Identification of False Stealthy Data Injection Attacks in Smart Meters using Machine Learning and Blockchain

Saurabh Shukla[1[0000-0002-3335-373X]], Subhasis Thakur[1[0000-0001-6579-724X]], Shahid Hussain[1[0000-0001-6147-403X]], John G. Breslin[1[0000-0001-5790-050X]], Syed Muslim Jameel [0000-0001-7179-8206]

[1]National University of Ireland Galway, Galway, Ireland
{saurabh.shukla, subhasis.thakur, shahid.hussain, john.breslin, muslimjameel.syed}@nuigalway.ie

Abstract

The current challenging issue in the Advanced Metering Infrastructure (AMI) of the Smart Grid (SG) network is how to classify and identify smart meters under the effect of falsification attacks related to stealthy data, which are injected in such small numbers or percentages that it becomes hard to identify. The problem becomes challenging due to sudden variation in the pattern for the power consumption of electrical data, the existing approaches and techniques are making such stealthy data attacks unrecognizable. Therefore, to identify such a small portion of data attacks we proposed a novel solution using a combination of blockchain, Fog Computing (FC), and linear Support Vector Machine (SVM) with Principal Component Analysis (PCA). In this paper, we proposed a 3-tier blockchain-based architecture, an advanced system model and a classification algorithm in a blockchain-based FC environment. The blockchain system is used here to verify the electrical data transmission and transaction between the user and the utility centre. Whereas FC is used to provide real-time alert messages in case of any false attacks related to stealthy data. A detailed analysis of the generated results is conducted by benchmarking with the other state-of-the-art techniques. The algorithm and model show a marked improvement over other technologies and techniques. The simulation of the algorithm was conducted using iFogSim, Ganache, Truffle for compiling, Python editor tool, and ATOM IDE.

Keywords: Smart grid, Fog computing, Blockchain, Linear SVM, PCA, Security, Privacy, Cyber-physical system, False data attack, Cyber-attack, machine learning.

1. Introduction

The Advanced Metering Infrastructure (AMI) in a Smart Grid (SG) network consists of multiple smart meters (IoT devices) that communicate and collect the energy data in a two-way or bi-directional form from customers to utility [1]. Architectural communication is used by smart meters for the transmission of energy data in a periodic manner, to various data management servers limited to the utility centres [2]. The involved servers processed the energy data received from smart meters for critical operations

such as billing, load balancing, daily monitoring of threshold peaks, shift demand, and demand response. This integrity of the energy or electrical data from devices like smart meters plays a major role in the success of SG.

See Fig.1. for the AMI network.

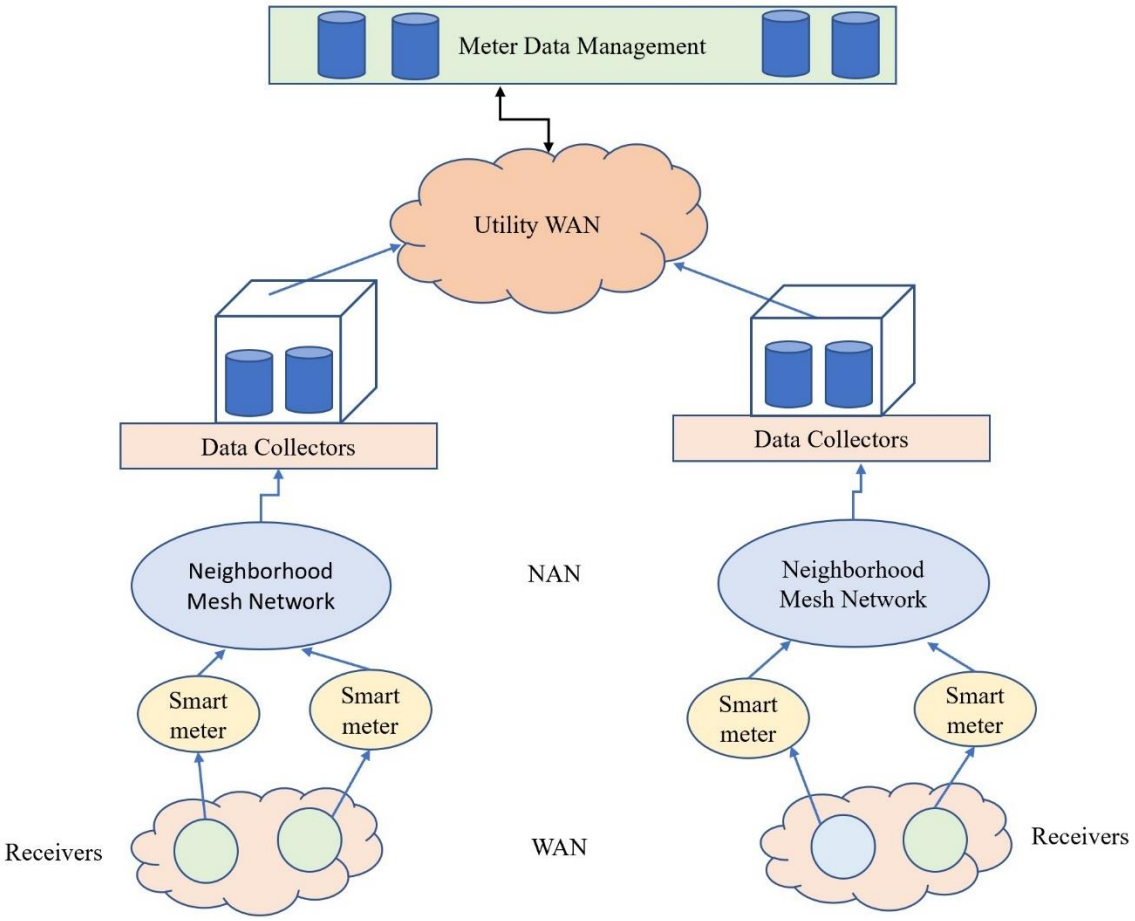

Fig.1. Advanced metering infrastructure network architecture

Fig.1. shows the AMI network architecture which consists of receivers connected to smart meters. The smart meters sent the electrical data readings to data collectors through the neighbourhood mesh network. Then, at last, they sent the data to meter data management. The data is collected, transmitted, and finally distributed from Wide Area Network (WAN), Neighborhood Area Network (NAN), and to utility WAN.

However, cyber, or physical attacks on smart meters are increasing every day as the smart meters relate to the cyber-physical world or with web-based portals through which they are connected to the smart home network at the customer site [3]. This type of cyber-physical attack consists of many smart meter devices connected to similar feeding data and then generates spoof false energy data readings. The false stealthy data injection leads to huge monetary losses to the consumers of smart cities.

1.1 Motivation and Challenges

Identification and authentication of smart meters which are involved/engaged in the transmission or usage of stealthy false electrical data consumption are key security and privacy challenges. The quantifiable parametric value which distinguishes the false stealthy data from the original clean electrical data is known as the mean average value of false attack strength [4]. The lower marginal value of attack value/ strength is stealthy and hence it becomes difficult to detect/identify them to quantify the parametric value of such attacks comprising a large set of smart meters is in the SG network is known as the "Scale of False Attack" [5]. Such minimal or lower kinds of stealthy attacks have a great significant impact on the utility bills/consumption readings when compromised to total cyberattacks cost. These attacks compromise with the smart meters QoS services. Such attacks are usually conducted by cybercriminals and organizational competitors to lower the marginal value of false data per smart meter by making hide them behind the random data generated from smart meter devices. This makes these smart meters hard to catch.

In the future, rival nations or organizations can use this approach of injecting false stealthy data attacks in the smart grid network. Since the smart meter involves the generation, transmission, distribution, and consumption of critical/important electrical energy data. Therefore, providing an enhanced classification technique to identify smart meters which are involved in the transmission of stealthy false data is of utmost importance. This classification approach uses a hybrid of Supervised and Unsupervised learning algorithms i.e., Support Vector Machine (SVM) and 2-Principal Component Analysis (PCA) using blockchain technology for verification of transactions and use of fog computing (FC) to alert the end-users for real-time intruder's attack. Our anomalies identification approach distinguishes itself from existing approaches. Lately, the method has to generalize across various such false attacks.

1.2 Contribution

In this paper, we propose a novel anomaly detection model, for false stealthy data injection, consumption, and transmission in smart meters. The model will be able to identify and detect a wide range of cyber-attack from very low to a high margin of attack strength and its scales. The model will be using FC for alarm notification and detection of false alarms, missed alarms, compared to the other state-of-the-art techniques. To accomplish this, the contributions of this paper are as follows:

1) We proposed a novel 3-tier blockchain-based machine learning architecture for false stealthy data identification in smart meters.

2) Next, we proposed and designed a novel and hybrid system model using blockchain and machine learning techniques in the FC environment.

3) At last, we designed and implement a hybrid blockchain-based machine learning algorithm for the identification of false stealthy data injection attacks on smart meters.

The proposed approach establishes a machine learning-based intelligent system for monitoring data falsification attacks. Moreover, the model was developed and generalized to successfully identify, deduct, and detect the various alternating switching attacks of multiple strength and strategies that were not used in the previous works. A comparison with the current existing woks exhibits improved performance in terms of percentage value of false stealthy attack and their strength level.

The paper is organized as follows: section 2 discussed the related work. Section 3. Presents the 3-tier architecture. Whereas section 4 presents the system model. Sec.5 presents the hybrid algorithm. Sec.6. discussed the experimental results and evaluation. And at last, sec.7. concludes the work.

2. Related Work

In this section, a complete detailed analysis of the current existing works related to false data attacks on smart metres and smart grids is conducted. We have tried to identify the research gaps mainly in the injection, transmission, and distribution of false stealthy data in smart metres. A comparison is drawn between the latest technology and techniques used by different authors and researchers in their proposed work.

Some of the techniques are highlighted as in [6], the authors proposed a Scoring Framework (SF) for identifying stealthy false data attacks on smart meters. They highlighted the issue of low margin false data injection in smart meters and smart grid networks. Their proposed method is based on a classification approach to identify the low strength of false data. Furthermore, they used the scoring technique with indexed-based solutions.

In [7], the authors designed a Zero parameter-information Data Injection Attack (DIA) class technique called ZDIA. They highlighted the problem of stealthy data attacks for tampering with the smart meter data without being noticed by the consumers. Through this, the attacker can extract the topology and branch information of the system parameter. They can easily predict the system states for various cyber-attacks. Next, they proposed countermeasures to address the vulnerability of various attacks conducted by cyber-criminals on smart grid networks using ZDIA. Furthermore, they presented a strategy and defined techniques against such DIA's.

In [8], the authors proposed a machine learning algorithm for the identification of False Data

Injection Attack (FDIA) in power systems susceptible to smart meters and SG networks. They discussed the various types of cyberattacks on grid infrastructure. They used the approach of feature selection to build a detection system for FDIA. Each experiment was evaluated about time complexity as the response time is a critical factor in an SG network when attacked by false data.

In [9], the authors proposed a machine learning scheme using Kalman filter and neural network to identify the FDIA on SG Network System. They applied a two-level learning mechanism where in the first level a Kalman filter was used for state prediction and a recurrent neural network was used to extract the data feature. In the second level, a backpropagation method was adapted to combine the result for two learners. Furthermore, they estimated the sum of square error between the observed value and the predicted value.

In [10], the authors discussed the issue of the stealthy cyber intrusion attack in SG. They proposed an advanced system model for using state estimation for the detection of cyber-attacks which compromises the security in meters. The model was able to nullify the effect of bad data using a detection algorithm. In [11], the authors proposed a real-time based, 2 -Tier Attack Identification (2-TAI) scheme to detect false stealthy data in smart meter infrastructure. In the first tier, the use of harmonics to the arithmetic mean ratio of total power consumption of electrical data is conducted to check whether it is under safe margin or not. Whereas, in the second-tier detection scheme the monitoring of the sum of the residuals i.e., the difference between the proposed metric ratio and the safe margin is conducted over a longer period and days. If the sum of residuals exceeds the average margin range, then the presence of a data falsification attack is confirmed. They further used the technique of the system identification phase for safe margins and standards limits. A real-time AMI microgrid data set is used collected from two different centres.

In [12], the authors proposed the measurement of a stability index to access reliability against stealthy false data attacks in SG networks. The FDIA degrades the value of the stability index which causes incorrect measurement of electric power readings and poorly load balancing. This further leads to a large communication delay that causes poor synchronization. The authors used a dynamic stable estimation technique to obtain the data from different states after the injection of a false data attack. Next, they analyzed its impacts on the stability index of the smart grid.

In [13], the authors proposed a new technique based on the Dimensionality Reduction Method (DRM) for the identification of FDIA in the smart grid. Their proposed method consists of two phases: a dimensionality reduction phase-1 and Gaussian-based semi-supervised learning phase -2 to minimize the error and to increase the distinction between the normal value of data and the bad data value. This generates a reduced dimension based on a new orthogonal. At last, the threshold value is checked using the Gaussian mixture model to identify the FDIA.

In [14], the authors proposed a Graph Neural Network (GNN) approach to detect and identify the presence of FDIA. They applied Graph filters using Auto Regressive Moving Average (ARMA). This technique automatically detects the localize FDIA in the SG network. They exploited the inherent

graph topology of the SG network with spatial correlations of measurement data. In [5], the authors used a deep-learning technique for the identification of FDIA in the SG network., They exploited the technique of the agent-based model. The research focuses on the decentralization of data integrity. The authors were able to achieve true data integrity against the stealthy cyber-attack in the SG network.

Most of the existing state-of-the-art techniques such as SF, ZDIA, 2-TAI, DRM, and ARMA are still in infancy and are unable to provide a secure communication channel for data transmission and distribution. The existing algorithms and techniques were unable to minimize the False Stealthy Data Injection Attack (FSDIA) percentage. Hence a novel solution is proposed to minimize and identify the FSDIA in smart meters and SG networks.

3. Blockchain-based 3-Tier Architecture

In this section, we discussed the proposed blockchain-based 3-tier architecture in the FC environment. The architecture was designed to minimize and detect the FSDIA percentage for electrical data transmission, distribution and consumption using smart meters in an SG network system. See Fig.2 for the architecture design.

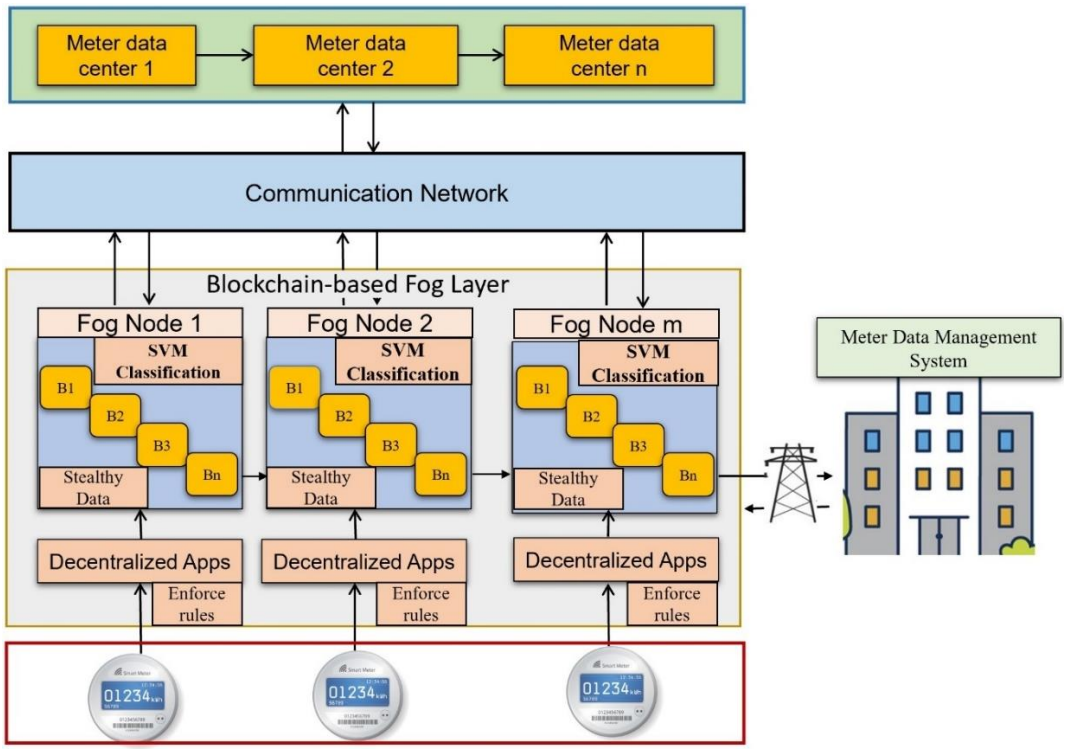

Fig.2. 3-Tier architecture

Fig.2 illustrates the blockchain-based 3-tier architecture for the identification of false stealthy injection in smart meters. The proposed architecture utilizes the concept of machine learning technique called Linear SVM and 2-PCA classification for separating the outliers from the electrical

data and readings collected from smart meters. Fog nodes are used here for running the machine learning algorithm inside the different processes and to send real-time notifications for any kind of attacks to end-users or meter management systems [15]. Whereas blockchain is used here to record and secure the various electrical data transactions in different chains of blocks called ledgers [16]. The architecture consists of smart meters, data connectors, Meter Data Management System, (MDMS), and fog nodes. The electrical data is sent to meter data centres using a communication network.

4. Conventional and Advanced System Model

In this section, we discussed the difference between the conventional system model and the proposed advanced system model for FSDIA in smart meters and SG networks. Furthermore, we discussed the advanced system for secure electrical data transmission communication in an SG network which enables the identification and detection of false stealthy data.

See Fig.1 for the conventional system model.

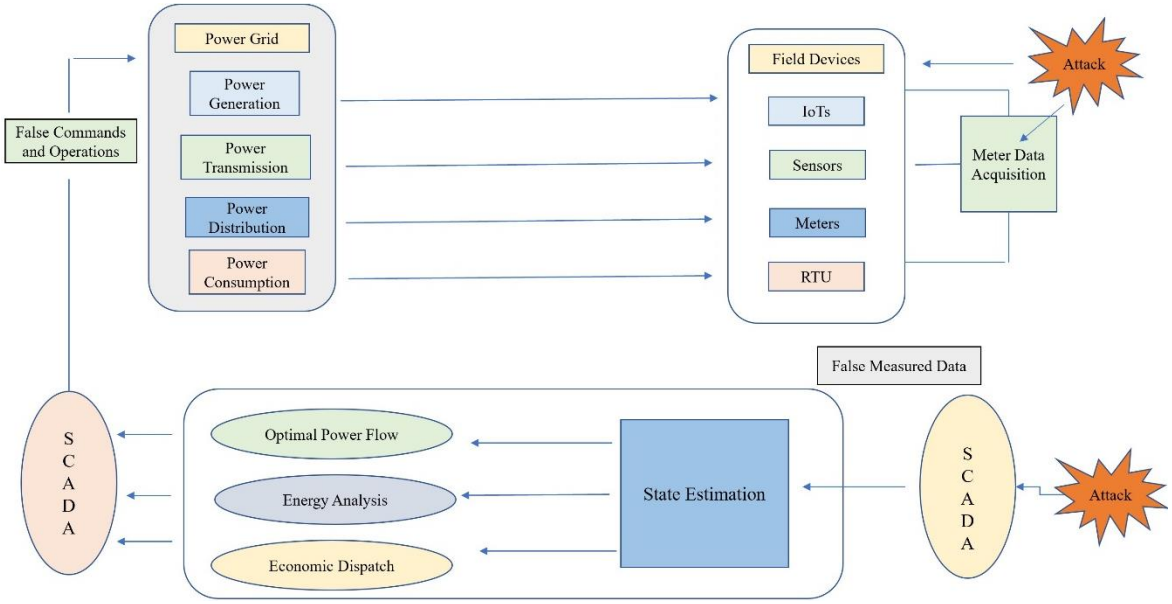

Fig.3. Conventional model

Fig.3 shows the basic traditional SG system model for electric data transmission. The model consists of smart meters, IoT devices, sensors, Remote Terminal Units (RTU) and a meter data acquisition system. The conventional model is prone to cyber-attacks when false measured data is injected through Supervisory control and data acquisition (SCADA), and it disturbs the state estimation of the SG network system. The false data is then transmitted to power grids through optimal power flow. This disturbs the energy analysis and economic dispatch. The false commands and operations are then sent

to the power grid system for power generation, transmission, distribution, and consumption. The conventional system model lacks advanced security features such as blockchain techniques. The conventional model is an open network for outside intruders and CPS attackers to manipulate the smart meter readings and insert false data during electric data transmission[17]. The model lacks the real-time decision-making capability to identify and detect the FSDIA.

See Fig.4 shows the novel system model for SG network communication, identification of false data, and classification of false stealthy injected data using fog nodes and blockchain.

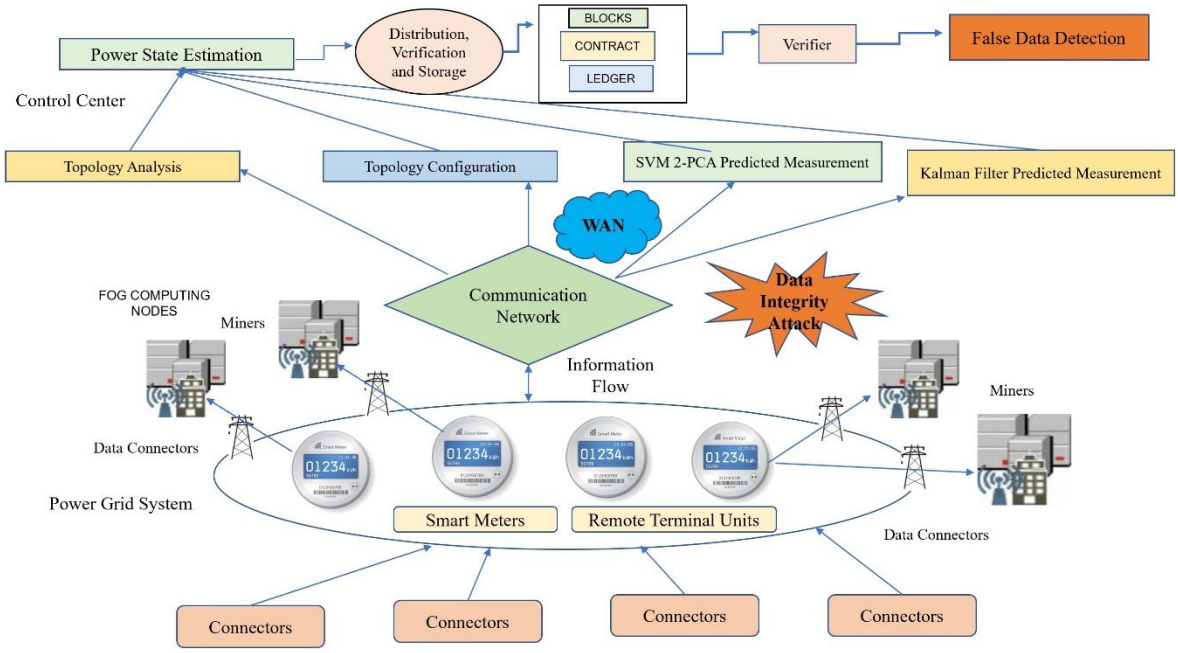

Fig.4. Advanced system model

The classification of electrical data and variables is conducted using a supervised machine learning approach. Linear SVM and 2-PCA techniques are used for reducing the number of parametric values and severity levels involved in the data generation, transmission, distribution, and consumption. and can easily classify by distinguishing the outliers and similar patterns. The FC nodes are used here as miners to process and mined the electrical data in a blockchain environment. The FC approach is employed in the SG to bring all the advanced features of the cloud. Fog nodes are responsible for secure communication between smart meter devices

Fig. 4 shows the advanced system model for false stealthy data identification in the SG network. The model consists of connectors, smart meters, RTU's, data connectors, and FC nodes. The novel Blockchain-based False Stealthy Data Identification Algorithm (BFSDIA) algorithm works in coordination with fog nodes where the classification of false data is conducted inside the fog nodes. The electrical data is classified using L-SVM which generated the predicted measured value which is then updated using Kalman filter and these updated values are sent for state estimation where the

electrical data transaction are verified using blockchain nodes. This technique detects the different kinds of failures and false data injection attacks related to electrical data transmission in smart meters deployed at the edge of the SG network system.

5. Blockchain-based False Stealthy Data Identification Algorithm (BFSDIA)

In this section, we discussed the proposed advanced hybrid BFSDI algorithm. The algorithm works to identify and detect the false stealthy data injected in an SG network during electrical data transmission. The novel algorithm utilizes the technique of machine learning algorithms called L-SVM and 2-PCA. This technique is used to classify the data along a hyper-plane to identify the outliers and false data. The data classified to the highest varied 2-PCA values using the ML algorithm to display not-under-risk and under-risk electrical data depending upon the false stealthy injected data presence. It involves no outsiders as the data is processed in the FC servers using blockchain techniques of distribution, storage, and verification conducted using previous and current hash codes of different distributed chains of blocks called ledgers. Furthermore, this section includes algorithm symbol notations, algorithm steps, and pseud-code.

BFSDI Algorithm Symbol Notations:

S_e: State estimation

FC_N: Fog computing nodes

C_s : Current sample

V: Voltage

P_l: Parametric level

S_l: Security level

S_m: Smart meter

E_{dt}: Electrical data

F_d: False data

L_{SVM}: Linear Support Vector Machine

w_v: Weight vector

D_t: Distance

D_b: Decision boundary

Mg_{w_d} : Marginal width

Ce_{DS}: The list of classified electrical data

A_l: electrical data packets having anomalies

C_V: Cross-validation

V_M: Variable minimization

2-PCA: 2-Principal Component Analysis

R_d: Reduced dimension

O_m : Original measurement

T_v: Threshold value

N_m: New measurement

C_t: Coordinate transform

$FSDA$: False Stealthy Data Attack

P_v : Parametric value

O_L : Outliers

Rx: Communication channel

Tx: Communication channel

D_V : Data verification

B_C: Blockchain

BFSDI Algorithm Steps:

Step 1: Creation of an FC system.

Step 2: Collection of different state estimations.

Step 3: Reading the values of voltages and current samples.

Step 4: Checking of parameter and security levels.

Step 5: Selection of targeted smart meters**.**

Step 6: Injection of electrical data in smart meters.

Step 7: Identification of false data using Linear SVM.

Step 8: Classification of electrical data using Linear SVM.

Step 9: Next, training of the machine learning model.

Step 10: Perform variable minimization using PCA.

Step 11: Conduct cross-validation**.**

Step 12: Dimension reduction and removal of identified outliers.

Step 13: Obtain the parametric level and threshold value**.**

Step 14: Data verification using blockchain.

Step 15: Identify the False stealth data attack on smart meters.

Step 16: To check the different types of failures from the attack on the states of smart meters.

Step 17: Apply the Kalman filter for the updated value both for predicted values and measured values.

Step 18: Notify the users and meter management system.

BFSDI Algorithm:

Input: Smart meter state estimation, smart meter data, electrical readings, measured values, and injected electrical data.

Output: Notification of stable threshold marginal value for false stealthy data.

Init: Perform initialization tasks, such as the reading of electrical data, network filters and IP addresses.

1: ***START***

2: *(FC-based blockchain system is created)*

3: ***While*** *collect* S_e *in* FC_N ***do***

4: *Read* V *and* C_s

5: *Check* P_l *and* S_l ***end***

6: *Select* S_m *using* S_e

7: E_{dt} *injection in* S_m

8: F_d *identification using* L_{SVM}

9: E_{dt} *classification using* L_{SVM}

10: ***While*** $(iter \leq \text{maximum iteration})$ ***do***

11: ***Function*** *Def Distance* $(self, w_d, with\_lagrange = True)$:

12: $D_t = self.y * (np.dot(self.X, w_v)) - 1$

13: get D_t from D_b from the current D_b

14: ***if*** Mg_{w_d} == 1

15: get D_t from D_b

16: generate Ce_{DS} and A_l

17: ***else if*** Mg_{w_d} **== 0**

18: then D_t not retrieve

19: ***end if***

20: ***end if***

21: ***end Function***

22: ***Function*** *Train (Model)*

23: *do* C_V

24: V_M *using 2-PCA*

25: *Construct* R_d

26: *get* R_d *and* O_m *of* S_m *data*

27: *Obtain* T_v *from* L_{SVM}

28: ***end Function***

29: ***For*** N_m

30: *do perform* C_t

31: *Compute* P_v

32: D_V *using* B_C

33: ***end For***

34: ***if*** $P_l >= T_v$

35: Possible $FSDA$

36: ***else*** *No* $FSDA$ *detection*

37: ***end if***

38: LS_e *in* FC_N *using* H_C *of* P_B *and* C_B

39: ***if*** *FSDA == Minor Failure || Moderate Failure || Severe Failure || Catastrophic*

40: *then do check* S_m *states*

41: *Remove identified* O_L *and* V_B *identified using SVM*

42: *else*

43: *System == stable state*

44: ***end if***

45: 46: ***Function*** *KALMAN_STATE result*

46: *KALMAN_update*（）

47: *Update Predict and Measure values*

48: *do notification using Rx/Tx*

49: ***end Function***

50: ***End***

6. Results and Discussion

This section discusses the performance evaluation along with simulation overview and settings for the proposed model and algorithm for generated results. In this section, the execution of the proposed Blockchain-based False Stealthy Data Identification Algorithm (BFSDIA) is analyzed. Next, to verify the proposed algorithm and system model a benchmarking of the existing techniques was conducted. This further helps in examining the robustness of the performance measures.

The simulation of the BFSDI algorithm is conducted in the iFogSim Simulator. The algorithm usage the Linear SVM and 2-PCA techniques for the classification of false stealthy electrical data by minimizing the number of variables across a hyperplane.

The missing values and outliers are removed and filled with a mean data value. These missing values are removed using a Kalman filter. To demonstrate the highest variation the 2-PCA values are used in the identified false stealthy electrical data. The algorithm is implemented using NetBeans and python with several main packages. The baseline for this simulation is the maximum false stealthy data detection accuracy percentage.

See Fig. 5. for the topology configuration of deployed smart meter devices and fog nodes in the proposed system model using the iFogSim simulator.

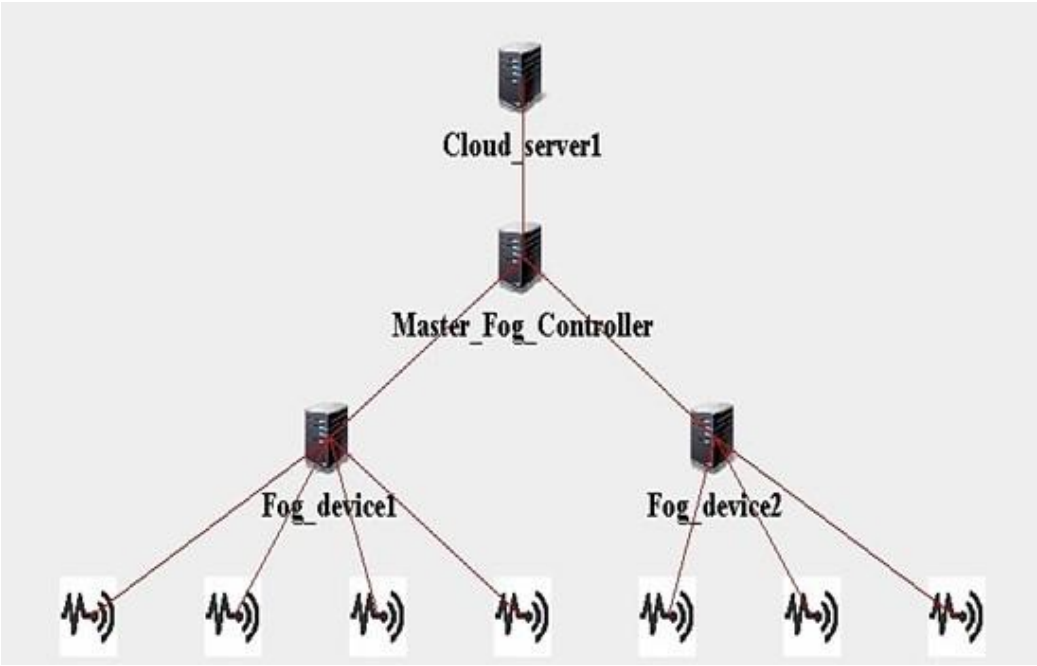

Fig.5. Graphical user interface configuration

Fig.5. shows the graphical physical topology configurations built-in in the iFogSim simulator. The configuration in Fig.5 is fully based on the concept of a proposed system model and BFSDI algorithm. The configuration consists of distributed smart meter devices placed at the edge of networks along with fog nodes that are further connected to cloud data centres. Whereas Fig.6 shows the classified false stealthy injected electrical data using the hybrid machine learning approach called linear SVM and 2-PCA.

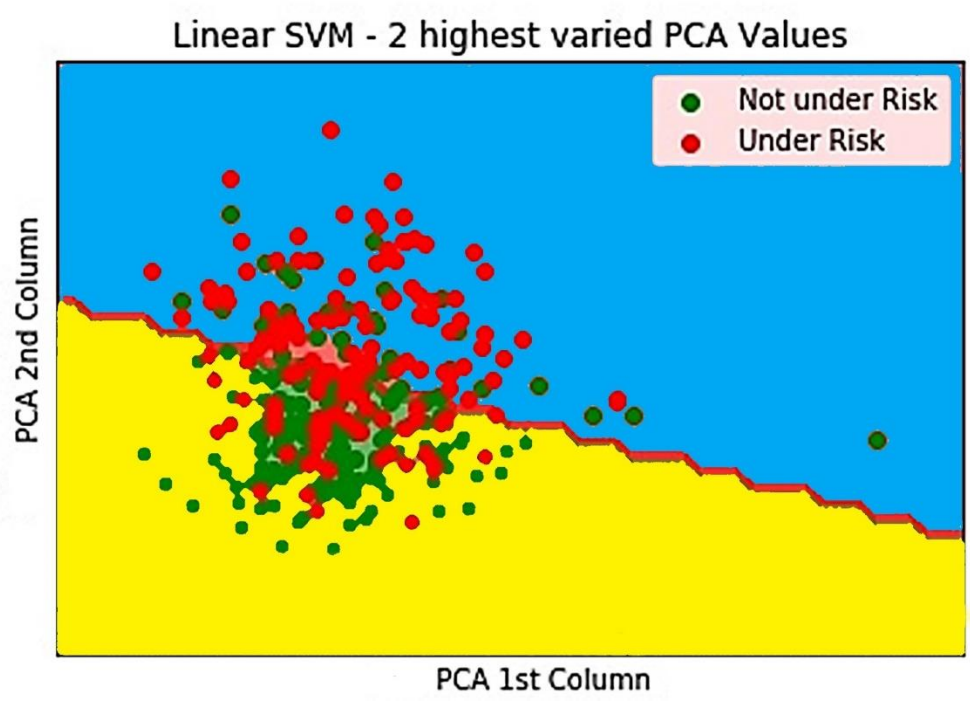

Fig.6. Classification for false stealthy electrical data using L-SVM and PCA

Fig. 6 shows the not-under-risk electrical data which is classified as false stealthy free data shown by green colour dots and under-risk false stealthy electrical data shown by red colour dots. The X-axis shows the electrical data PCA 1st column, and the Y-axis shows the electrical PCA 2nd column.

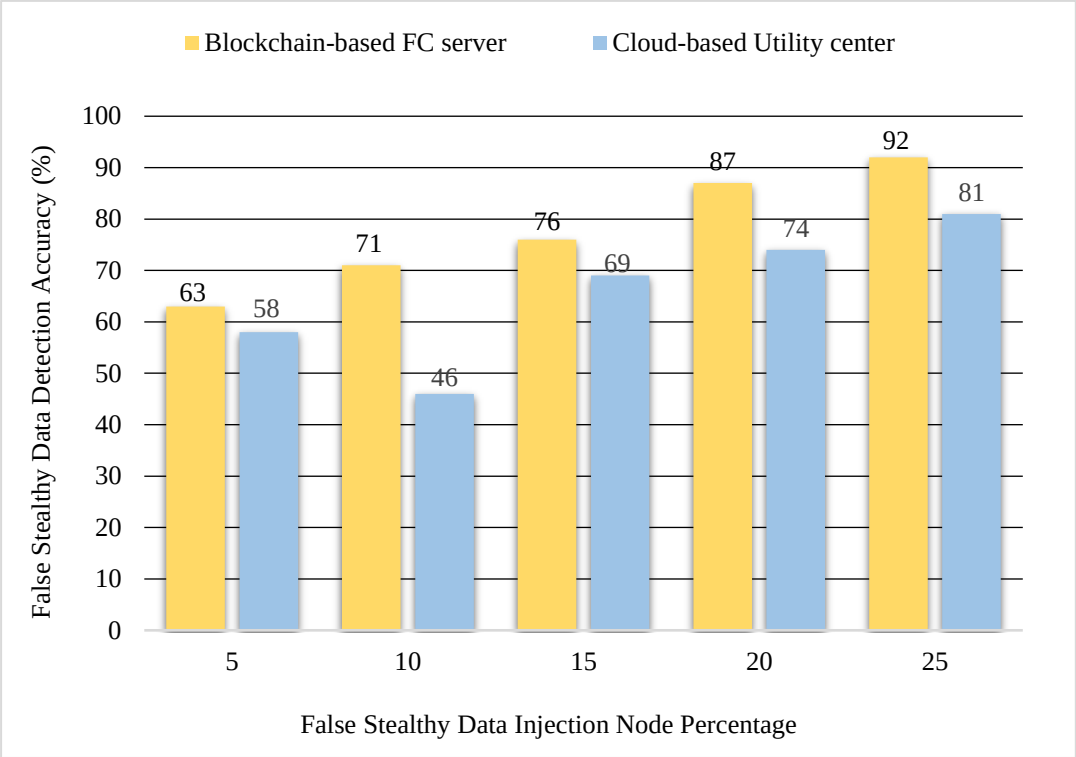

Fig.7. False stealthy data detection accuracy vs node with false stealthy data injection percentage

Fig. 7 shows the percentage of a node with false stealthy data injection in blockchain-based FC server and cloud-based utility centre along with the false stealthy data detection accuracy. The minimum false stealthy data detection accuracy of the BFSDI algorithm in FC-based servers and cloud-based utility centres is 63% and 58%. Whereas the maximum detection accuracy of the BFSDI algorithm in fog servers and cloud environments is 92% and 81%.

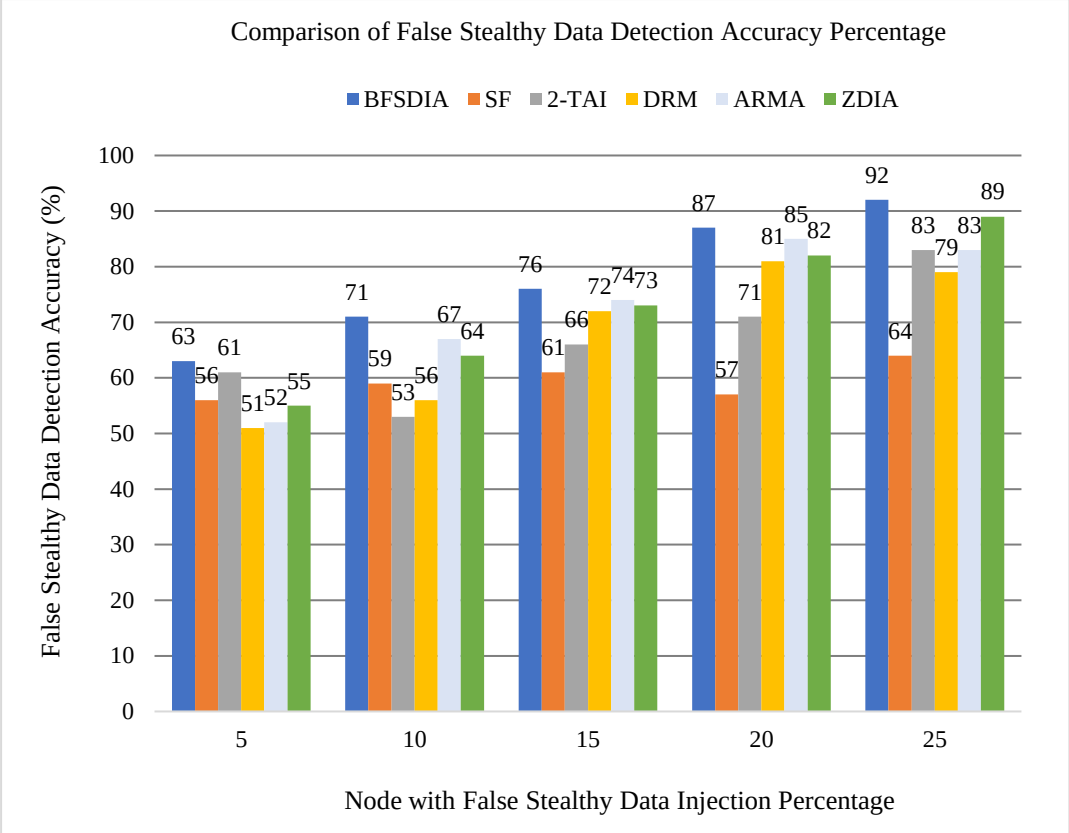

Fig.8. Anomaly detection accuracy vs node with anomaly percentage performance evaluation

Fig. 8 shows the comparison of a node with false stealthy data percentage vs false data detection accuracy of the proposed BFSDI algorithm with the other existing techniques. The minimum false data detection accuracy is 51% for DRM. Whereas the minimum false data detection accuracy for the BFSDI algorithm is 63%. However, the maximum false data detection accuracy is 89% for ZDIA. Whereas the maximum false data detection accuracy for the BFSDI algorithm is 92%.

7. Conclusion

The advancement in Industry 4.0 has evolved the role of AMI for smart cities and societies in an SG network. This SG network consists of multiple smart meter devices. The smart meter devices are the perfect examples of Internet-of-Things (IoT) that communicate the energy information flow in a bi-directional form from end-users to utility centres. Since the smart meter is a cyber-physical system. Therefore, it is prone to various kinds of cyber-attacks from outside attackers or intruders. Sometimes a similar feeding of data is transmitted to smart meters that generate spoof false energy data readings. This leads to huge monetary losses to the customers. This false stealthy data is transmitted in such minimal or low forms that they are hard to distinguish from the main electrical data. The injection of, malicious data insertion, and false stealthy data inside the smart meter devices have generated a large risk to the SG network.

Hence to overcome this issue we have proposed a 3 -tier blockchain-based architecture, an advanced system model in FC environment, and a novel hybrid machine learning algorithm that utilizes the concept and technique of both blockchain and FC. The algorithm uses the L-SVM and 2-PCA machine learning techniques for the classification and identification of FSDIA on smart meter devices. When compared for performance analyses and an evaluation with the existing technologies such as SF, ZDIA, 2-TAI, DRM, and ARMA the proposed algorithm easily outperforms them in terms of false stealthy data detection accuracy. The proposed model and algorithm successfully address the problem of FSDIA identification and detection in different distributed smart meters of an SG network system.

Acknowledgement

This publication has emanated from research supported in part by a research grant from Cooperative Energy Trading System (CENTS) under Grant Number REI1633, and by a research grant from Science Foundation Ireland (SFI) under Grant Number SFI 12/RC/2289_P2 (Insight), co-funded by the European Regional Development Fund.

References

1. Wu, K., et al., *A lightweight SM2-based security authentication scheme for smart grids.* Alexandria Engineering Journal, 2021. **60**(1): p. 435-446.
2. Zou, T., et al., *Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks.* Electric Power Systems Research, 2020. **187**: p. 106490.
3. Lohachab, A., et al., *Performance evaluation of Hyperledger Fabric-enabled framework for pervasive peer-to-peer energy trading in smart Cyber–Physical Systems.* Future Generation Computer Systems, 2021. **118**: p. 392-416.
4. Zhang, M., et al., *False data injection attacks against smart gird state estimation: Construction, detection and defense.* Science China Technological Sciences, 2019: p. 1-11.
5. Sengan, S., et al., *Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning.* Computers & Electrical Engineering, 2021. **93**: p. 107211.
6. Bhattacharjee, S., P. Madhavarapu, and S.K. Das. *A Diversity Index based Scoring Framework for Identifying Smart Meters Launching Stealthy Data Falsification Attacks*. in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*. 2021.
7. Zhang, Z., et al., *Zero-Parameter-Information Data Integrity Attacks and Countermeasures in IoT-Based Smart Grid.* IEEE Internet of Things Journal, 2021. **8**(8): p. 6608-6623.
8. Kumar, A., N. Saxena, and B.J. Choi. *Machine Learning Algorithm for Detection of False Data Injection Attack in Power System*. in *2021 International Conference on Information Networking (ICOIN)*. 2021. IEEE.
9. Wang, Y., et al., *KFRNN: An Effective False Data Injection Attack Detection in Smart Grid Based on Kalman Filter and Recurrent Neural Network.* IEEE Internet of Things Journal, 2021.
10. Khazaei, J. and A. Asrari, *Second-Order Cone Programming Relaxation of Stealthy Cyberattacks Resulting in Overvoltages in Cyber-Physical Power Systems.* IEEE Systems Journal, 2021.
11. Bhattacharjee, S. and S.K. Das, *Detection and forensics against stealthy data falsification in smart metering infrastructure.* IEEE Transactions on Dependable and Secure Computing, 2018.

12. Rashed, M., et al. *Assessing Reliability of Smart Grid Against Cyberattacks using Stability Index*. in *2021 31st Australasian Universities Power Engineering Conference (AUPEC)*. 2021. IEEE.
13. Shi, H., L. Xie, and L. Peng, *Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method.* Computers & Electrical Engineering, 2021. **91**: p. 107058.
14. Boyaci, O., et al., *Joint Detection and Localization of Stealth False Data Injection Attacks in Smart Grids using Graph Neural Networks.* arXiv preprint arXiv:2104.11846, 2021.
15. Shukla, S., et al. *A Blockchain-Enabled Fog Computing Model for Peer-To-Peer Energy Trading in Smart Grid*. in *International Congress on Blockchain and Applications*. 2021. Springer.
16. Shukla, S., et al., *Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model.* Internet of Things, 2021. **15**: p. 100422.
17. Shukla, S., S. Thakur, and J.G. Breslin. *Secure Communication in Smart Meters using Elliptic Curve Cryptography and Digital Signature Algorithm*. in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2021. IEEE.