Mesopotamian journal of Cybersecurity
Vol.2022, **pp**. 38–46
DOI: https://doi.org/10.58496/MJCS/2022/005; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Research Article

Detection of False Data Injection Attack using Machine Learning approach

Siti Nur Fathin Najwa Binti Mustaffa [1], muhammad Farhan[2, *]

[1]*PhD Computer Science and Software Engineering UMP, Malaysia*

[2]*Lecturer at Institute of computing and information technology, Pakistan*

ARTICLEINFO

Article History

Received 10 May 2022
Accepted 15 July 2022
Published 20 July 2022

Keywords

Deep Neural Networks
false data injection
real-time simulation

ABSTRACT

The "False Data Injection" (FDI) attack is one of the significant security risks that the deep neural Network is susceptible to. The purpose of the FDI attacks is to deceive industrial platforms by faking sensor readings. considered a few relevant systematic reviews that have been previously published. Recent systematic reviews may include both older and more recent works on the topic. Therefore, I restricted myself to recently published works. Specifically, we analyzed data from 2016-2021 for this work. Attacks using FDI have effectively beaten out traditional threat detection strategies. In this paper, we provide an innovative auto-encoder-based technique for FDI attack detection (AEs). use of the temporal and spatial correlation of sensor data, which may be used to spot fake data. Additionally, the fabricated data are denoised using AEs. Performance testing demonstrates that our method is effective in finding FDI attacks. Additionally, it performs much better than a similar technique based on a support vector machine. The ability of the denoising AE data cleaning method to recover clean data from damaged (attacked) data is also shown to be quite strong.

1. INTRODUCTION

The connection between the data stream and energy stream in power frameworks is expanding because of the ongoing advancement of data innovation [1]. Conventional power frameworks have formed into cyber-physical power systems (CPPS) using the joining of PC frameworks, correspondence networks, and actual settings [2]. Digital frameworks are turning out to be increasingly more coordinated into brilliant matrices' creation of the board and dispatch control processes. Because of the intrinsic vulnerabilities of sustainable power creation, the mix of renewables is imperiling the safe working of the present CPPS [3]. Notwithstanding, certain digital framework defects may be taken advantage of by aggressors, introducing significant dangers to the actual framework across digital actual spaces. They may even temporarily paralyze crucial infrastructure [4]. In the CPPS, FDIAs are sophisticated and long-lasting data integrity attacks. The system state estimate will be distorted as a result of changing the measurement data obtained, and the power grid will sustain harm from switches acting improperly [5]. People's attention has steadily been drawn to the CPPS's cyber security. Furthermore, the efficient identification of the FDIA has emerged as a critical issue that must be resolved for power systems to operate safely and steadily.

FDIAs in the CPPS have gained a lot of attention recently in power system research. In Liu et al., the FDIA was initially suggested (2011) [6]. The appropriate precepts are portrayed. At the point when the aggressor totally comprehends the framework geography data and related boundaries, it is guessed that they can really go after the power framework by staying away from the regular terrible data discovery instrument. Notwithstanding, practically speaking it is more hard for an assailant to get this information. Research has uncovered that FDIA can be started according to the aggressor's perspective regardless of whether they totally figure out the topological data. [7] Recommended a successive example mining way to deal with unequivocally extricate examples of organization attack and power framework obstruction from heterogeneous time synchronization data. The arrangement line can't be resolved utilizing this methodology since there is no satisfactory division plot. An elective way to deal with breaking down peculiar data was proposed, and therefore an AI

based model for power framework attack discovery was made. That procedure included recreating attributes that all around existed, which raised the registering cost. An attack location procedure in light of the CNN-GRU crossover model

*Corresponding author. Email: muhammadfarhan01@gmail.com

was introduced after the system and approach of FDIA under DC and AC models were investigated. To investigate the identification of FDIA attack signal under CPPS, the best combination assessment approach was made [8]. No direction is given on the most proficient method to pick the legitimate pay factor.

CPPS sensing technology is currently expanding, and data volume is growing as well. Traditional techniques' identification accuracy can no longer keep up with the rising demand in reality. At the same time, there are always new FDIA kinds appearing. Even if the topological information is not completely understood, it may launch attacks without using the standard detection system.

Coming up next are a few restrictions of the flow research on AI-based FDIA discovery: 1) One-sided attack location frameworks battle to perceive complex digital actual attacks because of the less cooperative examination of digital and actual data properties. 2) Powerful element mining approaches are required since the first CPPS data's qualities are confounded and include determination and change straightforwardly influence the dependability and exactness of the recognition discoveries. 3) Attack location speed is a critical part of real designing, consequently accelerating model computation is fundamental.

This exploration recommends a methodology for finding the FDIA in the CPPS in view of digital actual qualities, considering the confounded parts of the CPPS data. Coming up next are this paper's key commitments:

- The possibility of "FDIA qualities" is put out from the stance of the digital and actual mix of force frameworks. Subsets of quality attributes that are useful for attack recognition are screened utilizing the softening handling of data highlights, which likewise resolves the high-layered issue of data highlights. The greatest data coefficient is then presented for highlight determination.
- A stack auto-encoding network is utilized to construct an FDIA quality extraction model (SAE). Attack qualities are extricated utilizing a solo pre-preparing encoder, and attacks are ordered utilizing a directed tweaking classifier. The theoretical FDIA quality is naturally educated and extricated utilizing deep realizing, which can all the more precisely mirror the vital attributes of the FDIA based Deep Neural Network (DNN).

2. LITERATURE REVIEW

The discovery of covertness attacks has been achieved utilizing a large number of procedures and algorithms. In this field, AI methods have shown enormous achievement. Recurrent neural networks (RNNs)- based administered learning was utilized in [9] to distinguish FDI attacks. DNN, k-nearest neighbor (kNN), and extended nearest neighbor (ENN), three administered AI classifiers, were used in Yan, J.; Tang, B.; He, H (2016) [10]. For estimation grouping, many AI procedures are introduced in Ozay, M.; Esnaola, I.; Vural, F.T.; Kulkarni, S.R.; Poor, H.V (2015) [11]. Estimations might be classified as secure or under attack. In that examination, k-closest neighbor, DNN, and scanty calculated relapse were utilized. Another strategy utilizing the Gaussian blend model for the recognizable proof of FDI attacks was put out in Foroutan, S.A.; Salmasi, F.R (2012) [12]. The work in Yang, C.; Wang, Y.; Zhou, Y.; Ruan, J.; Liu, W (2018) [13] involved unaided advancement as its establishment. For FDI attack recognition, four AI strategies — a one-class DNN, a neighborhood exception factor, a seclusion timberland, and a powerful covariance assessment — were utilized. An AI-based system that used gathering learning was utilized by Ashrafuzzaman, M.; Das, S.; Chakhchoukh, Y.; Shiva, S.; Sheldon (2020) [14]. Numerous classifiers are utilized in outfit learning, and the ends arrived at by the different classifiers are additionally ordered. Two outfits were utilized in the proposed procedure. In the principal troupe, administered classifiers were used, while in the subsequent group, solo classifiers.

In Farrukh, Y.A.; Khan, I.; Ahmad, Z.; Elavarasan, R.M (2021) [15], directed learning was recommended utilizing two-layer progressive engineering. In the principal layer, the method of activity, like a typical state or a digital attack, was recognized. The sort of digital attack was classified in the subsequent layer. Acosta, M.R.; Ahmed, S.; Garcia, C.E.; Koo, I (2020) [16] Utilized an AI-based procedure for digital attacks that utilized a staggeringly irregular trees technique. Three AI strategies — a support vector machine (SVM), k-closest neighbor algorithm, and counterfeit neural organization — were utilized in Sakhnini, J.; Karimipour, H.; Dehghantanha (2019) [17] to empower FDI attack discovery. Three separate element determination techniques were utilized to every philosophy.

To distinguish FDI attacks, Xue, D.; Jing, X.; Liu, H (2019) [18] utilized an outrageous learning machine structure. Auto-encoders were used in Aboelwafa, M.M.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A (2020) [19] to distinguish FDI attacks. Utilizing auto-encoders, the secret relationship structures were found in the data. The fleeting and the spatial aspects were utilized to become familiar with the association in two aspects. Moreover, denoising auto-encoders were used to tidy up the harmed data. For the ID of attacks, strategies in light of consideration-based auto-encoders Wang, C.; Tindemans, S.; Pan, K.; Palensky, P (2020) [20] and auto-encoder neural networks Kundu, A.; Sahu, A.; Serpedin, E.; Davis, K (2020) [21] were additionally utilized. The commitment of Chen, J.; Mohamed (2021) [22] recognized the power framework's customary activity and the activity during the covertness attack. Two AI-based

strategies were utilized to recognize the covert attacks. An assortment of marked data was used for managed learning in the principal technique. That data was utilized to prepare a support vector machine (SVM). The inconsistency of the readings was found utilizing the subsequent methodology, which used no preparation data. To recognize secrecy attacks, an irregularity location method was utilized. Deep learning models were likewise used for the errand of FDI attack recognition. For the order of digital attacks in a savvy lattice, the deep neural network (DNN) model was utilized. Another deep learning-based way to deal with identifying FDI attacks was put out by Niu, X.; Li, J.; Sun (2019) [23].

A convolutional neural network (CNN) and a long short-term memory (LSTM) network were utilized in the recommended technique to distinguish dangers. A deep Q-network detection (DQND) technique acquainted might be utilized to find data honesty dangers in AC power frameworks. It is a strategy for deep support learning. To recognize deceitful data, utilized a neural organization model. In this case, the perceptron model's bits of feedback were the remaining components delivered through state assessment. Highlight extraction from estimation datasets and dimensionality decrease were both done utilizing auto-encoders. An improved generative adversarial network (GAN) design was then added, and this was used to recognize the FDI attacks. The strategies given AI were very powerful in identifying FDI attacks. They do, be that as it may, have specific limitations and weaknesses. A named dataset is expected for directed learning algorithms. They depend on a couple of acknowledged attack precepts. Like this, deep learning techniques additionally have critical disadvantages. To utilize these strategies, significant preparation is required. Deep learning procedures likewise request more memory space. The essential objective of the discovery structures is to protect against interruptions in the entire correspondence framework. A safe correspondence network is one of the fundamental parts of miniature matrices. The plan of a correspondence network is essential to its development. A complex plan for the execution of heterogeneous computerization and was recommended to screen the framework. Six practical levels were set up in the recommended plan to consider the reconciliation of equipment and programming gear. An itemized clarification of a shrewd matrix and the many kinds of correspondence methods might be found. The many types of correspondence were portrayed alongside their advantages and weaknesses. The mixture correspondence simulation model filled in as the establishment for commitment. Half and half organization geographies utilize both specific wired and remote media. To approve significant framework plan prerequisites, an assortment of mixture correspondence simulation models was made.

Manandhar, K.; Cao, X.; Hu, F.; Liu (2014) [24] Offered a numerical model of the power framework and recommended solid security design. The model's factors were assessed utilizing a Kalman channel. An internet-based data-driven framework for distinguishing FDI attacks on synchrophasor estimations. To find irregularities in the data, the proposed approach utilized thickness-based nearby exception factor examination. To gauge the express, the Kalman channel was utilized. The quickest recognizable proof of the attacks was made conceivable by means of a summed-up combined total methodology. The monetary impact of secretive FDI attacks on market tasks in real-time. It was likewise told the best way to construct a viable going-after system for the aggressor. It depicted the way that an assailant could make a secrecy FDI attack without monitoring the framework's design. The assailant approaches the framework design and may send off an attack.

To distinguish digital attacks, Du, D.; Li, X.; Li, W.; Chen, R.; Fei, M.; Wu, L (2019) [25] presented a circulated state gauge approach in view of the other heading technique for multipliers (ADMM). In this example, the K-implies approach was utilized to isolate the local subsystems. To find digital attacks, the methodology gives a web-based gauge of the time-shifting and obscure attack boundaries. By setting up a functioning data change method, the FDI attacks were found. Prior to being conveyed across correspondence networks, estimations and control data were changed in that procedure. A Kalman channel procedure and the comparable to show of a load frequency control (LFC) framework were utilized to make the recommended FDI attack identification technique.

The issue of false data location was depicted as low-rank grid recuperation. The issue was settled utilizing raised enhancement. The mix of the l1 standard and atomic standard was normalized utilizing the suggested approach. To accomplish a high union rate, the blended standard improvement issue was tended to utilizing the upgraded Lagrange method of multipliers. The issue of incorrect data identification was delegated a framework division issue. Attacks by FDI are rare. A strategy was made to recognize the conditions of the power framework and the inconsistencies. Low-rank grid factorization and atomic standard decrease were utilized to handle the issue.

3. MATERIAL AND METHOD

3.1. Description of False Data Injection Attack

FDI attack detection is the goal of this work. We apply the attack model in order to modify the application of our approach to the requirements and makeup of IoT systems. In this scenario, the intruder may change and/or inject fake data into one or more sensors at any moment to keep the false data within an acceptable range of real readings.

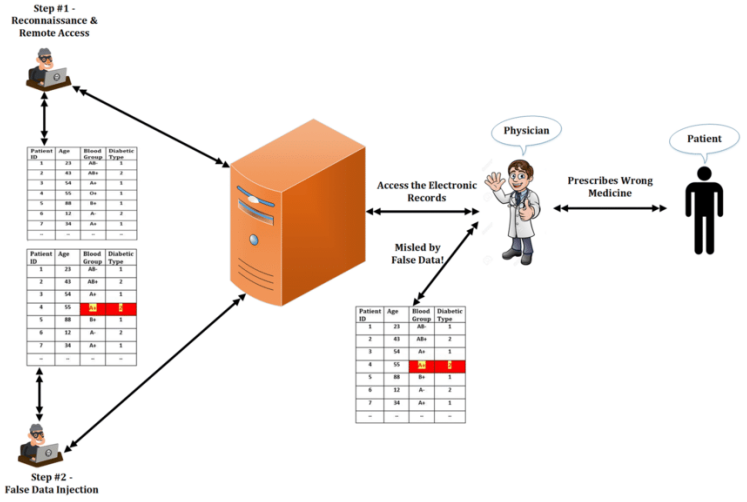

Fig 1 Proposed False Data Injection (FDI) Attack

3.2. Proposed Attack Detection Algorithm

As previously noted, an AE is utilised in this research for attack detection since it has the capacity to capture the data's structure and understand the association between readings. The corrupted data that the AE had previously discovered is then cleaned using a DAE.

3.2.1. Detection method based on autoencoders

The original data collected from the sensors is supplied to the AE during the training phase. The same data is the collection of target values. By the conclusion of this phase, the network is capable of compressing and subsequently decompressing the input vector using the inter-correlation between elements. The AE may then be utilized for false data detection when the training phase is over and the weights are determined. The network attempts to compress and decompress the input vector when erroneous data are supplied to the AE. The Mean Square Error (MSE), however, is higher than anticipated since the bogus data lacks the anticipated correlation pattern. The MSE is compared to a predetermined threshold, which is selected as the mean of the validation MSE, in order to identify incorrect data. An attack is declared when the MSE value goes beyond the specified threshold. It is important to note that validation is required to prevent overfitting, which occurs when the machine learns the training data too well and becomes unable to examine fresh data. This occurs when the validation error continues to rise while the training data are becoming less. Therefore, by keeping an eye on the validation error, the training process is abruptly stopped as it begins to rise.

3.2.2. Denoising Auto-encoder-based Data Cleaning

Following the detection of an attack, corrupted data is fed into a DAE. The original data is used as the goal output and the corrupted data is used as the training input for DAEs. The DAE is thus capable of retrieving the correlation between inputs. The DAE produces a clean version of the faulty input when false data are given into it. This version may then be used as a stand-in for the sensor being fixed while the system is still being processed.

3. RESULTS AND DISCUSSION

3.1. Simulation Setup and Parameters

The data set was used in simulations. The suggested conspires Auto encoder (AE) is created using 60% of the data, its approval is completed using 20% of the data, and its attempt is completed using the remaining 20%. To ensure that the

MSE is constrained, target values are defined during the preparation stage to be identical to include values, and loads are updated continuously throughout time. No objective outcome is established during approval and testing. The outcome is established in light of how the preparation altered the loads before determining the MSE. The approval error is used for two things. First of all, it is recommended to avoid overfitting. Second, it is used to calculate the edge that, when exceeded by the MSE, sets a warning (recognized attack). Testing error is examined (for each contribution) using the edge to determine if the information data are obtained. Neither misleading information during preparation nor marks for information preparation information must be supplied to AEs.

The contribution to the AE is adjusted to include more than one reading from each sensor at each emphasis rather than just one reading for each sensor to benefit from both the relationships between the sensors and the autocorrelation of the readings of a single sensor in the time-space. The AE was constructed and tested for Nt = 1, 2, 3, 4, 5, and 10, where Nt is the number of readings (time moments) from each sensor that must be handled by the AE at each age, to determine the ideal number of time moments to be considered. Fig. 2 shows the preparation hardship for each Nt esteem. At Nt = 2, the preparation and approval misfortune esteems are the lowest at 3.99e-7 and 4.37e-7, respectively. At Nt = 2, there is a trend of decreasing preparation and approval disasters.

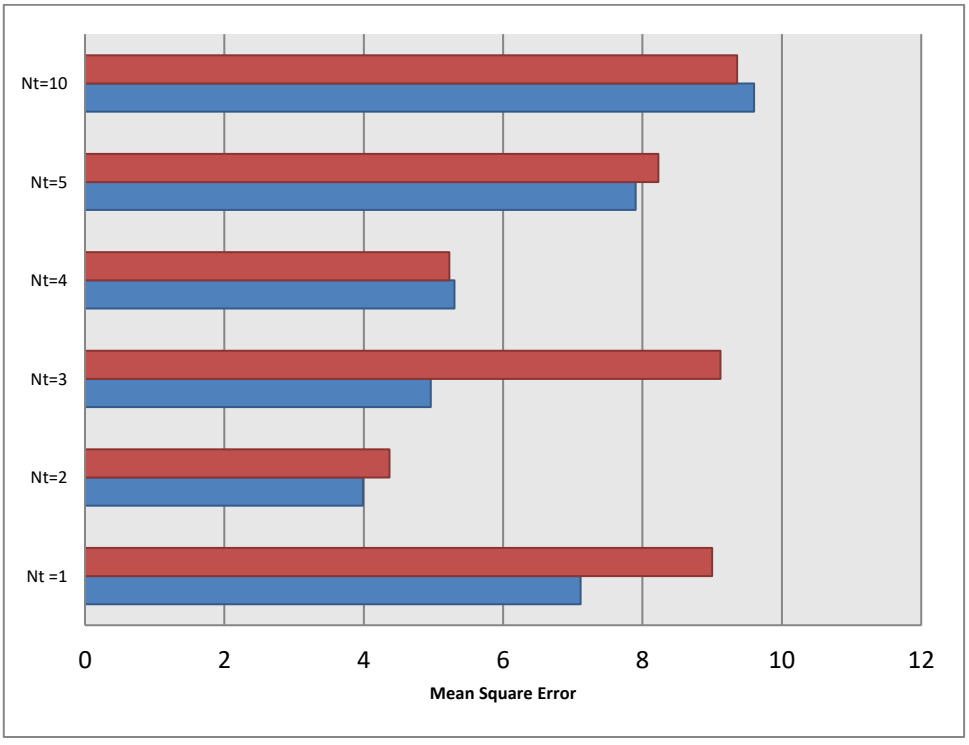

Fig. 2 The Impact of Variable Sensor Reading Count on Training and Validation Losses

The readings from each sensor are handled by the AE while the several sensors are lined up. There are 15 sensors throughout the company, and each one sends Nt consecutive readings to the AE every cycle. The information layer receives a total of 15 Nt neurons as a result. The resulting layer is the same as the info layer, as was previously mentioned. There are five hidden layers used. The pressure factor, which measures how many sources of information there are about the deepest layer of secrecy that still stands between the encoder and the decoder, is set at 3. The pressure factor shows that the hidden layers between the info (yield) layer and the deepest layer immediately shrink in size. It is important to note that, after a few preliminary steps, the number of hidden layers and the pressure factor are still very much up in the air.

However, while looking at the connection using DNN, we discover that DNN should be ready with the two types of data (false and unique), along with grades for each class. To prepare and name each arrangement of sensor data, some more

labor is needed to build up the fake (gone after) data. The machine creates the streamlining model during the preparation phase (given Lagrange multipliers). The model then explores fresh information sources throughout the testing phase and groups all of the classes (false data class or clean data class). Two methods are used to get the false data needed for testing and DNN preparation. 1) If all else is equal, add an irregular number to the passages. The uniform distribution draws the irregular number. Fig. 3: Misfortunes at the Preparation and Approval Stage. the range of +/ 10% of the initial value; referred to as "Case 1" in the next section. 2) Only change the portions of one sensor (to mimic the instance of just a single went-after sensor). The components of one sensor are replaced with another value taken from a typical distribution, whose mean and variance are comparable to those of unique data (To make a situation harder to be recognized). The rest of this part refers to this case as "Case 2." Under the two circumstances, the two machines (AE and DNN) were tested. The AE was tested for Nt = 1, 2, 3, 4, 5, and 10, as mentioned before. For each value of Nt, an actual test is conducted under "Case 1" and "Case 2" to provide further confirmation of the most optimal choice of Nt. Additionally, the DNN test was completed to create a fair correlation.

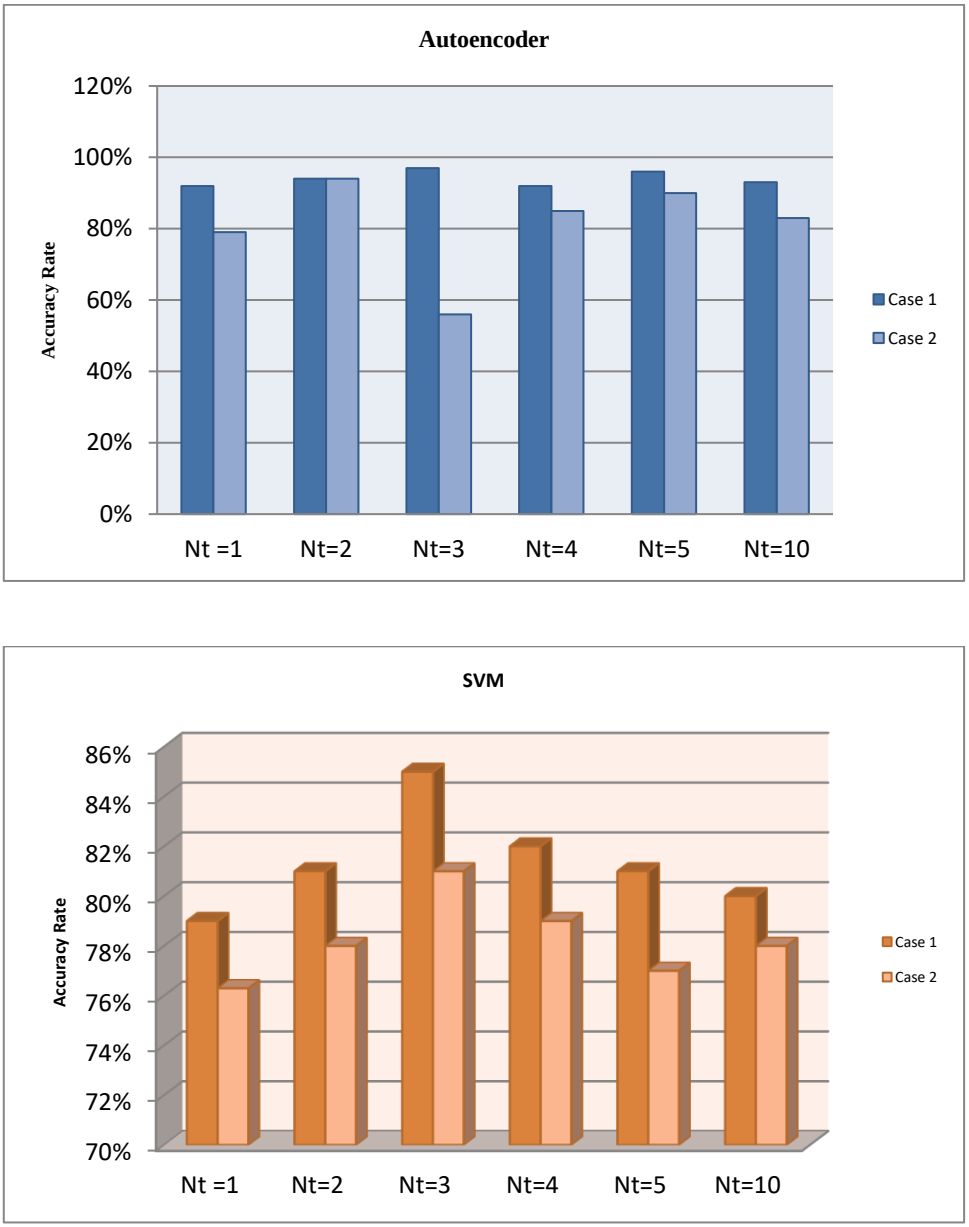

Fig 3 the impact of different sensor reading counts on decision accuracy

Fig. 3, which plots the degree of accurate selections, should show the results. The Precision Rate in the figure may be defined as the ratio of the number of passages that the machine precisely determined to the total number of passages (whether or not an attack or clean was completely set in stone). We may conclude from the figure that Nt = 2 is the best choice for the suggested AE-based graphic. Despite this, Nt = 3 seems to provide better results for the DNN. As a result, more correlations involving the optimal value of Nt for the comparison plan will take place. Additionally, Fig. 3 shows that "On the off chance that 1" (for the two machines) has a better exactness than "Case 2." This is due to the difficulty of locating only one faulty (gone after) sensor. Additionally, it is quite difficult to differentiate the kind of attack. This is because replacing the sensor readings with numbers from an average appropriation with a comparable mean and change would somewhat alter the readings between connections. It is also important to note that the suggested conspiracy has better accuracy overall than the DNN-based scheme.

3.2. Accuracy of the final decision is tested and compared

The demonstration of the two devices' capabilities for accurate attack detection and false alarm detection. The Pace of Discovery in the figure refers to the degree of erroneous information that the PC accurately identified as false in comparison to all parts. Additionally, the Pace of False Caution refers to the percentage of clean passages that are partially accepted to be phony data. As was previously said, the AE's ability to master the data structure is limited, which leads to more advanced execution and notable accuracy. False warnings and missed findings as a result of using the AE-based strategy. It is crucial to remember that sometimes the AE isn't superior to the DNN. For instance, AE was unable to identify the attack at time 175 but DNN could. However, AE genuinely provides a more notable degree of location and an unmatched standard presentation. The Receiver Operating Characteristics (ROC) plot for the two devices is shown in Fig. 4. The ROC describes the relationship between the rate of false alarms and the rate of recognition. When comparing two strategies, a unique strategy produces a higher identification rate for a given false caution rate. Fig 4 demonstrates that the AE-based plot outperforms the DNN-based conspiracy in terms of ROC as well.

3.3. Complexity Analysis

The preparation complexity of the DNN is about O (N3), where N is the total number of data passes [24]. The difficulty of creating AEs, however, is O (d k) for each cycle, where d is the number of informational aspects and k is the number of encoding aspects [25].

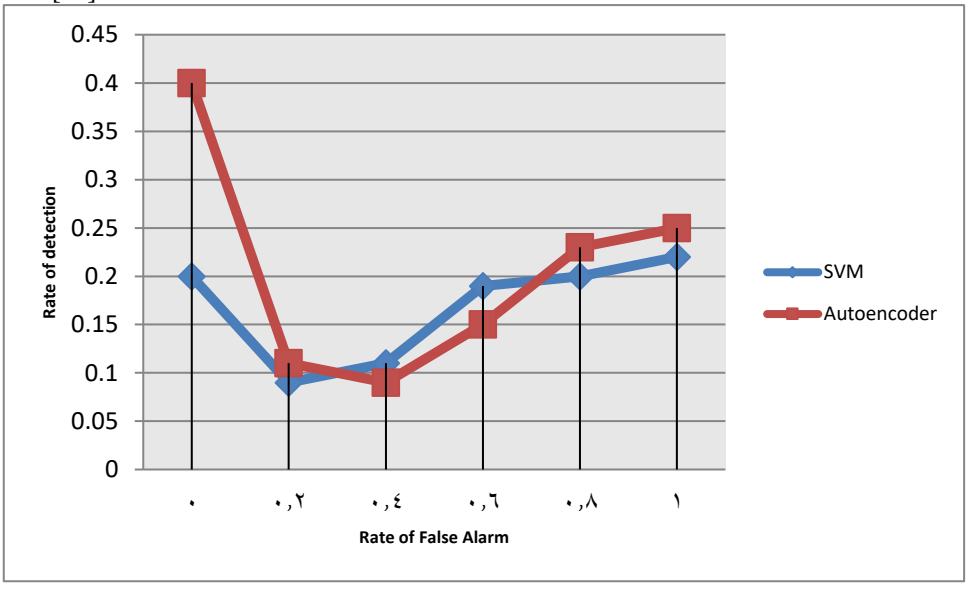

Fig 4 plot of the receiver operating characteristics

To apply this current to the circumstance, 132300 data were gotten from every sensor. Just 60% of the complete is used for preparing, yielding 79380. Each cycle, Nt = 3 readings from every sensor are taken, bringing about a sum of 79380 3 (= 26460) passages for every sensor. On account of 15 sensors, this yields N = 396900 data passages. This outcome in a

preparation intricacy for the DNN that is about identical to O(6e16). Interestingly, the AE's feedback vector has a component of d = Nt 15 = 30, though the encoded vector's size is k = 10. (Since the pressure factor is decided to be 3). Furthermore, the number of preparation ages — in our model, 20 — should be considered

4. CONCLUSION

In this work, we gave a creative strategy for recognizing counterfeit data injection attacks. When contrasted with approaches given DNN the recommended recognition technique performs better regarding identification execution. Also, on the grounds that AEs don't require marked data for preparation, they are more straightforward to create.

AEs may likewise learn to stow away muddled relationship designs in the data, which permits them to distinguish different attacks. The AE-based attack location framework is equipped for recognizing any attack that may physically change these relationship structures. This isn't valid for different classifiers, for example, DNN, which are instructed to perceive "specific" attacks (or a gathering of attacks), and which are unsure to perceive some other attacks for which they were not prepared to utilize named data. In the examination, we utilized two particular FDI attack situations that we alluded to as case 1 and case 2. In current technique gave the most obvious opportunity with regards to going after location in the two cases, alongside the least false alerts and fastest execution times. We also looked at the outcomes of using a denoising autoencoder to repair the damage the attack did to the data. The results demonstrated the demonizing auto encoder’s strong capacity to restore the data to its original state with very low mean square error values.

Funding

Funding for this paper was entirely self-sustained by the authors, and no financial assistance was sought from any academic or corporate entity.

Conflicts Of Interest

The authors disclose no conflicts of interest that could influence the impartiality or interpretation of the findings presented in this paper.

Acknowledgment

The authors extend their heartfelt appreciation to the anonymous reviewers for their constructive feedback, which significantly enhanced the quality of this paper.

References

[1] X. Yu and Y. Xue, "Smart grids: A cyber-physical systems perspective," Proc. IEEE, vol. 104, no. 5, pp. 1058–1070, 2016. doi: 10.1109/jproc.2015.2503119.

[2] R. He, H. Xie, J. Deng, T. Feng, L. L. Lai, and M. Shahidehpour, "Reliability modeling and assessment of cyber space in cyber-physical power systems," IEEE Trans. Smart Grid, vol. 11, pp. 3763–3773, 2020. doi: 10.1109/TSG.2020.2982566.

[3] Y. Li, C. Wang, G. Li, J. Wang, D. Zhao, and C. Chen, "Improving operational flexibility of integrated energy system with uncertain renewable generations considering thermal inertia of buildings," Energ. Convers. Management, vol. 207, p. 112526, 2020. doi: 10.1016/j.enconman.2020.112526.

[4] U. Adhikari, T. H. Morris, and S. Pan, "Applying hoeffding adaptive trees for real-time cyber-power event and intrusion classification," IEEE Trans. Smart Grid, vol. 9, no. 5, pp. 4049–4060, 2017. doi: 10.1109/TSG.2017.2647778.

[5] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," IEEE Trans. Smart Grid, vol. 8, no. 4, pp. 1630–1638, 2016. doi: 10.1109/TSG.2015.2495133.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 1–33, 2011. doi: 10.1145/1952982.1952995.

[7] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," IEEE Trans. Ind. Inf., vol. 11, no. 3, pp. 650–662, 2015. doi: 10.1109/tii.2015.2420951.

[8] L. Gao, B. Chen, and L. Yu, "Fusion-based FDI attack detection in cyber-physical systems," IEEE Trans. Circuits Syst. II: Express Briefs, vol. 67, no. 8, pp. 1487–1491, 2019. doi: 10.1109/TCSII.2019.2939276.

[9] A. Ayad, H. E. Farag, A. Youssef, and E. F. El-Saadany, "Detection of false data injection attacks in smart grids using recurrent neural networks," in Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2018, pp. 1–5.
[10] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in Proceedings of the International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 2016, pp. 1395–1402.
[11] M. Ozay, I. Esnaola, F. T. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," IEEE Trans. Neural Netw. Learn. Syst., vol. 27, pp. 1773–1786, 2015.
[12] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," IET Cyber-Phys. Syst. Theory Appl., vol. 2, pp. 161–171, 2017.
[13] C. Yang, Y. Wang, Y. Zhou, J. Ruan, and W. Liu, "False data injection attacks detection in power system using machine learning method," J. Comput. Commun., vol. 6, p. 276, 2018.
[14] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning," Comput. Secur., vol. 97, p. 101994, 2020.
[15] Y. A. Farrukh, I. Khan, Z. Ahmad, and R. M. Elavarasan, "A sequential supervised machine learning approach for cyber attack detection in a smart grid system," arXiv preprint arXiv:2108.00476, 2021.
[16] M. R. Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," IEEE Access, vol. 8, pp. 19921–19933, 2020.
[17] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in Proceedings of the IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 108–112.
[18] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework," IEEE Access, vol. 7, pp. 31762–31773, 2019.
[19] M. M. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial IoT," IEEE Internet Things J., vol. 7, pp. 8462–8471, 2020.
[20] C. Wang, S. Tindemans, K. Pan, and P. Palensky, "Detection of false data injection attacks using the autoencoder approach," in Proceedings of the International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Liège, Belgium, 2020, pp. 1–6.
[21] A. Kundu, A. Sahu, E. Serpedin, and K. Davis, "A3d: Attention-based auto-encoder anomaly detector for false data injection attacks," Electr. Power Syst. Res., vol. 189, p. 106795, 2020.
[22] J. Chen, M. A. Mohamed, U. Dampage, M. Rezaei, S. H. Salmen, S. A. Obaid, and A. Annuk, "A Multi-Layer Security Scheme for Mitigating Smart Grid Vulnerability against Faults and Cyber-Attacks," Appl. Sci., vol. 11, p. 9972, 2021.
[23] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2019, pp. 1–6.
[24] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," IEEE Trans. Control Netw., vol. 1, pp. 370–379, 2014.
[25] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," IEEE Trans. Syst. Man Cybern. Syst., 2019.

.