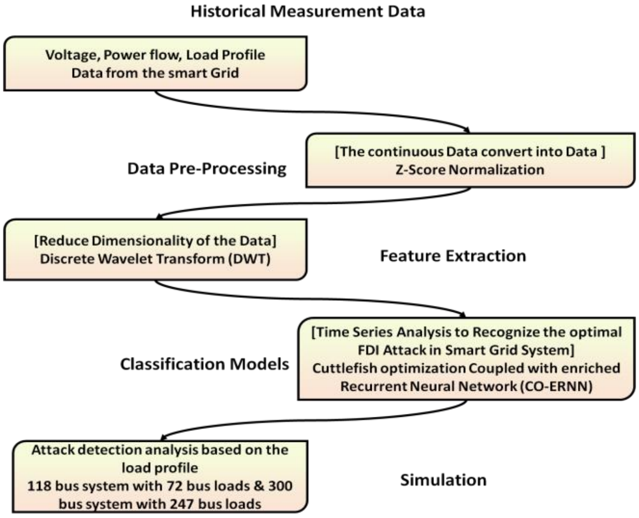
Historical Measurement Data
Voltage, Power flow, Load Profile Data from the smart Grid
Data Pre-Processing
[The continuous Data convert into Data] Z-Score Normalization
[Reduce Dimensionality of the Data] Discrete Wavelet Transform (DWT)
Feature Extraction
Classification Models
[Time Series Analysis to Recognize the optimal FDI Attack in Smart Grid System] Cuttlefish optimization Coupled with enriched Recurrent Neural Network (CO-ERNN)
Attack detection analysis based on the load profile 118 bus system with 72 bus loads & 300 bus system with 247 bus loads
Simulation

Figure 1: CO-ERNN model

2.1.1 Historical data

A SCADA system communicates the measurement data from the power flow, bus voltage, load profiles, and branch power flow. Load profiles monitor energy consumption trends, which helps to identify the irregularities related to cyber-attacks. Data on branches' power flows reveals the flow of electricity and its significance for identifying the power flow alterations. Bus voltage detects possible cyber breaches and guarantees grid reliability. Bus power circulation provides continuous monitoring enabling quick identification of threats. In the study, 30% is obtained for training, and 70% is used for testing. Accurate node localization techniques, such as adaptive methods using environmental thresholds, can also contribute to improved sensor placement and detection accuracy in power systems [28].

2.1.2 Data pre-processing technique using z-score normalization

This approach, which normalizes all input historical data to a single scale with an average of 0 and a standard deviation (SD) of 1, is the most used normalization method. For each of the characteristics, the mean and SD are calculated. The computed SD and mean are used to normalize each value in feature A. Equation (1) provides the transition.

$$X = \frac{(y - mean\ (Y))}{std(Y)} \tag{1}$$

In this case, mean (Y) is the attribute Y's mean, and $std\ (Y)$ is the attribute Y's SD. The fact that this strategy reduces the impact of outliers on the data makes it beneficial. Virtual fingerprint mapping approaches such as those using taper functions may also be considered for sensor signal normalization and spatial data smoothing in future work [27].

2.1.3 Feature extraction using discrete wavelet transform (DWT)

The wavelet scales and translations make up the discrete set known as the DWT is used to reduce the dimensionality of the pre-processed data. But this transformation breaks down the signal into a set of wavelet structures that are orthogonal to each other. The DWT uses a dynamic grid, in which the mother wavelet is translated by an integer $(b = k2j)$ and scaled by power two$(a = 2j)$, where j is the total number of scales and k is a location index that spans from $0\ to\ J$ $(J$ is the number of observations). The DWT is represented by the subsequent formula in Equation (2).

$$\psi_{i,r}(d) = 2^{\frac{i}{2}}\psi(2^i d = r) \tag{2}$$

The DWT coefficients are obtained from the following expression in the Equation (3)

$$U_{ir} = U(2^i, r2^i) = 2^{-i/2}\int_{-\infty}^{\infty} l(d)\overline{\psi 2^{-\iota} d - r)}td \tag{3}$$

2.1.4 Enriched recurrent neural network (ERNN)

Enriched Recurrent neural networks (ERNNs) are enhanced by using long short-term memory (LSTM) to form an ERNN. LSTM addresses the issue of missing and expanding gradient by using simple ERNN units to analyze the time series data to recognize the optimal FDI attack. Compared to standard ERNNs, LSTMs are far better at handling long-term dependencies. The LSTM layer, which provides the categorized output, is the model's last layer. While the LSTM layer is used for classification and prediction, the hidden layers are utilized to extract features from the input data. There are four gates in this stratum, and they are described from Equation (4) to Equation (5). Segmentation techniques, including both static and dynamic fingerprinting, have been

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

proven effective in related localization domains and may enhance feature extraction reliability when adapted for smart grid environments [26].

Input Activation

$e_d = tanh(U_e.Y_d + W_e.out_{d-1} + p_e)$ (4)

Input Gate

$j_d = \sigma(U_j.Y_d + W_j.out_{d-1} + p_i)$ (5)

Forget Gate

$l_d = \sigma(U_l.Y_d + W_l.out_{d-1} + p_l)$ (6)

Output Gate

$q_d = \sigma(U_q.Y_d + W_q.out_{d-1} + p_q)$ (7)

This resulted in

Internal state

$state_d = e_d \Theta j_d + l_d \Theta state_{d-1}$ (8)

Output

$out_d = tanh(state_d)\Theta q_d$ (9)

Based on the previous hidden state, the forget gate in an LSTM cell regulates the information flow from the cell state. Information is discarded according to the current input when it's implemented as a sigmoid activation function. It assigns the proper class to the characteristics that were taken out of the preceding layer. The softmax function is an activation function that is used to forecast the outcome and classify these extracted properties.

***Output Layer*:**

Binary data was obtained as the output. Output values 0 (FDI attack recognized yes) and 1 (FDI attack recognized no) are provided by the output layer shown in Figure 2.

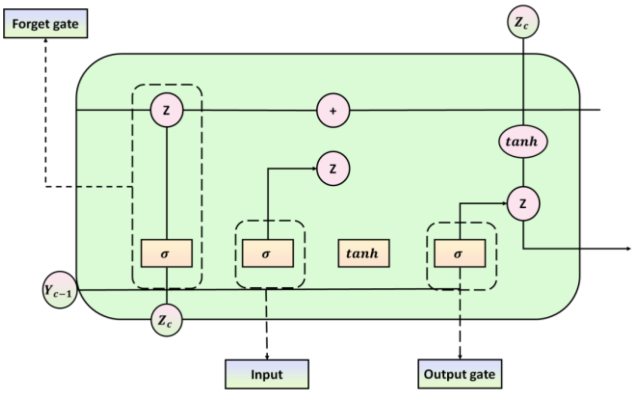

Figure 2: Architecture of ERNN

2.1.5 Cuttlefish optimization (CO) model

An algorithm for optimizing using global meta-heuristics is called the CO. The cuttlefish creatures' instinctive behavior serves as the paradigm. The cuttlefish's primary three skin layers, and the ray layers, allow it to alter its reflection color and rearrange the arrangement of its three skin cell layers in six different scenarios. Reflection and visibility are the two primary methods utilized in the algorithm to identify the optimal FDI attack. It's provided in the Equation (10).

$Err_{min} = \sum_{j=1}^{r} \sum_{Y\epsilon N_j} \sqrt{(Y - V_j)^2}$ (10)

Where, r is the number of clusters, N_j is a subset of data belonging to cluster j, Y is a data vector belonging to N_j and V_j is the mean of the points in N_j which represent the center of cluster$j$. Finding the pertinent cluster centroids that minimize the distances between the data vectors and the cluster centers using Equation (11) is the job of the CFO in the cluster.

$Y_{new} = Reflection + Visibility$ (11)

CFO clustering follows the following phases:

Phase 1: Set up the population initially. $P$is the cuttlefish's swarm position, and each particle in the population is given the appropriate cluster of centroids at random.

Phase 2: Determine each particle's efficiency value and the best overall answer globally.

Phase 3: Make four groupings out of the population. Every group offers the answer using the subsequent formulas as a basis.

(a) Determine the best global solution's average value.

(b) Group 1 provides the updated solution based on the existing one as represented from Equation (12) to Equation (19),

$Reflection = K * Y_{cur}$ (12)

$Visibility = C * (Y_{best} - Y_{cur})$ (13)

(c) Group 2 provides a fresh approach based on the most effective one at the moment.

$Reflection = K * Y_{best}$ (14)

$Visibility = C * (Y_{best} - Y_{cur})$ (15)

(d) Group 3 provides a fresh approach focused on the optimal resolution.

$Reflection = K * Y_{best}$ (16)

$Visibility = C * (Y_{best} - Y_{avg})$ (17)

(e) Group 4 provides the updated solution based on a haphazard exploration of the subject area.

$Reflection = randomly\ created\ solution$ (18)

$Visibility = 0$ (19)

Where, Y_{best} the best possible global approach, Y_{cur} is the current conclusion, Y_{avg} is the mean of the optimal solutions, K and C are the uniform distribution's random values between $[k1, k2]$ and $[c1, c2]$ and which is determined by applying the equation $K = ((0 + (1-0).* rand(1,1)) * (k1 - k2)) + k2, C = ((0 + (1 - 0).* rand(1,1)) * (c1 - c2)) + c2$ Based on the choices

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

made for $k1, k2, c1$, and $c2$, the values of K and C are altered.

Phase 4: Update the particle's position by contrasting this solution with the earlier one.
Phase 5: Determine each particle's fitness based on its most recent position.
Phase 6: Update the particle's global best position.
Phase 7: Continue doing this until the stop requirement is met.

Those phases are depicted the Figure 3.

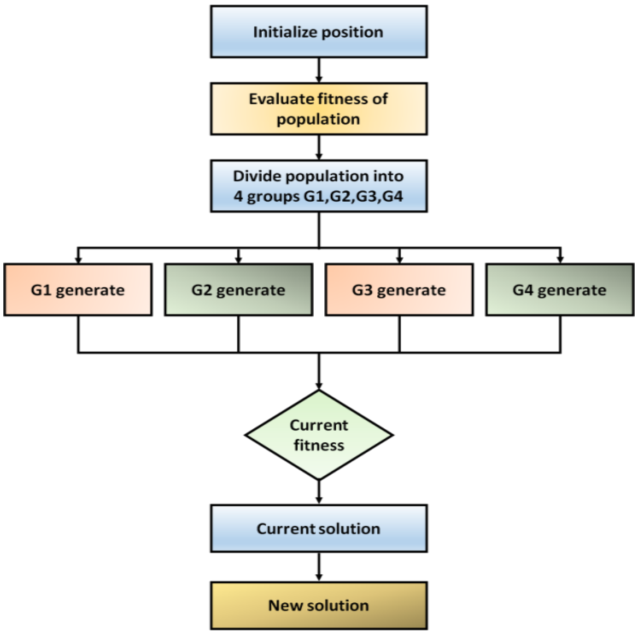

Figure 3: Architecture of CO

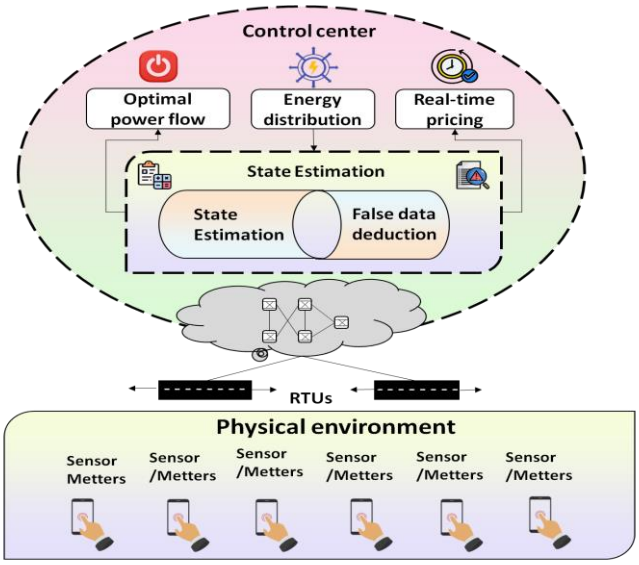

Figure 4: Power grid communication control system

2.1.6 CO-ERNN for recognize the optimal invisible FDI attack

The research proposes a CO-ERNN approach for recognizing Foreign Direct Investment (FDI) attacks in Singapore, merging LSTM with RNNs. The LSTM layer handles long-term dependencies and gradient problems, while the hidden layers extract features. The output layer categorizes the retrieved features, producing binary outputs indicating FDI attacks. The CO algorithm mimics cuttlefish behavior to optimize FDI attack recognition in SG. System state estimation is crucial for electrical network efficiency and reliability. SCADA computers send sensor data to a command center for on-site and distant data collection. The system evaluates data; estimates power system states, searches for emergencies, and provides guidance to Remote Terminal Units. Figure 4 depicts the Power grid communication control system.

2.1.7 Estimating direct current state and attacking false data injection

The control center's state estimator predicts the system's current state over time utilizing the steady system model and measurement data provided by the SCADA system. Let $h = [h_1, h_2, \dots h_m]^D \epsilon \mathbb{R}^n$ Vector of quantification, $y = [y_1, y_2, \dots y_m]^D \epsilon \mathbb{R}^m$ function as a condition variable, $e = [e_1, e_2, \dots e_m]^D \epsilon \mathbb{R}^n$ stands for the vector of measurement error, the observational approach can be explained in the Equation (20) as follows.

$$h = z(y) + e \tag{21}$$

For the direct current (DC) power flow approach, Equation (22) provides more information on the observed paradigm:

$$h = Zy + e \tag{22}$$

The matrix of Jacobian shapes illustrating the structure of the power system $Z\epsilon\mathbb{R}^{n\times m}$ represents the Additive White Gaussian Noise (AWGN) model of the environment and standard deviation$a \sim \mathcal{N}(0, \sigma^2)$. The approximate state of the system y can be expressed by the following equation by using statistical estimation standards, such as the Minimum Mean-Square Error (MMSE) as shown in Equation (23),

$$\hat{y} = (Z^D \Lambda Z)^{-1} Z^D \Lambda h \tag{23}$$

Herediagonal-matrix is Λ, and its diagonal members are $\Lambda_{ii} = \sigma^{-2}$. The perpetrators in the position can initiate attacks on FDI for the theft of electricity because they are aware of the system topology, which can be expressed through the Jacobianmatrix h, and they can compromise a restricted quantity of state estimate data load profiles. When FDI attacks are

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

https://doi.org/10.4314/njt.v44i2.14

present, the observational model is explained in Equation (24) as follows based on these presumptions.

$$\hat{h}_a = Zy + a + e \tag{24}$$

Where, a represents an attack direction and $a \neq 0$ in the event of FDI attacks.

2.1.8 The attack detection technique

The proposed real-time method for FDI attack prevention is illustrated in Figure 5 and consists of the State Vectors Estimate (SVE) and cuttlefish optimization coupled with an enriched recurrent neural network (CO-ERNN) scheme.

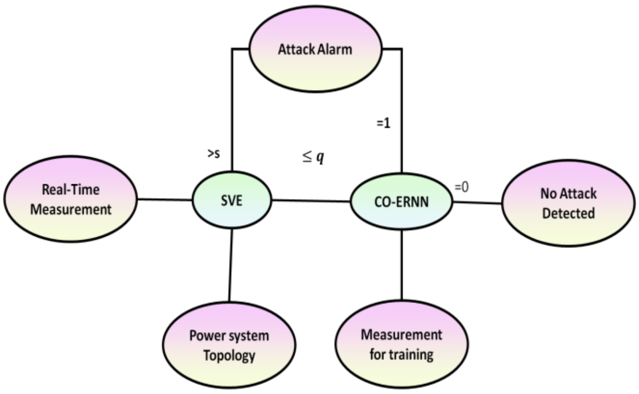

Figure 5: Proposed model for false data identifying

The proposed CO-ERNN system and an SVE make up the current time mechanism that has been proposed for identifying FDI attacks. By computing $\ell 2$-norms of capacity and comparing among preset entranceτ, SVE assesses real-time data from measurements. The paper explored the numerical threshold value τ, highlighting its impact on the resilience of the SVE system to environmental noise and its efficacy. By distinguishing between FDI attacks that are detectable by SVE and those that are not, the suggested detection technique increases the effectiveness of the detection process by using the CO-ERNN scheme to identify unobservable FDI attacks as shown in Equation (25).

$$\begin{cases} \eta = \left\| \hat{h} - Z\hat{y} \right\|_2 > \tau \; Attack\ alarm\ is\ reported; \\ \eta = \left\| \hat{h} - Z\hat{y} \right\|_2 \geq \tau \; No\ Attack\ alarm\ is\ reported; \end{cases} \tag{25}$$

We refer to FDI attacks that SVE can identify as visible FDI attacks and that SVE is unable to identify as invisible FDI attacks. Consequently, the role of the CO-ERN method in the suggested surveillance system is to recognize invisible FDI attacks.

3.0 RESULTS AND DISCUSSION

3.1 Results

The IEEE 118-bus and IEEE 300-bus power test structures are used to test a cyber-assault recognition technique. The MAT-POWER toolkit is used to create a Jacobian matrix and acquire state and standard observation variables. Simulations use load profiles from actual load profiles. The proposed approach for SG is used to create synthetic and artificially manufactured compromised data. The IEEE's real-time cyber-attack authentication system is expected to distort 72 load features and 247 load features against foreign direct investment attacks. IEEE 118 bus-system model shows in Figure 6.

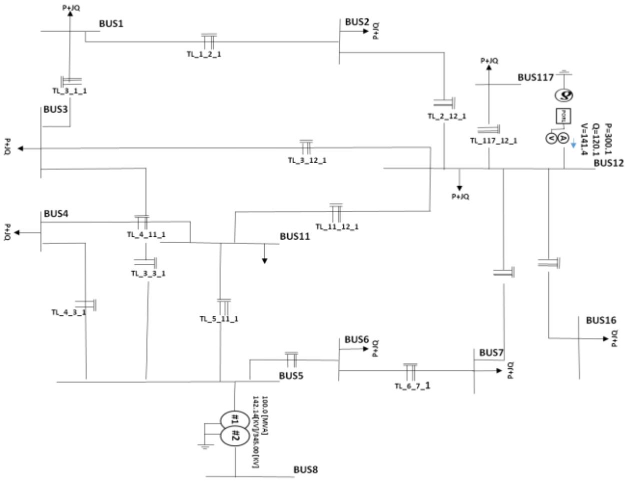

Figure 6: IEEE 118 bus-system model

Case 1: The IEEE 300-bus energy evaluation system is used to evaluate the scalability of the load bus monitoring technique. Although the computer system classifies 247 bus lines as loading buses, hackers could be able to compromise up to 179 buses by employing FDI attacks. A higher detection threshold of $\tau = 30$ and an $AGWN = 0.5$ standard deviation are established to minimize false positives. The bigger framework is more vulnerable to disturbance from its surroundings due to its intricate architecture. The recognition technique works best with an accuracy rate of over 85, based on the outcomes of the experiment.

Case 2: In this case, it initiates the investigation of real-world FDI attacks for the theft of electricity. It's logical to anticipate that the attacker is going to exert an effort to reduce the attacking ratio, which is calculated as the proportion of the FDI values to the corresponding real estimations of the utilization of load. When these attacks occur in real life, the assailants' intention is to steal electricity with the least amount of chance of detection to be $\leq \zeta$. As a result, we update the attack model's third restriction in the following equation: Where the attackers' personalities influence the choice of "$\zeta, and\ \zeta = 1/2$" is the model in the present instance is chosen.

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

https://doi.org/10.4314/njt.v44i2.14

The updated attack approach is employed to assess the effectiveness of the proposed identification strategy. The assessment findings are shown in Figure 7 and Table 1, respectively, using matrices of confusion and the Receiver Operating Characteristic (ROC) curve.

The detection method's resilience in differentiating between compromised and unaffected states inside the power grid network is demonstrated by its high accuracy of 97.48% for recognizing susceptible situations and 97.73% for normal ones. Figure 8 depicts the comparison graph for vulnerability and normal of the detection approach accuracy.

Table 1: Outcome of detection of the FDI Attack

Actual Label	Quantity of testing Data	Determined to be vulnerable	Determined to be normal	Accuracy (%)
Vulnerable	1405	1204	92	97.48
Normal	1207	24	1359	97.73

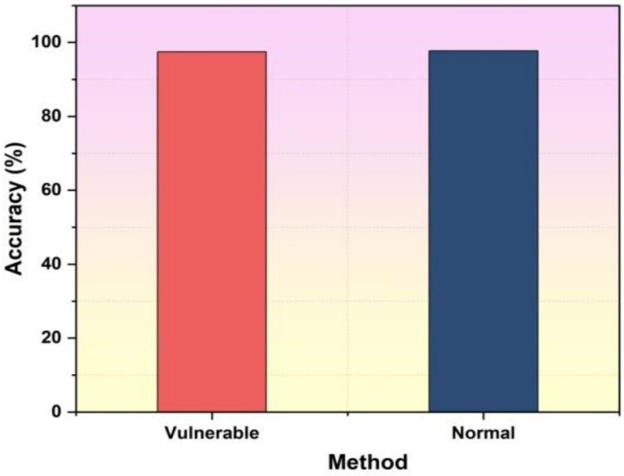

Figure 7: Accuracy of the CO-ERNN

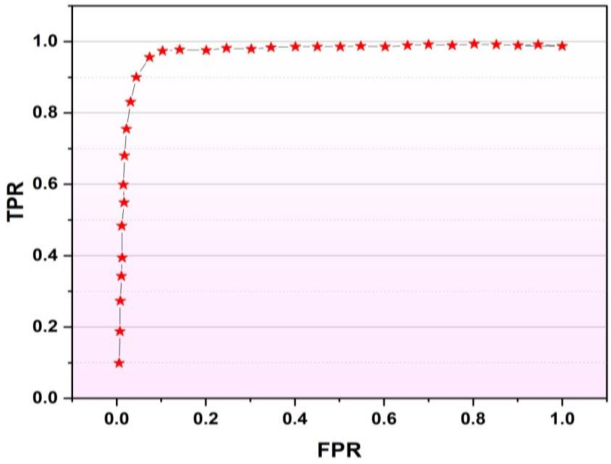

Figure 8: ROC curve of detection of the FDI attack

The ROC curve for the cyber-attack recognition strategy is displayed in Figure 8. Plotting the FPR against the True Positive Rate (TPR) yields the ROC. The recognition system's sensitivity is measured by FPR, which CO-ERNN defines as the probability that the standard information is identified as affected. To determine the sensitivity of the CO-ERNN technique, one uses TPR, and the probability that compromised information will be identified as compromised.

The proposed detection technique successfully identifies the realistic FDI attacks, as evidenced by the fact that it can identify invisible FDI attacks with detection accuracy greater than 97%. The modified FDI attack model is solved to produce synthetic tagged compromised data that is used to train the CO-ERNN architecture of the monitoring strategy.

3.2 Discussion

The significant improvement on operational efficiency and monitoring constituted the integration of computers in Smart grid management. The SCADA architecture were vulnerable to the FDI attack, which poses a serious danger to data integrity and system dependability. To detect the behavioral characteristics of FDI assaults utilized DL algorithms in conjunction with historical measurement to solve issues. The proposed CO-ERNN approach successfully identifies FDI assaults. The cybersecurity attack detection system were more reliable, which lowers presumptions about possible attack scenarios. The integration of optimization approaches enables the CO-ERNN model to exhibit strong detection capabilities and adjust different assault patterns. The CO-ERNN approach improves the detection system's adaptability and capacity to manage a range of assault situations, enhancing the energy system's overall security. Simulation outcomes using the IEEE 118-bus test system verify the efficiency of the CO-ERNN approach. The results illustrate how successfully the suggested attack detection method detects FDI assaults, highlighting its potential for real-world use in raising the security and dependability of smart grids.

4.0 CONCLUSION

In this research, we offer a real-time FDI attack detection technique based on DL. We suggest an exclusive type of FDI attack that uses an optimization model as a tool to steal power. By utilizing CO-ERNN, the proposed method successfully displays the incredibly high dimensionality periodical action aspects of the invisible false data attacks that avoid the SVE apparatus. Using an IEEE 300-bus system and an IEEE 118-bus power test system; we use four simulations to demonstrate the approach. In the first two scenarios, we examine how the attack recognition strategy performs regarding the number of

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

compromise measurements, the SVE's recognition threshold, and the amount of noise outside. In the third scenario, The IEEE 300-bus network is used to investigate the scalability of the CO-ERNN approach. The enormous volume of information created and communicated by smart grids combined with its complexities and interconnectedness makes it difficult to detect malicious information attacks. The CO-ERNN technique has difficulties with actual time execution, complicated assault situations, computational difficulty, and limited duration and resource restrictions. Algorithms must constantly change due to the fast growth of cyber-attacks. As machine learning and artificial intelligence (AI) progress, it will become easier to identify fake data hacking attempts because they can assess large amounts of historical information during actual time and more accurately recognize trends and abnormalities. Block chain-based technologies can improve the integrity and confidentiality of data, but creating novel approaches will require cooperation among researchers, information security specialists, and economic players.

REFERENCE

[1] Unsal, D. B., Ustun, T. S., Hussain, S. S., and Onen, A. "Enhancing cyber security in SG: false data injection and its mitigation", *Energies*, 14(9), p.2657; 2021. https://www.mdpi.com/1996-1073/14/9/2657#

[2] Sengan, S., Subramaniyaswamy, V., Indragandhi, V., Velayutham, P. and Ravi, L. "Detection of false data cyber-attacks for the assessment of security in SG using deep learning", *Computers & Electrical Engineering*, 93, p.107211; 2021. https://doi.org/10.1016/j.compeleceng.2021.107211

[3] Kandasamy, V., and Roseline, A. A. "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks", *Sci Rep* 15, P.1697-1712 (2025). https://doi.org/10.1038/s41598-025-85547-5

[4] Reda, H. T., Anwar, A., Mahmood, A. N. and Tari, Z. "A Taxonomy of Cyber Defence Strategies Against False Data Attacks in SG",. ACM Computing Surveys, 55(14s), pp.1-37; 2023. https://doi.org/10.1145/3592797

[5] Algarni, A., and Thayananthan, V. "Autonomous vehicles: The cyber security vulnerabilities and countermeasures for big data communication", *Symmetry*, 14(12), p.2494. 2022. https://doi.org/10.3390/sym14122494

[6] Cui, L., Qu, Y., Gao, L., Xie, G., and Yu, S. "Detecting false data attacks using machine learning techniques in SG: A survey", *Journal of Network and Computer Applications*, 170, p.102808. 2020. https://doi.org/10.1016/j.jnca.2020.102808

[7] Stoustrup, J., Annaswamy, A., Chakrabortty, A. and Qu, Z. "SG control", *Springer International Publishing*, 10, pp.978-3. 2019. https://doi.org/10.1007/978-3-319-98310-3

[8] Niu, X., Li, J., Sun, J. and Tomsovic, K. "Dynamic detection of false data injection attack in SG using deep learning", *In 2019 IEEE Power & Energy Society Innovative SG Technologies Conference (ISGT)*, pp. 1-6; 2019 February. https://doi.org/10.1109/ISGT.2019.8791598

[9] Mahi-Al-Rashid, A., Hossain, F., Anwar, A. and Azam, S. "False data injection attack detection in SG using energy consumption forecasting", *Energies*, 15(13), p.4877. 2022. https://doi.org/10.3390/en15134877

[10] Al Siam, A., Alazab, M., Awajan, A., and Faruqui, N. "A Comprehensive Review of AI's Current Impact and Future Prospects in Cybersecurity," in IEEE Access, vol. 13, pp. 14029-14050, 2025, doi: 10.1109/ACCESS.2025.3528114.

[11] Gupta, R., Kumari, A. and Tanwar, S. "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications", *Transactions on Emerging Telecommunications Technologies*, 32(1), p.e4176. 2021. https://doi.org/10.1007/978-981-99-2115-7_16

[12] Vivek Menon, U., Vinoth Babu Kumaravelu, Vinoth Kumar, C., Rammohan, A., Sunil Chinnadurai, and Rajeshkumar Venkatesan, "AI-Powered IoT: A Survey on Integrating Artificial Intelligence With IoT for Enhanced Security, Efficiency, and Smart Applications," IEEE Access, vol. 13, pp. 50296–50339, 2025, doi: 10.1109/ACCESS.2025.3551750.

[13] Krishnamoorthy, R., Kamala, K., Soubache, I. D., Karthik, M. V. and Begum, M. A. "Integration of blockchain and artificial intelligence in smart city perspectives", *Smart City Infrastructure: The Blockchain Perspective*, pp.77-112. 2022. https://doi.org/10.1002/9781119785569.ch3

[14] Amin, B. R., Taghizadeh, S., Rahman, M. S., Hossain, M. J., Varadharajan, V. and Chen, Z. "Cyber attacks in SG–dynamic impacts, analyses, and recommendations", *IET Cyber-Physical Systems: Theory & Applications*, 5(4),

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/

pp.321-329. 2020. https://doi.org/10.1049/iet-cps.2019.0103

[15] Habib, A. A., Hasan, M. K., Alkhayyat, A., Islam, S., Sharma, R. and Alkwai, L. M. “False data injection attack in SG cyber-physical system: Issues, challenges, and future direction”, *Computers and Electrical Engineering*, 107, p.108638. 2023. https://doi.org/10.1016/j.compeleceng.2023.108638

[16] Nawaz, R., Akhtar, R., Shahid, M. A., Qureshi, I. M., and Mahmood, M. H. “Machine learning-based false data injection in SG”, *International Journal of Electrical Power & Energy Systems*, 130, p.106819. 2021. https://doi.org/10.1016/j.ijepes.2021.106819

[17] Li, Y., Wei, X., Li, Y., Dong, Z. and Shahidehpour, M. “Detection of false data injection attacks in SG: A secure federated deep learning approach”, *IEEE Transactions on SG*, 13(6), pp.4862-4872. 2022. https://doi.org/10.1109/TSG.2022.3204796

[18] Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M., and Mohammadi-Ivatloo, B. “Ensuring cyber security of SG against data integrity attacks under concept drift”, *International Journal of Electrical Power & Energy Systems*, 119, p.105947. 2020. https://doi.org/10.1016/j.ijepes.2020.105947

[19] Akbarian, F., Ramezani, A., Hamidi-Beheshti, M. T. and Haghighat, V. “Advanced algorithm to detect stealthy cyber-attacks on automatic generation control in SG”, *IET Cyber-Physical Systems: Theory & Applications*, 5(4), pp.351-358. 2020. https://doi.org/10.1049/iet-cps.2019.0074

[20] Muthubalaji, S., Muniyaraj, N. K., Rao, S. P. V. S., Thandapani, K., Mohan, P. R., Somasundaram, T. and Farhaoui, Y. “An Intelligent Big Data Security Framework Based on AEFS-KENN Algorithms for the Detection of Cyber-Attacks from SG Systems”, *Big Data Mining and Analytics*, 7(2), pp.399-418. 2024. https://doi.org/10.26599/BDMA.2023.9020022

[21] Nijim, M., Kanumuri, V., Al Aqqad, W., and Albataineh, H. March. “Machine Learning-Based Analysis of Cyber-Attacks Targeting SG Infrastructure”, *In International Conference on Advances in Computing Research, Cham: Springer Nature Switzerland*, pp. 334-349; 2024, March. https://doi.org/10.1007/978-3-031 -56950-0_28

[22] Zhang, Y., Wang, J., and Chen, B. “Detecting false data injection attacks in SG: A semi-supervised deep learning approach”, *IEEE Transactions on SG*, 12(1), pp.623-634. 2020. https://doi.org/10.1109/TSG.2020.3010510

[23] Mukherjee, D. “Detection of data-driven blind cyber-attacks on SG: A deep learning approach”, *Sustainable Cities and Society*, 92, p.104475. 2023. https://doi.org/10.1016/j.scs.2023.104475

[24] Ismail, M., Shaaban, M. F., Naidu, M. and Serpedin, E. “Deep learning detection of electricity theft cyber-attacks in renewable distributed generation”, *IEEE Transactions on SG*, 11(4), pp.3428-3437. 2020. https://doi.org/10.1109/TSG.2020.2973681

[25] Ashrafuzzaman, M., Das, S., Chakhchoukh, Y., Shiva, S., and Sheldon, F. T. “Detecting stealthy false data injection attacks in the SG using ensemble-based machine learning”, *Computers & Security*, 97, p.101994. 2020. https://doi.org/10.1016/j.cose.2020.101994

[26] Koyuncu, H. and Yang, S. H. “Improved adaptive localisation approach for indoor positioning by using environmental thresholds with wireless sensor nodes”, *IET Wireless Sensor Systems*, 5: 157–165; 2015. https://doi.org/10.1049/iet-wss.2013.0100

[27] Koyuncu, H., and Yang, S. H. "Improved Fingerprint Localization by Using Static and Dynamic Segmentation," 2014 International Conference on Computational Science and Computational Intelligence, Las Vegas, NV, USA, 2014, pp. 149–156. https://doi.org/10.1109/CSCI.2014.32

[28] Koyuncu, H., and Yang, S. H. "Indoor Positioning with Virtual Fingerprint Mapping by Using Linear and Exponential Taper Functions," *IEEE International Conference on Systems, Man, and Cybernetics*, Manchester, UK, 2013, pp. 1052–1057. https://doi.org/10.1109/SMC.2 013.183

© 2025 by the author(s). Licensee NIJOTECH.
This article is open access under the CC BY-NC-ND license.
http://creativecommons.org/licenses/by-nc-nd/4.0/