Secure Data Transmission in Smart Meters Using Q-Learning in Fog Computing Environment

Saurabh Shukla[1[0000-0002-3335-373X]], Subhasis Thakur[1[0000-0001-6579-724X]], and John G. Breslin[1[0000-0001-5790-050X]]

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

Abstract. With the advancement in technology and connectivity, the concept of smart grids with smart meters has significantly increased the interest of both electric consumers and power suppliers. Nowadays the smart cities are using the technology of smart meters in their household. Which can transfer the electrical data in a bi-directional way to consumers and smart grids. It consists of various internet-connected sensors, software applications, to connect different devices. This makes the smart grid network more complex which is further vulnerable to the cyber-attack. Moreover, it gives rise to various malicious attack such as false data injection (FDI) in smart meters which leads to incorrect decisions due to a large number of open access points in a network which is accessible to outside intruders. In smart meters, Home Area Network (HAN) and smart meter collectors are more vulnerable for cyber-attacks as they are directly involved in bi-directional communication between the devices such as smart grid, data connectors and smart meters. Since smart meters work in a distributed environment where fog computing (FC) placed at the edge of the networks can play a major role by integrating with blockchain for secure electric data transmission and to avoid the FDI in smart meters. Here FC nodes will act as miners to makes the decisions on the data transmission while monitoring the states of the system. Hence, we propose a novel solution for the above mention issue which consists of 3-tier FC-based blockchain architecture and Smart Meter-based Q-Learning Encryption (SMQE) algorithm to verify the system in FC environment. The algorithm performs the identification of FDI, and malicious attacks conducted on smart meters during data transmission. It opens a blockchain-based channel for secure data transmission in smart meters. The simulations tools used for this purpose are iFogSim, SimBlock, Python (Anaconda) with Geth version 1.8.23.

Keywords: Smart grid, smart meter, fog computing, cloud computing, smart data collector, cyber-attack, Q-learning, Markov decision process, reinforcement learning.

1 Introduction

Please Traditional gird with conventional meters has been used for a quiet long period in our households. These grids connect the meters, power grids and the consumers in a single directional way. Here meters have a limited role to play for the electric data

transmission. They lack the real-time transmission, connectivity between different electrical appliances and meters which makes them unsuitable for the current existing smart cities[1]. Secure electric data transmission with low latency and high throughput play a central role in smart meters. Lately due to the advancement in the deployment of smart meters in smart cities have opened a security challenge to avoid cyberattack on the complex network of smart grid. Here the electric data is usually transferred from Home Area Network (HAN) to Neighborhood Area Network (NAN) to Wide Area Network (WAN) [2]. Current consumption in cities requires constant monitoring and efficient secure transmission between smart grids, smart meters and consumers in real-time. These smart meters can be connected and disconnected at the ease of consumers depending upon their requirements and usage in their households. Smart meters are a kind of computers which are a part of the cyber world[3]. The network of a smart grid is open and decentralized which further makes it more vulnerable from cyber-attacks such as malicious data inclusion, false data injection (FDI) and erroneous values transmission [4].

The attackers here can easily change or manipulate the meter value according to their requirement and needs by monitoring the user power consumption level. They can have a monitory benefit with this illegal approach and attack [2]. Wrong feedback can be provided by smart meters to smart grids regarding the electricity supplies and power consumption. Existing smart grids are deployed in a decentralized manner and connected to centralized cloud servers which can be an issue of a single point of failure[1]. With the advancement in technology especially for distributed networks; edge computing and fog computing (FC) plays a major role to safeguard the electric data distribution across a spread decentralized open network. FC works in Local Area Network (LAN) and can connect with HAN, NAN and WAN in smart meter network [5]. Whereas, blockchain also works in a centralized manner by keeping the transaction records of all the blocks using an attached timestamp[6, 7].

FC nodes act like miners in the blockchain environment since blockchain also works in a decentralized manner. Both FC and blockchain technology can minimize the cyber-attack possibilities in smart meters [8, 9]. Miners here consists of an encryption algorithm to encrypt the meter data and readings from the outside world [10]. This data can further be securely distributed among fog nodes. Therefore, we have proposed a Smart Meter-based Q-Learning Encryption (SMQE) algorithm which uses Q-learning technique of Reinforcement Learning (RL) algorithm to makes the decisions in the stochastic environment by solving the problem of Markov Decision Process (MDP) as the system state of smart meter network changes with time.

Recent works mostly focused on the detection of electricity theft in smart meters, classification of malicious data using a machine learning algorithm. They lack real-world implementation. Hence, we propose a novel solution using a machine learning technique in FC-based blockchain environment for secure electric data transmission in smart meters network. This local deployment of fog nodes at the edge will be able to minimize the overhead cost related to energy and communication in the smart grid and smart meter. Furthermore, it will also minimize the complexity of the system and deployment cost-related for the system setup and installation in real-world.

2 Background and Related work

In the existing scenario smart meters plays a major role in electric data transmission in smart cities through data connectors to utility offices. They measure and record the power consumption of the household and transfer the data from milliseconds to seconds to various connecting meter management system. However, this network system is so complex and vulnerable that's it's easy for cyber attackers to easily hack the system. The smart meter is nothing but a computer system therefore it is vulnerable to outside attack.

The six main aspects of cybersecurity concern of smart meters and smarts grid which are open to research work are 1) Integrity 2) Confidentiality 3) Availability 4) Reliability 5) Authentication and 6) Authorization [11-13]. Here the cyber threat in smart grid network is related to all the three networks, i.e. NAN, HAN, and WAN. Attacks such as false data injection (FDI) can easily change the system state which leads to stochastic state and it's become difficult to monitor the data and identify the malicious attack [1, 14]. This attack can further incorporate the flow of data traffic by misleading the original flow of data.

The FDI can be sub-divided into four major attacks such as 1) Attack on smart meter device 2) Data attack 3) Attack on privacy and 4) Attack on the network [2, 6]. Considering this issue many of the researchers have highlighted this problem to find the exact solution but most of them just worked on the electrical theft using machine learning algorithms [15, 16]. Some of them have classified the malicious data using 2 PCA Linear SVM[17]. But still, there is the major gap to fulfil the QoS requirement for electric data transmission between smart meters, consumers, prosumers, meter management system and utility offices. This requires the identification of FDI in smart meters and authenticity of connecting meters and data connectors. Some of the works have been mentioned in this section also.

In [18], the authors used a fog computing-based model to design a grid topology using MATLAB Simulink for smart grid monitoring. Their proposed model was developed to monitor voltage and power loss during transmission of data in the smart grid network. Their primary focus was on the monitoring of data transmission using Fog-Cloud network. However, no work has been done considering the cyberattack related to the smart grid. In [19], the authors proposed a novel solution to identify the FDI using an input observer-based distributed detection system. The system was able to easily detect the transition in states. Moreover, they were able to isolate the FDI using their proposed distributed detection approach. They mostly considered the stealthy characteristics of False Data Injection Algorithm (FDIA). However, it lacks the real-world implementation of their proposed work.

Similarly, in [20], the authors suggested blockchain as a tool for security in a smart grid system. They also mentioned how blockchain as a tool can be efficient for a smart grid complex network system by keeping the record of several transactions with an attached timestamp. Moreover, with this technology, the user can verify the records of power consumption bills and meter readings. This will help in return to maintain system confidentiality and integrity. The user can easily track the history of the transaction occurred in the smart meter network. In [1], the author conducted a complete survey

analysis of smart grid and smart meter highlighting the benefits and drawbacks related to the security aspect of electric data transmission and consumers records. Moreover, the author has also highlighted the network topology used in the smart grid network along with communication protocols.

On a similar note, the authors in [4], highlighted the issue of cybersecurity and cyber threat on the smart grid network. Furthermore, they discussed the challenges, threats and potential measures to overcome these attacks. They conducted an in-depth analysis of several network threats and their effects on national security. A detailed discussion and description were given in their research article about the attacks on Cyber-Physical System (CPS) of smart grid and smart meters. Some future perspective and measurements were also given to minimize the effect of cyber-attacks on smart grids. In [21], the authors implemented the integrated blockchain model with Ethereum and Hyperledger to measure the performance of the smart grid network. Furthermore, they presented a virtual network of smart gird to monitor the data transaction and transmission by making a slight modification in their smart contracts.

The authors in [22], proposed a detection method for FDI in smart grids. This method was based on the Graphical Signal Processing (GSP) by utilizing the graph Fourier transform. Their derivation was based on the graph model and the flow of the AC power. By calculating the deviations in frequency and measuring it by a threshold value they were able to detect the FDI including the previous one also which were present in the historical record of transitions. In [23], the authors suggested and conducted a detailed survey analysis of blockchain for futuristic smart grids. They further discussed the issued related to the complex network system of the smart grid system and role of blockchain as a decentralized system to minimize the cyber-attacks and keep a record of the previous transaction. They have identified many challenges linked to smart grid that can be resolved using the blockchain model. At, the last they concluded with future direction and challenges while integrating blockchain with smart grid network. This article opens a research directive for other researchers to work on the issue related to the smart grid.

Similarly, the authors in [24], discussed the security and communication in the smart grid network. Moreover. They highlighted the importance of cybersecurity by mentioning its key features and aspects for smart grid network topology. They mostly focused on the security-related communication protocols in the smart grid. The authors in [16, 17] and [15] have used machine learning and statistical techniques such as SVM and reinforcement learning to overcome the issue of FDI in smart grid and smart meters. In [3], the authors proposed an FC-based model integrated with IoT for smart grid network for real-time data analytics and transmission. They have highlighted the issue of a single point of failure in the cloud due to its centralized deployment. Whereas here the FC nodes can be deployed near the smart grid network at HAH and NAN. Their proposed model was able to minimize the latency in the network of the smart grid by maintaining the workload distribution and achieving the Quality-of-Service requirement (QoS). The above-mentioned existing work on the issue of cyber-attack and security in the smart grid and smart meter mostly focused on the theoretical aspects of the solution. They lack the real-world implementation which can be useful at the local deployment sites. Most of the previous works have focused mainly on communication

protocols and in energy management. Hence there is an urgency to work in the direction of cybersecurity in smart grid and smart meters for smart city development and deployment. Which in turn will benefit both the society and consumers.

3 3-Tier FC-Based Blockchain Architecture for Smart Meter

This section discusses the prosed 3-tier FC architecture with blockchain. The section further discusses the importance of FC and blockchain for smart meters deployed at the user's household. See Fig. 1 for 3-tier FC architecture.

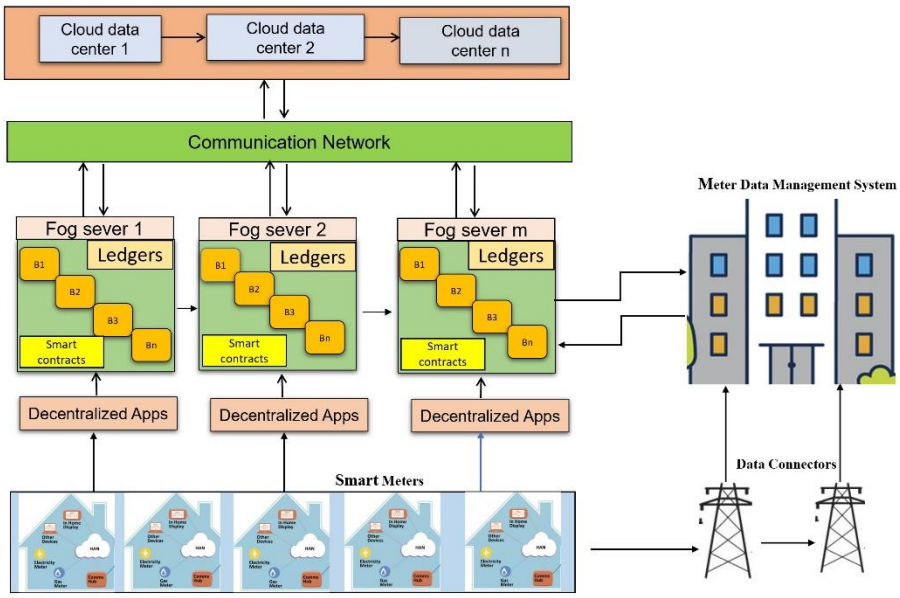

Fig. 1. A 3-tier FC-based blockchain architecture for smart meter

The proposed 3-tire FC -based architecture consists of three layers. The first layer consists of smart meters placed at the consumer site. These smart meters are connected using HAN and NAN to FC nodes which are deployed at the middleware layer. The smart meters are further connected to the meter data management system through various data connectors using WAN. The electric data is then transferred to the middleware layer which consists of fog servers; these fog servers are divided into various virtual machines (VM). These machines consist of software and application for smart contracts and decentralized apps with ledgers to identify the false data injected between transmission from smart meters to fog servers and meter data management system. Here FC nodes will act as miners for secure data transmission. Next, the data is further transferred to a cloud server for further processing and analysis. This data is usually the

historical records of consumers household electric data consumption along with big data related to power consumption. The data can be transferred directly in single-hop count from fog servers to the utility office.

4 Proposed Advanced System Model

This section discusses the conventional method of electric data transmission and proposed advanced system model for the secure electric data transmission between smart meters, FC nodes, cloud servers, and meter data management system through various data connectors. See Fig. 2 shows the traditional method of electric data transmission.

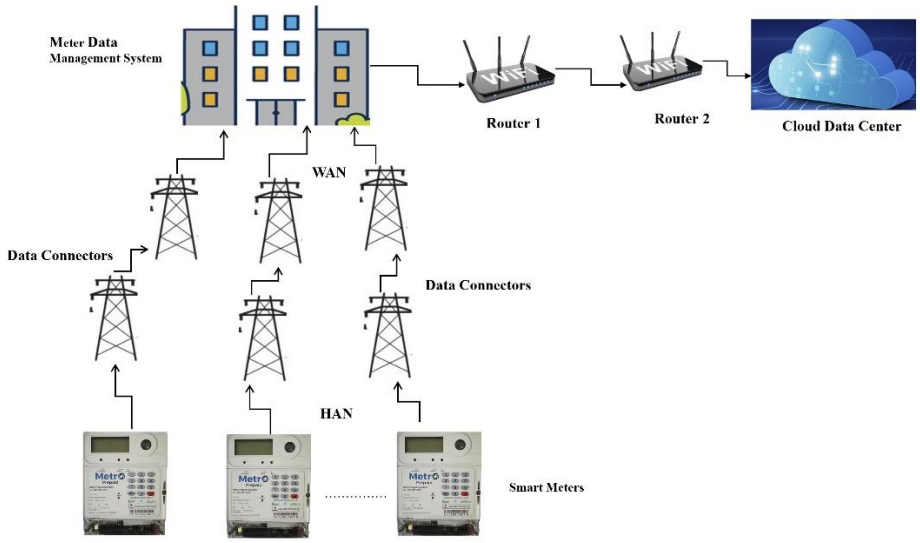

Fig. 2. Conventional system model for electric data transmission

Fig. 2 is a conventional system model which is used nowadays for electric data transmission. Here the smart meters are connected through data connectors. The data is transmitted from HAN to WAN [25]. Furthermore, the meter data management system is connected to a cloud server for the request and retrieval of information for user power consumption. The main drawback with this system is that it is an open network where smart meters are connected to many data connectors with multiple hop counts which helps in transmission to the meter data management system. This makes it vulnerable to cyber-attacks on the electric data where a false data is injected at the meter site and on the data connector sites. The meter system unit is connected to a cloud server for further data processing. Here cloud servers itself is the vulnerable factor due to the single point of failure because of its centralized functioning. Therefore, we proposed an advanced system model for smart meter using FC and blockchain.

See Fig. 3 shows the proposed system model for secure data transmission.

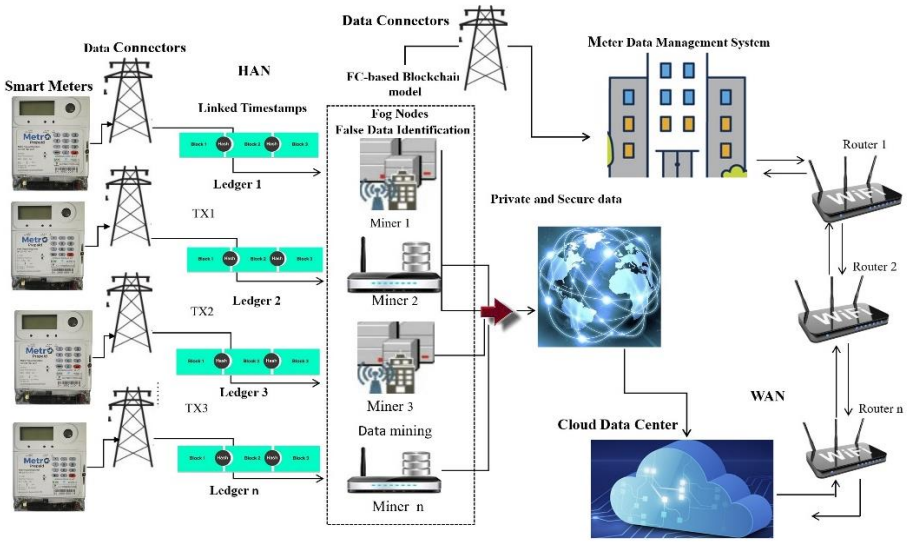

Fig. 3. Proposed advanced system model for data transmission

Fig. 3 shows an advance system model for secure electric data transmission for smart meters. The model utilizes the concept of distributed FC deployed at the local household sites. These fog nodes work in HAN and connect through WAN to the meter management system. The smart meters measure the reading and send the data through data connectors to fog nodes. The fog nodes receive the data in the form of ledgers by an attached time stamp for the identification of smart meters and electric data readings. These fog nodes now act as miners using private blockchain model. The fog serves uses Q-learning technique of reinforcement learning (RL) algorithm to solve the Markov Decision Process (MDP) using the best quality of action to identify the false data injection (FDI) inside the stochastic system. The proposed system states are continuously changing with the change in the readings of smart meters as these reading and data are generated in real-time with minimum latency. In the proposed model the data is directly transferred to the meter management system and utility offices through data connectors in a single hop count. Next, the historical data is transferred to the cloud using Wi-Fi routers. The system works in a closed network when compares to traditional meter system, which makes it more secure from outs side cyber-attack and FDI.

5 Smart Meter-based Q-Learning Encryption (SMQE) Algorithm

The principal aim of this research is the development of a novel approach to meet the QoS requirement related to security, identification and authenticity of data transmission

between smart meters, fog nodes, data connectors, consumers, and the cloud servers using FC-based blockchain approach. To accomplish the main aim, we propose a 3-tier FC-based blockchain architecture for smart-meters. Next, we designed and developed a novel SMQE algorithm. The algorithm performs the identification of False Data Injection (FDI) by predicting the change in the system state, verification of data sources and targets when data is transmitted data via different smart meters and fog nodes.

The algorithm uses a Q-learning technique to solve MDP in smart meters [26]. The data is encrypted and then decrypted using private blockchain and different cryptographic operations inside fog nodes. FC nodes acting as miners in smart meter network plays a major role by identifying the FDI. Here FC nodes make decisions on the transmission of flow of data while monitoring the states of the system. Miners here consists of encryption algorithm to encrypt the meter data and readings from the outside world. The smart meters measure the reading and send the data through data carriers to fog nodes. The fog nodes receive the data in the form of ledgers with an attached time stamp for the identification of smart meters and data readings. Q-learning solves the MDP using the best quality of action to identify the FDI inside the stochastic system as the meter reading and data changes with time.

The algorithm performs security of data transmission between smart meters fog nodes, meter management system, and consumers. The algorithm uses the FC-based blockchain system for storing and securing the data. The users can then retrieve the data from these nodes. The algorithm further performs the encryption of data over the blockchain. The data is generated from smart meters and is encrypted using an algorithm. The output is the secured data. The algorithm further performs the identification of FDI using Q-learning technique of reinforcement learning algorithm by solving MDP in a stochastic environment. Asymmetric public-private key pairs are also used in the development of an algorithm. The algorithm performs the asymmetric decryption of smart meter data using fog node private key and a symmetric key.

SMQE Algorithm Symbol Notations

C_m : Consumer

M_s : Meter management system

S_m : Smart Meters

E_d : Electric data

E_d_ID: ID of the participated smart meters

F_n: Fog nodes

L: The list of the configuration S_m devices sent by the F_n

α_i : Learning rate

γ_i : Discount factor

$(\in)$: Exploration policy

K_{sym} : Symmetric key

K_{pub} : Public key
F_nK_{pub} : Fog node public key
$Encrypt_{Sym}$: Symmetric encryption
$Encrypt_{Asym}$: Asymmetric encryption
C: Ciphertext
C_K : Cipher key
F_nK_{prvt} : Fog node private key
K_{Sym} : Symmetric key
F_s : Fog server
T_s : Timestamp
K: Key
H_c : Hash code
$Prvt_K$: Private key
D_F : Data format
M : Miners
C_s : Cloud server
S_m_D: Smart meter data
E_{da}: Electric data allocation
Q_L : Q-learning

Algorithm Steps:
Requirement: F_n and S_m devices are present in the fog layer and smart meter layer
Step 1: Classification of S_m_D
Step 2: F_s consists of F_n
Step 3: Next E_{da} at F_n using private blockchain and Q_L
Step 4: F_n are used to store the E_d
Step 5: A timestamp T_s is attached to the block of E_d
Step 6: S_m send the E_d to f_n using ledgers and making decisions using Q_L to identify FDI
Step 7: F_s allocates the S_m_D
Step 8: Next to perform E_{da} and mining at the individual F_n
Step 9: S_m sends a key and E_d to the F_s
Step 10: F_s verifies the key K
Step 11: Generate the H_c
Step 12: Next, to send the H_c to miners M
Step 13: Send S_C to F_n
Step 14: D_f checking
Step 15: M status is checked
Step 16: Verification of S_m and F_n
Step 17: Consumers and meter management system can use their own

SMQE Algorithm:
Input: Encrypted S_m_D C, Encrypted Symmetric key C_k
Output: Decrypted S_m_D
1: ***START***
2: (FC-based blockchain system is created)
3: Data classification
4: **if** ($S_m\_D == Malicoius\ data$) then
5: get geo-location and send the data for verification to F_n using $SPARK$
6: **else if** ($S_m\_D == non-malicious\ data$)
7: then
8: S_m_D send to F_n to C_s
9: F_n allocates the E_d to F_s
10: **for** each S_m_D do ($S_m <- C_T$)
11: $C_T + T_s <$ - S_m_D
12: **if** F_s == Available
13: allocate the E_d
14: **else** no allocation
15: **end if**
16: **end**
17: ***Set*** $Q(s,a) = 0(\forall s \in S_i)(\forall a \in A_i(a))$, $iter := 0$, *and* $s := (1,1\{(Q_1 - - - - - - - - Q_N) \mid Q_i = 0\})$
18: ***While*** $(iter \le \text{maximum iteration})$ ***do***
19: *Select* $a \in A_i(a)$ *applying* $\in$*- greedy algorithm*
20: *Allocate the data packets conferring to action* a *and examine the next state* s' *and reward* r.
21: $Q(s,a) \leftarrow (1-\alpha_i)Q(s,a) + \alpha_i\left[R_i(s,a) + \gamma_i \max_{a' \in A_{s'}} Q(s',a')\right]$
22: $s \leftarrow s'$
23: $iter \leftarrow iter + 1$
24: **Function** Encryption (S_m_D)
25: **if** S_m confirms E_d storage over blockchain then
26: Generate a K_{sym}
27: $C <- Encrypt_{Sym}$ (S_m_D , K_{sym})
28: $C_k <- Encrypt_{Asym}(K_{sym}, F_nK_{pub})$
29: **else**
30: do no operation
31: **end if**
32: **end function**
33: **function** $DECRYPTION$ (C, C_k, F_nK_{prvt}, K_{sym})
34: K_{sym} <-$Decryption_{Asym}(C_k, F_nK_{prv})$
35: S_m_D <- Decryption (C, K_{sym})
36: **end function**

6 Results and Discussion

This section discusses the result and simulation of the proposed work. The SMQE algorithm is simulated using iFogSim and SimBlock simulator. iFogSim is an open-source simulator used for creating physical topology design, resource placement, and packet allocation by creating different edges, networks, nodes, and devices with cloud and fog sever. It is a Graphical User Interface (GUI) based open-source platform for fog-based simulation. The Proof-Of-work (PoW) concept for SMQE algorithm performance is conducted using SimBlock and JSON by showing the VM telemetry.

Next Geth version 1.8.23 is used to show the block receipts and block headers with new entries while executing the simulation. The performance of the FC-based blockchain model that incorporates the proposed algorithm is analyzed through simulation and experiments. The baseline for this simulation is FDI for secure data transmission in smart meters. We developed a Proof of Work (PoW) implementation for the smart meter-fog system, Ethereum was chosen as the blockchain-based technology for PoW. Next, Profiler of NetBeans IDE 8.1 act as performance analysis tools for our proposed model and algorithm in simulation.

See Table 1 for software and hardware 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	32GB
System Type	64-bit Windows 10
Platform	iFogSim, SimBlock, and Spyder
Language	Java and Python

The algorithm is to be implemented using Netbeans and python with several main packages, modules, and classes.

Fig. 4 represent physical topology configuration. 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.

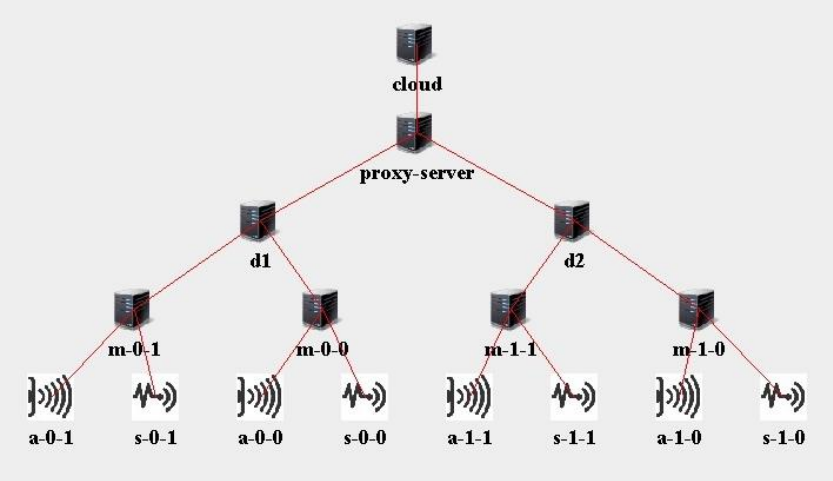

Fig. 4. GUI configuration

Fig. 4 shows the physical topology for configuration built-in the iFogSim simulator. The configuration is solely based on the concept of a proposed system.

See Fig. 5 shows the VM telemetry of the proposed novel SMQE algorithm for PoW in fog node acting as miners during execution

Fig. 5. VM telemetry of SMQE algorithm for Proof of Work (PoW) in miner

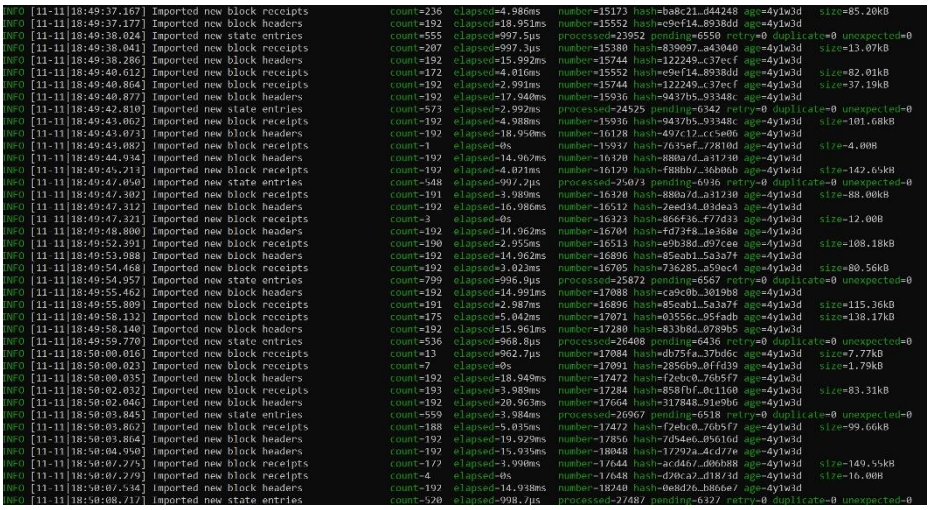

Fig. 6. SimBlock simulation for new state entries, block receipts and block headers

Fig. 6 shows the simulation of nodes for new state entries, new block headers and new block receipts in SimBlock simulation tool.

Fig. 7. Comparison of packet error

Fig. 7 shows the comparisons of packet error using SMQE algorithm between fog nodes and cloud servers at different time intervals. The figure shows the packet error in fog nodes is much lesser when compared to the cloud during data transmission between smart metes, data connectors, meter management system, and consumers.

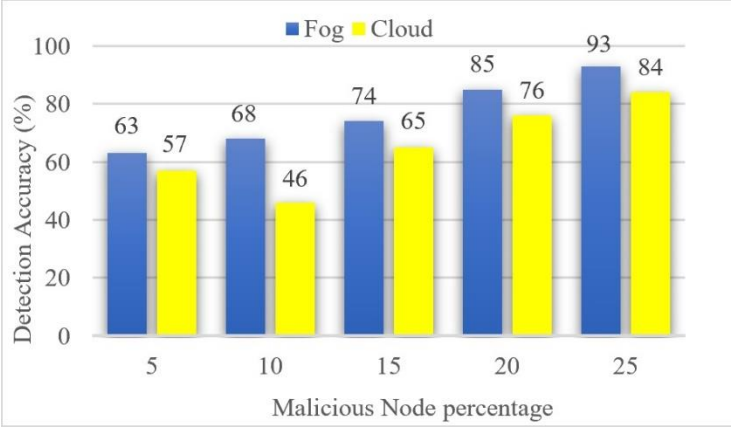

Fig. 8. Malicious node percentage vs detection accuracy

Fig. 8 shows the malicious node percentage in fog and cloud along with the detection accuracy in percentage. The figure shows that the detection accuracy in fog nodes is much greater when compared to the cloud during data transmission between smart metes, data connectors, meter management system, and consumers.

7 Conclusion

Smart meters are now used in smart cities for the transmission of electric data with minimum delay. The consumers can access the data through physical means such as using their mobile devices through HAN, NAN and WAN. Smart meters are a cyber-physical system such as smart computer where information can be access in real-time. However, the system is so complex and wide that it makes it vulnerable to cyber-attacks such as FDI where an intruder or an attacker adds some malicious data and changes the configuration where the meter start responding and generating false or erroneous value. Which leads to huge loss to smart city and consumer society.

Therefore to overcome this issue we have proposed a 3-tier FC-based blockchain architecture, and Smart Meter-based Q-Learning Encryption (SMQE) algorithm to identify the FDI and encrypt the data which further helps in a secure data transmission between smart meters, fog nodes acting as miners, consumers, meter management system, and cloud servers. The future work includes the benchmarking and comparison with other existing works in terms of algorithm performance and efficiency.

References

1. Kabalci, Y., *A survey on smart metering and smart grid communication.* Renewable and Sustainable Energy Reviews, 2016. **57**: p. 302-318.
2. Khattak, A.M., S.I. Khanji, and W.A. Khan. *Smart meter security: Vulnerabilities, threat impacts, and countermeasures*. in *International*

Conference on Ubiquitous Information Management and Communication. 2019. Springer.

3. Hussain, M. and M. Beg, *Fog computing for internet of things (IoT)-aided smart grid architectures.* Big Data and cognitive computing, 2019. **3**(1): p. 8.
4. Gunduz, M.Z. and R. Das, *Cyber-security on smart grid: Threats and potential solutions.* Computer Networks, 2020. **169**: p. 107094.
5. Khan, S., S. Parkinson, and Y. Qin, *Fog computing security: a review of current applications and security solutions.* Journal of Cloud Computing, 2017. **6**(1): p. 19.
6. Pop, C., et al., *Blockchain based decentralized management of demand response programs in smart energy grids.* Sensors, 2018. **18**(1): p. 162.
7. Li, M., et al., *Blockchain-based anomaly detection of electricity consumption in smart grids.* Pattern Recognition Letters, 2020. **138**: p. 476-482.
8. Yetis, R. and O.K. Sahingoz. *Blockchain Based Secure Communication for IoT Devices in Smart Cities*. in *2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*. 2019. IEEE.
9. Yang, Y., et al., *A Blockchain Based Data Monitoring and Sharing Approach for Smart Grids.* IEEE Access, 2019.
10. Alladi, T., et al., *Blockchain in smart grids: A review on different use cases.* Sensors, 2019. **19**(22): p. 4862.
11. Musleh, A.S., G. Yao, and S. Muyeen, *Blockchain applications in smart grid–review and frameworks.* IEEE Access, 2019. **7**: p. 86746-86757.
12. Gilbert, G.M., et al. *A critical review of edge and fog computing for smart grid applications*. in *International Conference on Social Implications of Computers in Developing Countries*. 2019. Springer.
13. Nehaï, Z. and G. Guerard. *Integration of the blockchain in a smart grid model*. in *The 14th International Conference of Young Scientists on Energy Issues (CYSENI) 2017*. 2017.
14. 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.
15. Chen, Y., et al., *Evaluation of reinforcement learning-based false data injection attack to automatic voltage control.* IEEE Transactions on Smart Grid, 2018. **10**(2): p. 2158-2169.
16. Esmalifalak, M., et al., *Detecting stealthy false data injection using machine learning in smart grid.* IEEE Systems Journal, 2014. **11**(3): p. 1644-1652.
17. Kallitsis, M.G., et al. *Adaptive statistical detection of false data injection attacks in smart grids*. in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. 2016. IEEE.
18. Forcan, M. and M. Maksimović, *Cloud-fog-based approach for smart grid monitoring.* Simulation Modelling Practice and Theory, 2020. **101**: p. 101988.
19. Wang, X., et al., *Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers.* International Journal of Electrical Power & Energy Systems, 2019. **110**: p. 208-222.

20. Agung, A.A.G. and R. Handayani, *Blockchain for smart grid.* Journal of King Saud University-Computer and Information Sciences, 2020.
21. Malik, H., et al. *Performance Analysis of Blockchain based Smart Grids with Ethereum and Hyperledger Implementations*. in *IEEE International Conference on Advanced Networks and Telecommunications Systems*. 2019.
22. Drayer, E. and T. Routtenberg, *Detection of false data injection attacks in smart grids based on graph signal processing.* IEEE Systems Journal, 2019.
23. Mollah, M.B., et al., *Blockchain for future smart grid: A comprehensive survey*. IEEE Internet of Things Journal, 2020.
24. Ericsson, G.N., *Cyber security and power system communication—essential parts of a smart grid infrastructure.* IEEE Transactions on Power Delivery, 2010. **25**(3): p. 1501-1507.
25. Lombardi, F., et al., *A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids.* 2018.
26. Saurabh Shukla, M.F.H., Low Tang Jung, Azlan Awang, Muhammad Khalid Khan, *An analytical model to minimize the latency in healthcare internet-of-things in fog computing enviornment.* https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0224934, 2019. **14**(PLOS ONE 14(11): e0224934): p. 1-31.