Anomaly Detection in Smart Grid Network Using FC-Based Blockchain Model and Linear SVM

Saurabh Shukla(✉), Subhasis Thakur, and John G. Breslin

National University of Ireland Galway, Galway, Ireland
{saurabh.shukla,subhasis.thakur,john.breslin}@nuigalway.ie

Abstract. Traditional grid network has played a major role in society by distributing and transmitting electric supply to consumers. However, with the advancement in technology in Industry 4.0 has evolved the role of the Smart Grid (SG) network. SG network is a two-way bi-directional communication Cyber-Physical System (CPS). Whereas traditional grid network is a one-way directional physical system. SG is a part of the most revolutionary application of Internet-of-Things (IoT). The information related to power consumption and supplies can be transmitted and recorded in real-time. The connection of SG with the internet has also created a lot of space for different types of anomalies injection and cyber-physical attacks. SG network is open and vulnerable to an outside hacker. The detection of an anomaly in real-time is of utmost importance otherwise it may lead to huge power loss, security, and monetary loss to the consumer, producer, and smart city society. In this paper, we have proposed a private blockchain system model for anomaly detection in SG along with a novel Linear Support Vector Machine Anomaly Detection (LSVMAD) algorithm in a fog computing (FC) environment. Here FC nodes will act as miners to support and make real-time decisions for anomaly detection in an SG network. The anomaly detection accuracy of the LSVMAD algorithm in the FC environment is 89% and in the cloud is 78%. The proposed LSVMAD algorithm easily outperforms the existing techniques and algorithms when compared for anomaly detection accuracy percentage. The simulation tool used in the implementation of works is iFogSim, Anaconda (Python), Geth version 1.9.25, Ganache, Truffle (Compile) and ATOM as a text editor for creating smart contracts.

Keywords: Smart grid · Fog computing · Linear SVM · Internet-of-Things · Smart meter · Cyber-physical system · Machine learning

1 Introduction

Smart Grid (SG) network majorly works on the three components; i.e. physical system, distributed computation, and the communication system [1]. This makes the SG network a complete system for power generation, distribution, transmission, and consumption. SG network is connected with data connectors and smart meters with Home Area Network (HAN), Building Area Network (BAN), and Neighbor Area Network (NAN). SG has

G. Nicosia et al. (Eds.): LOD 2021, LNCS 13163, pp. 157–171, 2022.
https://doi.org/10.1007/978-3-030-95467-3_13

played a major role in smart cities where they were able to provide bi-directional real-time information [2]. The main characteristic of the SG network is to make a clear balance between the generation of power and its consumption over the channel or network. However, the SG network has some major challenges when it comes to avoiding cyber-physical attacks and anomaly detection [3].

The main drawback of the SG network is its open communication channel which makes it's vulnerable for outside attackers to manipulate the electric data consumption, along with an addition of erroneous value in sensor readings, inaccurate electricity bills, and short-circuits in smart meters [4]. All this could be possible by injecting various anomalies during transmission and communication over the SG network [1]. Cyber intruders can further overload and degrade the performance of different sub-station over the SG network. This may lead to continuous consumption of electricity by changing the paraments over the smart meter which is also one of the major neglected issues. The security over the SG network for electric data transmission and consumption is related to three factors or IACC goals; Integrity, Authentication, Availability, and Confidentiality [5]. All these factors are major aspects and concern while working for anomaly detection, classification and avoiding Cyber-Physical System (CPS) attacks.

SG networks work in a distributed open environment; where blockchain can play a major role to secure the electric data from manipulation by outside hackers and attackers [2]. Blockchain operates in a decentralized manner where every transaction is secured using hash functions, encryption techniques, cryptographic operations, and the use of public and private keys. Furthermore, there is a record of every transaction that occurred between various distributed units [6]. On a similar note, fog computing (FC) nodes act as miners close to the edge of SG networks and connect over LAN, BAN, NAN, and WAN [7]. FC is a kind of distributed network where the information is shared between the different nodes at LAN. These FC nodes work at the edge of networks close to the smart grid network and smart meters [8]. The data is processed and filtered for anomalies in FC nodes to make decisions in real-time mode by transmitting the data over a single hop count to consumers and producers. Classification of data and outliers using supervised machine learning techniques such as K-Nearest Neighbors (KNN) and Linear-SVM (Linear-Support Vector Machine) with Principal Component Analysis (PCA) are used to identify the irregular pattern of movement in the data set [9]. These algorithms are used for regression and classification.

In this paper, we have proposed a blockchain-based advanced system model, and a novel Linear Support Vector Machine Anomaly Detection (LSVMAD) algorithm in an FC environment; where FC nodes will act as miners to overcome and identify the different anomalies and malicious data injected by CPS attackers. The proposed system is expected to act promptly to respond to various anomalies occurring in an SG network. Furthermore, the proposed algorithm meets the Quality-of-Service (QoS) requirement for SG network electrical theft and anomaly detection. The main objective of the proposed research work is to detect and classify the anomalies along with malicious data for secure electric data transmission in an SG networks.

2 Background and Related Work

In this section, recent research work has been discussed related to anomaly detection and False Data Injection (FDI) in an SG network. Many of the researchers have highlighted the issue of cyber-physical attacks with the involvement of outside intruders to insert malicious data on the network infrastructure of the SG [10–12]. Some of the works related to the security of communication and computation are mentioned here.

In [5], the authors proposed an advanced novel system model to monitor the anomalies in an SG network promptly. The anomaly detection techniques are facing challenges due to the large transmission of data. Therefore, they further presented a framework to detect electricity consumption anomalies accurately with timely usage of sensor and meter readings. In [13], the authors proposed a framework for anomaly detection. The data is further integrated when collected from smart meters for pattern classification and matching. This classification helps in detecting the values. The system was able to identify and detect one type of anomaly at a time.

In [14], the authors proposed a scheme to detect anomalies in an SG network. They use the unsupervised machine learning technique to identify the irregular pattern in the observed data. The data used for identification was time-series data. The classified data was presented in a hierarchical form. Their proposed approach was based on pattern and cluster-based techniques. Similarly, in [15], the authors proposed a novel approach to identify the anomalies in SG electricity consumption. They used large data sets for training and testing smart meter network data. The proposed scheme has two phases first one is consumption prediction and the second one is anomaly detection. They further used a hybrid Neural Network (NN) approach for the prediction of electricity consumption in a real-time environment. At last, the anomalies are identified by measuring the difference between predicted and real values in consumption.

In [16], the authors proposed a novel approach to cope with external and internal threats. The approach was targeted to detect malicious activities. It was an anomaly detection system to analyze the monitoring data and identify the possible cyber-physical attacks. It was a novel system for ICS/SCADA (Industrial Communication System)/(Supervisory Control and Data Acquisition) protocols to enable real-time monitoring of power consumption and anomaly detection. In [17], the authors conducted a comprehensive survey analysis of the existing cybersecurity solutions for the SG network with the FC approach. They discussed the role of FC placed at the edges of the network of the smart grid network. Furthermore, they discussed various architectures for SG network and fog-based SCADA systems. The authors classified the security requirements into four major categories i.e., authentication, data privacy, preservation, identification, key management, and intrusion detection solutions. Next, they provide a taxonomy of cyber-physical attacks where they highlight the nine categories of Intruders Detection (ID) and their types of attacks.

In [18], the authors discussed the role of the blockchain model for secure communication on an SG network. A complete in-depth analysis was conducted to elaborate on the benefits of blockchain for SG security solutions. Blockchain worked here in a decentralized manner to secure and close various open entry points of an SG network. In [19], the authors developed and presented a Smart Analyzer tool for security analysis in Advanced Metering Infrastructure (AMI). AMI is a core component in the SG network. The authors

mainly focused on the development of the formal model to represent the behaviour of AMI for various types of cyber-attacks. The model works on the device configuration, network topology and interconnected components with LAN, BAN, NAN, and HAN. The system was tested for scalability and reliability on the AMI testbed. The proposed system model and LSVMAD algorithm are designed to detect and identify anomalies along with malicious data for SG networks using blockchain and machine learning (ML) techniques in FC environment. The model further provides a secure communication channel for energy transaction between prosumers and smart meters. Whereas the other state-of-the-art techniques lacks the real-world implementation and development. The existing models and techniques are still in infancy when compares with the proposed novel model and algorithm. Hence, the current algorithms and techniques such as Anomaly Detection Framework (ADF), Cluster-Based Technique (CBT), Hybrid Neural Network (HNN), and Fog-based SCADA (F-SCADA) are not optimized for secure electric data transmission and could not address the above-mentioned issue of anomaly injection and malicious data detection.

3 System Model for Smart Grid

In this section, we discussed the difference between the conventional system model and the proposed advanced system model for the SG. Furthermore, we discussed the advanced system for secure communication in an SG network which enables the identification of anomalies and malicious data during data transmission. See Fig. 1 for the conventional system model.

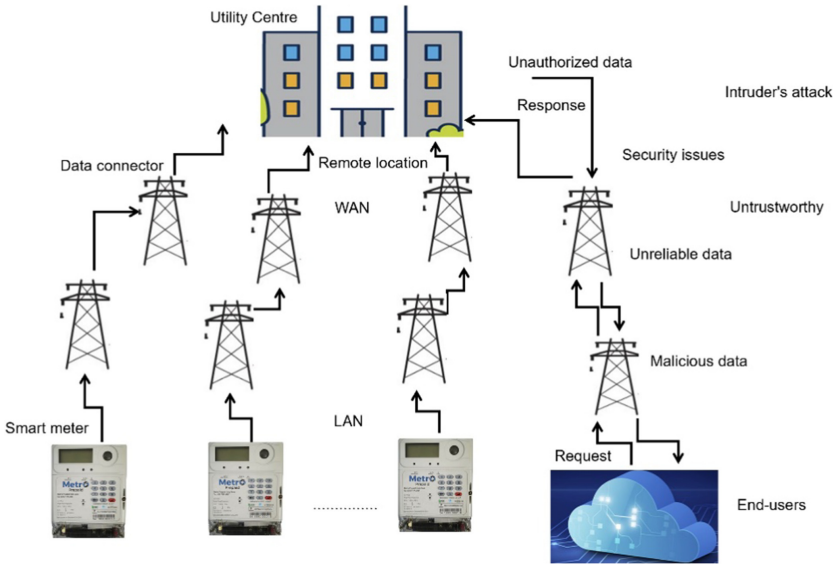

Fig. 1. Conventional system model for data communication flow in the SG network

Figure 1 shows the basic conventional system model for the electric data transmission in the SG network. The model consists of smart meters, data connectors, and a utility centre. All these components in the SG network are connected via LAN and WAN to a remote location. The conventional system model lacks advanced security features such as cryptographic operations and blockchain techniques for secure data transmission. It does not consist of an intelligent system to operate or monitor the electrical data flow status. 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. The model lacks the real-time decision-making capability to identify and detect anomalies and malicious data.

See Fig. 2 shows the novel system model for SG network communication, identification of anomalies, and classification of malicious data using fog nodes. Where the classification of outliers is conducted using a supervised machine learning approach. Linear SVM with the 2-PCA technique is used for reducing the number of parameters involve and can easily classify by distinguishing the outliers and similar patterns. In this concept, the fog node serves as a small sub-cloud server with limited storage and processing capabilities. Furthermore, the FC approach is employed in the SG to bring all of the advanced features of the cloud, such as resource sharing and server virtualization, closer to the SG network. As a result, unlike the cloud, the FC has no single point of failure.

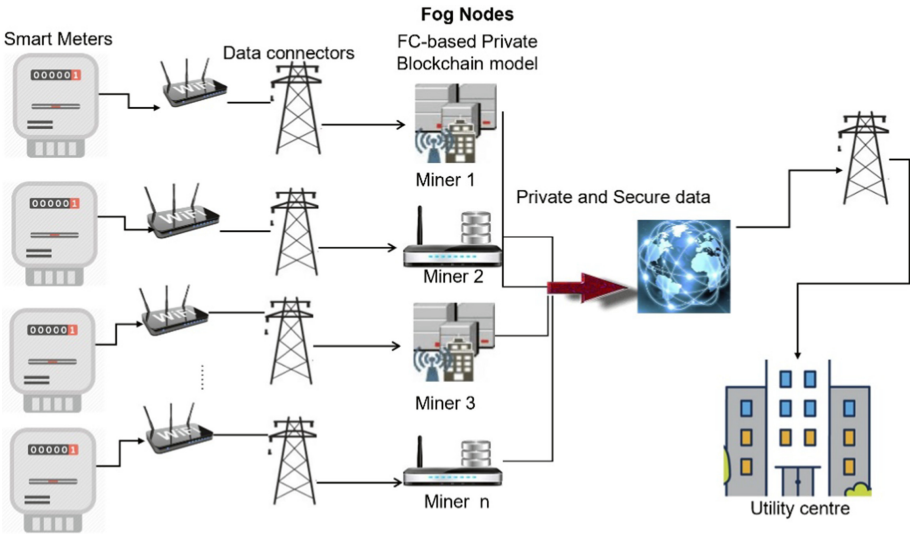

Fig. 2. Advanced system for anomaly detection in the SG network

Figure 2 shows the advanced system model for anomaly and malicious data detection in the SG network. The model consists of smart meters, Wi-Fi routers, data connectors, fog nodes, and a utility centre. The model works in an FC environment where the fog nodes play the role of miners by keeping the data transaction record in the SG network. The novel Linear Support Vector Machine Anomaly Detection (LSVMAD) algorithm works in coordination with fog nodes where the classification of malicious data is conducted inside the fog nodes. FC plays a key role here, utilizing blockchain technology to provide a distributed, scalable network at the smart meter's edge. Distributed FC nodes serve as miners, collecting transaction data in blocks and verifying its correctness. Fog nodes in our proposed work are responsible for handling all possible communication between smart meter devices to provide secure transactions between nodes, devices, and end-users. The proposed advanced system model for the SG network is smart enough to link with a decentralized blockchain model and distributed FC servers placed at the edge of the SG network. Therefore, this decision-making ability makes the advanced SG network an intelligent system when compared with the conventional system model and has an upper hand over it related to the security of the electrical data transmission from outside intruders and cyber-physical attackers. Only the secured encrypted data is transferred to consumers i.e., the smart meter users. The data is further decrypted by the utility office and the trusted authorities by the public-private key arrangement.

4 Linear Support Vector Machine Anomaly Detection (LSVMAD) Algorithm

In this section, we discussed the proposed advanced novel LSVMAD algorithm. The algorithm works to identify the anomalies in an SG network during electrical data transmission. The novel algorithm used the supervised machine learning (ML) algorithm called Linear SVM (Support Vector Machine) with 2-Principal Component Analysis (PCA) values. This technique is used to classify the data along a hyper-plane to identify classifiers. 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 anomalies present. The electrical data is encrypted using private-public key arrangements; the data is encrypted and then decrypted as per the user requirement. The algorithm uses asymmetric cryptographic operations for the security and verification of data. No third party is involved as the data is processed in the FC nodes. Furthermore, this section includes algorithm symbol notations, algorithm steps, and pseudocode.

LSVMAD Algorithm Symbol Notations

A_L: The list of electrical data packets having anomalies
A : Anomalies
$ASYM_{EC}$: Asymmetric encryption
C_s: Cloud server
CE_{ds} : The list of classified electrical data
C_T: Ciphertext
C_K : Cipher key
$dist$: distance
D_F : Data format
Db : Decision boundary
$Decryption_{Asym}$: Asymmetric decryption
E_{dp} : Electric data packet
E_{ds} : Electrical data set
E_{dpa}: Electric data packet allocation
$Encrypt_{sym}$: Symmetric encryption
$Encrypt_{Asym}$: Asymmetric encryption
FC_nPUB_K : Public key of the fog node
FC_n: Fog computing node
FC_nPRVT_K : Fog node private key
H_c : Hash code
K_{sym} : Symmetric key
k: Key
L_{SVM} : Linear SVM classifier
M : Miners
MG_w : Marginal width
np: Array for NumPy library package
$PRVT_K$: Private key
PUB_K : Public key
$2-PCA$: Principal component analysis
Sm_u : Smart meter users
ST_m : Smart Meters
S_mD: Smart meter data
$SPARK$: Real-time analyzer
T_s : Timestamp
U_O : Utility Office
w: Weight vector
X: Input vectors
y: Input vectors

LSVMAD Algorithm Steps

Requirement: FC_n and ST_m devices.
Step 1: Classification of E_{ds} using L_{SVM}
Step 2: Next E_{dpa} at FC_n using private blockchain.
Step 3: FC_n are used to store the E_{dp}
Step 4: A timestamp T_s is attached to the block of E_{dp}
Step 5: ST_m send the E_{dp} to F_n using ledgers and making decisions on A_L
Step 6: FC_n allocates the E_{dp}
Step 7: Applying $2 - PCA$ and predicting the anomalies.
Step 8: Next to perform E_{dpa} and mining at the individual FC_n
Step 9: ST_m sends a key K and E_{dp} to the FC_n
Step 10: Start of encryption process.
Step 11: FC_n verifies the key K
Step 12: Generate the H_C
Step 13 Next, to send the H_C to FC_n acting as miners.
Step 14: Checking of A_L
Step 15: Checking of CE_{ds}
Step 16: FC_n status is checked.
Step 17: Start of decryption process.
Step 18: Verification of ST_m and FC_n
Step 19: Consumers and meter management system can use their own $PRVT_K$ to retrieve the CE_{ds}

LSVMAD Algorithm:

Input: E_{dp} is the electric data packet, K_{sym} Symmetric key, FC_nPRVT_K Fog node private key, S_mD, and E_{ds} Electrical data set.
Output: Decrypted E_{dp} and $A_L$the list of electrical data packets having anomalies and CE_{ds}.

1: START
2: (FC-based blockchain system is created for anomalies identification)
3: E_{DS} classification using L_{SVM} 2 − PCA
4: **if** (S_mD == A_L) then
5: get geo-location and send the data for verification to FC_n using $SPARK$
6: **else if** (S_mD == $non - A_L$)
7: then
8: S_mD send to FC_n to C_s
9: E_{dp} is allocated to FC_n
10: **for** each E_{dp} do (ST_m <− C_T)
11: $C_T + T_s$ <- E_{dp}
12: **if** FC_n == Available
13: allocate the E_{dp}
14: **else** no allocation
15: **end if**
16: **end**
17: While $(iter \leq \text{maximum iteration})$ do
18: **function** def distance (self, w, with_lagrange =True):
19: $dist = self.y * (np.dot(self.X, w)) - 1$
20: get $dist$ from Db from the current Db
21: **if** MG_w == 1
22: get $dist$ from Db
23: generate CE_{ds} and A_L
24: **else if** MG_w == **0**
25: then $dist$ not retrieve
26: **end if**
27: **end if**
28: **end function**
29: $iter \leftarrow iter + 1$
30: **function** Encrypt (E_{dp})
31: **if** ST_m confirms E_{dp} storage over blockchain then
32: Generate a K_{sym}
33: C_T <− $Encrypt_{sym}$ (E_{dp} , K_{sym})
34: C_K <− $Encrypt_{Asym}$(K_{sym}, FC_nPUB_K)
35: **else**
36: do no operation
37: **end if**
38: **end function**
39: **function** $Decrypt$ (C_T, C_K, FC_nPRVT_K, K_{sym})
40: K_{sym} <-$Decryption_{Asym}$(C_k, FC_nPRVT_K)
41: E_{dp} <- $Decryption$ (C_T, K_{sym})
42: **end function**
43: **END**

5 Results and Discussion

This section discusses the results and simulation of the LSVMAD algorithm in the iFogSim Simulator. Next, we have used Anaconda (Python), Geth version 1.9.25, Truffle (Compile) and ATOM as a text editor for creating smart contracts. The algorithm usage the Linear SVM-2-PCA for the classification of data where anomalies are identified and classified by reducing the number of variables across a hyperplane. Moreover, the time complexity of the proposed LSVMAD algorithm for encryption function is $O(N)^2$ and for decryption function is $O(N)^3$. The combined time complexity for both functions used in the LSVMAD algorithm is $T(C) = O(N)^2 + O(N)^3$.

Next, it is necessary to remove the missing values and outliers and then fill the values with a mean data value. The missing values are removed using a Kalman filter. The 2-PCA values are considered to show the highest variation in the classified electrical data. The Geth version 1.9.25 is used to show the block receipts and block headers with new entries while executing the simulation. The algorithm is to be implemented using NetBeans and python with several main packages, modules, and classes. See Table 1 for hardware and software specifications.

Table 1. The hardware and software used for the implementation of the proposed algorithm

Hardware and software	Specification
Processor	Inter® Core™ i9-8750H
CPU	5.30 GHz
RAM	32 GB
System Type	64-bit Windows 10
Platform	iFogSim, SimBlock, and Spyder
Language	Java and Python

See Fig. 3 represent the physical topology configuration consisting of fog devices, master fog controller, cloud server and smart meter devices acting at the edge of the networks. This configuration will help in the future to get the preliminary idea of real-world implementation and deployment of the smart meter-FC-cloud system with sensors and actuators.

Figure 3 shows the physical topology for configuration built-in in the iFogSim simulator. The configuration is solely based on the concept of a proposed system.

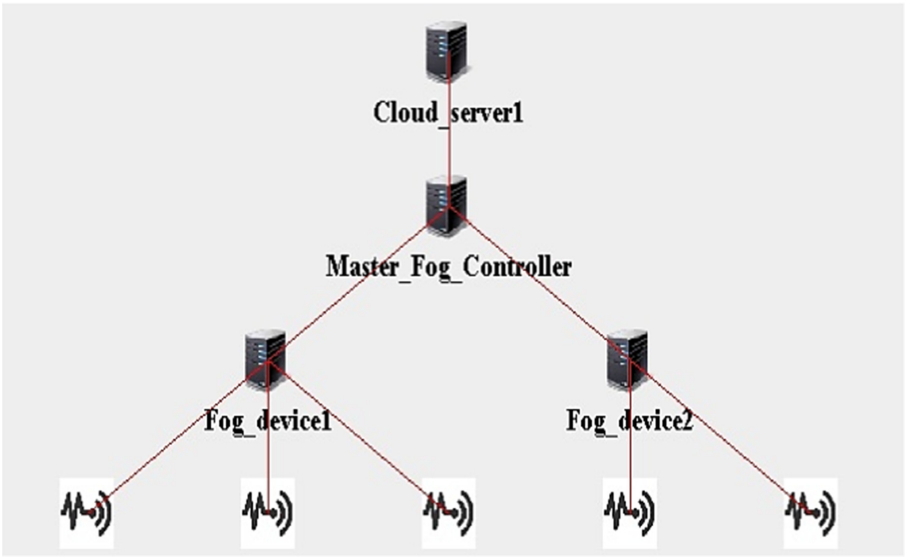

Fig. 3. GUI configuration using iFogSim

Whereas Fig. 4 shows the electrical data is classified for anomaly detection to the highest varied 2-PCA values using the linear SVM.

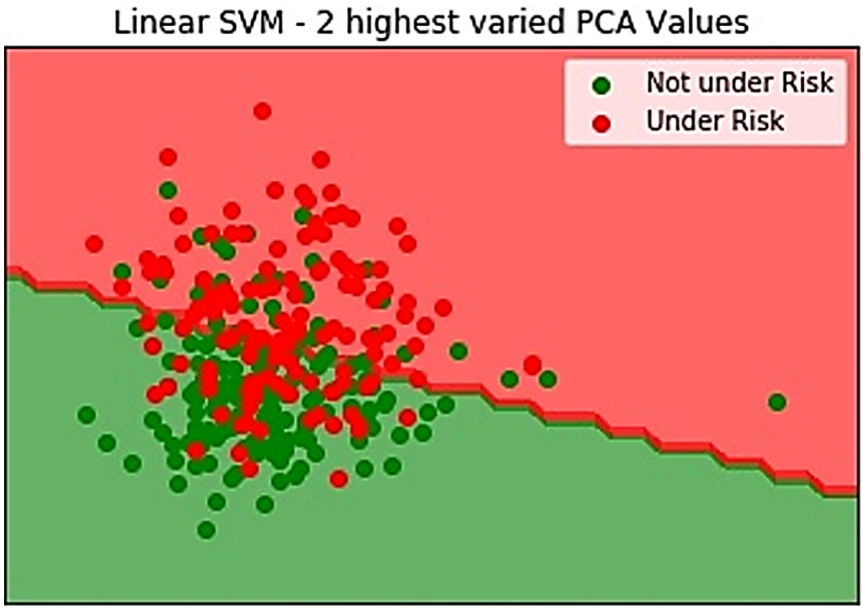

Fig. 4. Electrical data classification using Linear SVM-2-PCA for anomalies detection (Color figure online)

Figure 4 shows the not-under-risk data which is classified anomaly free data shown by green colour and under-risk data shown by red colour which consist of anomalies. The X-axis shows the electrical data PCA first column, and the Y-axis shows the electrical PCA second column.

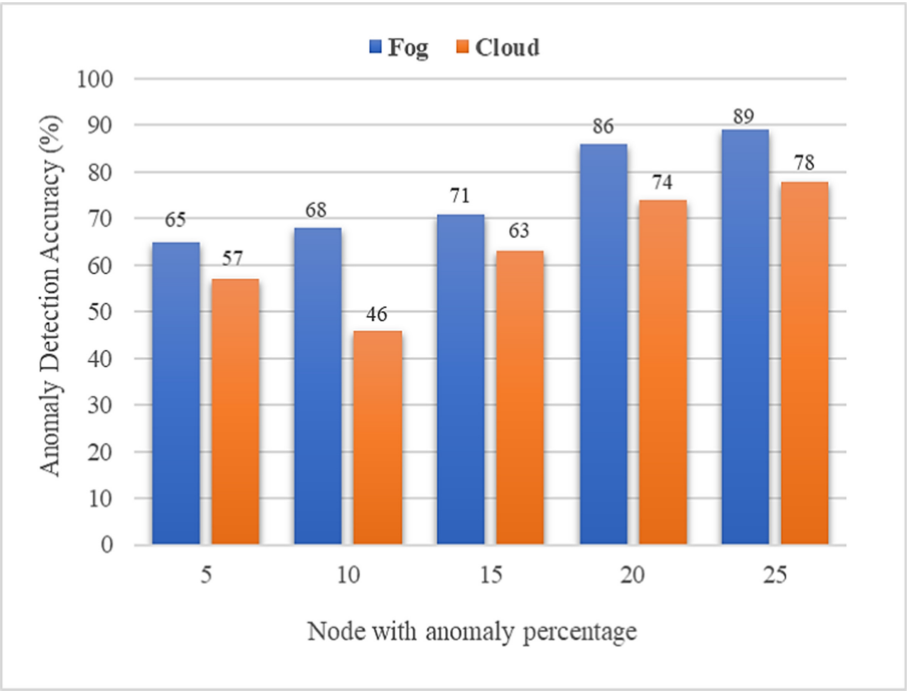

Fig. 5. Anomaly detection accuracy vs node with anomaly percentage

Figure 5 shows the percentage of a node with anomalies in fog and cloud along with the anomaly detection accuracy in percentage. The figure shows that the anomaly detection accuracy in fog nodes is much greater when compared to the cloud during data transmission between smart metes, data connectors, and consumers. The minimum anomaly detection accuracy of the LSVMAD algorithm for a node with anomaly percentage 5 in FC and cloud using iFogSim simulator is 65% and 57%. Whereas the maximum detection accuracy of the LSVMAD algorithm for a node with anomaly percentage 25 in FC and cloud environment is 89% and 78%. The proposed algorithm for anomaly detection accuracy percentage is tested on five different physical topology configurations at different anomaly node percentages. The detection accuracy increases with an increase in anomaly node percentage.

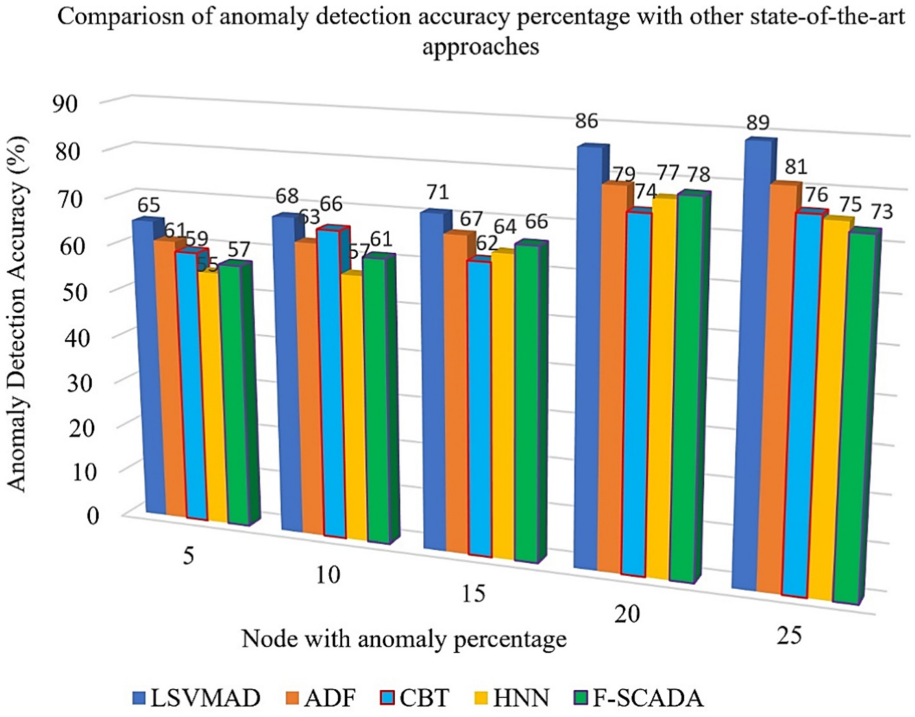

Fig. 6. Anomaly detection accuracy vs node with anomaly percentage performance evaluation

Figure 6 shows the comparison of a node with anomaly percentage vs anomaly detection accuracy for performance evaluation of the proposed LSVMAD algorithm with the other existing state-of-the-art techniques. Different existing algorithms are considered for benchmarking using the iFogSim simulator in five different physical topology configurations. The minimum detection accuracy is 55% for HNN at anomaly node percentage 5. Whereas the minimum detection accuracy for the LSVMAD algorithm is 65% at anomaly node percentage 5. Similarly, the maximum detection accuracy is 81% for ADF at anomaly node percentage 25. Whereas the maximum detection accuracy for the proposed LSVMAD algorithm is 89% at anomaly node percentage 25. The LSVMAD algorithm easily outperforms the other techniques. From Fig. 6 for the anomaly detection accuracy percentage, the proposed algorithm yields marked improvement over the other techniques.

6 Conclusion

SG network has a major role to play in smart cities. They can provide bi-directional information from consumers to the meter-management system and vice-versa. The energy and power are generated, transmitted, distributed, and at last, consumed at the site of smart meter users. However, with the advancement in technology and Industrial Revolution 4.0 (IR 4.0); the SG network becomes vulnerable to outside hackers and cyber-physical

attacks. The injection of anomalies, electrical theft, malicious data insertion, and FDI inside the SG network has generated a large risk to the SG network and its consumers.

Hence to overcome this issue we have proposed an advanced system model which consists of distributed fog nodes working as miners at the edge of the SG network with the help of blockchain technology. These fog nodes are intelligent enough to identify and classify anomalies during the transmission of electrical data. Next, we have proposed a novel Linear Support Vector Machine Anomaly Detection (LSVMAD) algorithm which uses the technique of Linear SVM with 2-PCA for data classification. The model was able to classify the anomalies from the electrical data set.

By analyzing the generated results from the proposed novel algorithm for anomaly detection accuracy; it is observed that the LSVMAD algorithm in the FC environment using blockchain and ML techniques easily outperforms the other existing state-of-the-art techniques such as ADF, CBT, HNN, and F-SCADA. The future work includes testing the algorithm to reduce the complexity of the SG system with the increase in the number of IoT devices, fog devices, smart meters, and end-users.

Acknowledgements. 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. Mollah, M.B., et al.: Blockchain for future smart grid: a comprehensive survey. IEEE Internet Things J. **8**(1), 18–43 (2020)
2. Musleh, A.S., Yao, G., Muyeen, S.: Blockchain applications in smart grid–review and frameworks. IEEE Access **7**, 86746–86757 (2019)
3. Gilbert, G.M., Naiman, S., Kimaro, H., Bagile, B.A.: critical review of edge and fog computing for smart grid applications. In: International Conference on Social Implications of Computers in Developing Countries, pp. 763–775. Springer (2019)
4. Drayer, E., Routtenberg, T.: Detection of false data injection attacks in smart grids based on graph signal processing. IEEE Systems Journal (2019)
5. Li, M., Zhang, K., Liu, J., Gong, H., Zhang, Z.: Blockchain-based anomaly detection of electricity consumption in smart grids. Pattern Recogn. Lett. **138**, 476–482 (2020)
6. Yang, Y., Liu, M., Zhou, Q., Zhou, H., Wang, R.: A blockchain based data monitoring and sharing approach for smart grids. IEEE Access **99**, 1 (2019)
7. Hussain, M., Beg, M.: Fog computing for internet of things (IoT)-aided smart grid architectures. Big Data Cogn. Comput. **3**(1), 8 (2019)
8. Jamil, B., Shojafar, M., Ahmed, I., Ullah, A., Munir, K., Ijaz, H.: A job scheduling algorithm for delay and performance optimization in fog computing. Concurrency Comput. Pract. Experience **32**(7), e5581 (2020)
9. Hashmani, M.A., Jameel, S.M., Ibrahim, A.M., Zaffar, M., Raza, K.: An ensemble approach to big data security (cyber security). Int. J. Adv. Comput. Sci. Appl. **9**(9), 75–77 (2018)
10. Gavriluta, C., Boudinet, C., Kupzog, F., Gomez-Exposito, A., Caire, R.: Cyber-physical framework for emulating distributed control systems in smart grids. Int. J. Electr. Power Energy Syst. **114**, 105375 (2020)

11. Zou, T., Bretas, A.S., Ruben, C., Dhulipala, S.C., Bretas, N.: Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks. Electric Power Syst. Res. **187**, 106490 (2020)
12. Wu, K., Cheng, R., Cui, W., Li, W.: A lightweight SM2-based security authentication scheme for smart grids. Alexandria Eng. J. **60**(1), 435–446 (2021)
13. Moghaddass, R., Wang, J.: A hierarchical framework for smart grid anomaly detection using large-scale smart meter data. IEEE Trans. Smart Grid **9**(6), 5820–5830 (2017)
14. Janetzko, H., Stoffel, F., Mittelstädt, S., Keim, D.A.: Anomaly detection for visual analytics of power consumption data. Comput. Graph. **38**, 27–37 (2014)
15. Chou, J.-S., Telaga, A.S.: Real-time detection of anomalous power consumption. Renew. Sustain. Energy Rev. **33**, 400–411 (2014)
16. Matoušek, P., Ryšavý, O., Grégr, M., Havlena, V.: Flow based monitoring of ICS communication in the smart grid. J. Inform. Secur. Appl. **54**, 102535 (2020)
17. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: Threats and potential solutions. Comput. Networks **169**, 107094 (2020)
18. Priyadharshini, N., Gomathy, S., Sabarimuthu, M.: A review on microgrid architecture, cyber security threats and standards. Mater. Today Proc. (2020)
19. Rahman, M.A., Al-Shaer, E., Bera, P.: A noninvasive threat analyzer for advanced metering infrastructure in smart grid. IEEE Trans. Smart Grid **4**(1), 273–287 (2012)