Secure Communication in Smart Meters using Elliptic Curve Cryptography and Digital Signature Algorithm

Saurabh Shukla
Data Science Institute (DSI)
National University of Ireland Galway (NUIG)
Galway, Ireland
saurabh.shukla@nuigalway.ie

Subhasis Thakur
Data Science Institute (DSI)
National University of Ireland Galway (NUIG)
Galway, Ireland
subhasis.thakur@nuigalway.ie

John G. Breslin
Data Science Institute (DSI)
National University of Ireland Galway (NUIG)
Galway, Ireland
john.breslin@nuigalway.ie

***Abstract*—With the advancement in the growth of Internet-of-Things (IoT), its number of applications has also increased such as in healthcare, smart cities, vehicles, industries, household appliances, and Smart Grids (SG). One of the major applications of IoT is the SG and smart meter which consists of a large number of internet-connected sensors and can communicate bi-directionally in real-time. The SG network involves smart meters, data collectors, generators, and sensors connected with the internet. SG networks involve the generation, distribution, transmission, and consumption of electrical power supplies. It consists of Household Area Network (HAN), and Neighborhood Area Network (NAN) for communication. Smart meters can communicate bidirectionally with consumers and provide real-time information to utility offices. But this communication channel is a wide-open network for data transmission. Therefore, it makes the SG network and smart meter vulnerable to outside hacker and various Cyber-Physical System (CPS) attacks such as False Data Injection (FDI), inserting malicious data, erroneous data, manipulating the sensor reading values. Here cryptography techniques can play a major role along with the private blockchain model for secure data transmission in smart meters. Hence, to overcome these existing issues and challenges in smart meter communication we have proposed a blockchain-based system model for secure communication along with a novel Advanced Elliptic Curve Cryptography Digital Signature (AECCDS) algorithm in Fog Computing (FC) environment. Here FC nodes will work as miners at the edge of smart meters for secure and real-time communication. The algorithm is implemented using iFogSim, Geth version 1.9.25, Ganache, Truffle for compiling smart contracts, Anaconda (Python editor), and ATOM as language editor for the smart contracts.**

Keywords—Smart grids, Smart meter, Fog computing, Cloud computing, Machine learning, Cryptography, Elliptic curve cryptography, Digital signature, Cyber-physical system, Internet-of-Things.

I. INTRODUCTION

The smart meter has emerged as one of the premier applications of Internet-of-Things (IoT) in smart cities. The escalation in the advancement of the Industrial Revolution (IR) 4.0; smart meters have come as a rescue for the electrical and power consumption real-time monitoring. A smart meter is a Cyber-Physical System (CPS) that includes many internet-connected sensors. It is a monitoring and measuring computer with some advanced features when compares with a traditional meter system [1]. The smart meter is a two-way system of information processing and transmission. Furthermore, it connects both the consumer and producers, where consumers can easily control the smart meter according to its usage and requirement. It's an essential part of a smart grid network where production, distribution, transmission, and consumption of electricity is conducted [2].

Moreover, the smart meters are connected with data connectors, utility offices, and meter management system through Local Area Network (LAN), Home Area Network (HAN), Neighborhood Area Network (NAN), and Building Area Network (BAN) [3]. In other words, the whole smart grid network is a modern infrastructure for power generation and distribution that can monitor the user electric consumption and readings at regular intervals. However, currently, the whole existing smart meter technology is facing a huge challenge from cyber-attacks; where outside intrudes have the benefit to add malicious data by adding erroneous values, manipulating the sensor reading, injecting false data etc [4]. In return, it affects the integrity, authentication, confidentiality, availability of the electric data transmission [5]. In the absence of confidentiality in smart meters, data become unauthorized for both consumers and producers.

A smart grid network consists of several smart meters, data collectors, and data connectors. There is also a bi-directional communication between Transmission Substation (TS), Distribution Substation (DS), Gateways (GW), Control Center (CC), NAN, BAN, HAN, and LAN [6]. Therefore, safe mutual authentication is required for secure communication between the clients and the smart meter management system. The smart meter is a part of IoT where devices are interconnected with the internet and can exchange information in a distributed network [7]. But this amalgamation of IoT and smart grid network connected with smart meters bring various opportunities for hackers and cyber-intruders to change the network operation and settings for their monetary benefit which affects both the society and smart cities. IP-based and bi-directional communication between smart meters and inbuilt sensors opens several entry points for cyber-attackers.[8] Here blockchain techniques can play a major role to provide secure communication between different entry points of the smart meter [7].

The blockchain model works in a decentralized manner which helps in maintaining the records of every transaction that occurred between the different places in a distributed network. Mutual authentication and confidentiality can be achieved used blockchain [9]. It also involves various cryptographic operations to encrypt and decrypt the electric data from outside intruders [9]. Next, the inclusion of Fog Computing (FC) with the blockchain model for smart grid further hides and secure the network several entry points from cyber-attackers [8].

FC nodes work in a distributed environment and are placed at the edge of networks close to smart meters and smart grid network. The processing of data is conducted at the fog node where users can communicate and access the data directly in a single hop count from the fog nodes [10]. To achieve the Quality-of-Service (QoS) requirement related to secure communication and to avoid cyber-attacks in smart meter we have proposed a blockchain-based FC system model and Advanced Elliptic Curve Cryptography Digital Signature (AECCDS) algorithm for mutual authentication and identification of malicious data and False Data Injected (FDI) in smart meters.

II. BACKGROUND AND RELATED WORK

In the recent scenario, lots of work has been conducted to compete the challenges related to smart grid and smart meter secure data communication. Some of the latest and existing research works have been highlighted inside this section which will further help the researchers to find the research gaps in terms of communication in smart meter and grids. The listed works are mentioned below.

In [11], the authors proposed a cyber-physical framework for both distributed computation and communication in SG. They further discussed that no work has been conducted to overcome these challenges simultaneously. The framework was based on a real-time simulator. The framework meets the QoS requirement for SG and smart meter by minimizing the data traffic flow, network congestion and queueing delay. This helps to overcome the security challenges developed by cyber intruders and attackers to hack the system.

In [12], the authors proposed an advanced novel system model to identify and rectify the FDI that occurred during the communication with the smart cyber-physical grid and meter network. They have presented a correction model which includes the Jacobian matrix and Taylor's series. Furthermore, a framework was presented for the measurement of data error during communication. The model was able to identify the malicious data and FDI during transmission, distribution and communication in an SG network using LAN, BAN, NAN, and HAN. Similarly, in [13], the authors proposed a novel 3-layered architecture for the interconnection of sensors connected to the internet in smart meter with, consumers, producers and data collectors. Moreover, the architecture was an interconnection mechanism infrastructure for secure connection and communication in a smart grid network using NAN, BAN, and HAN. It provides interoperability, reliability and coupling level in the smart grid network.

In [14], the authors proposed a lightweight security authentication mechanism and a key agreement scheme was proposed to ensure integrity and confidentiality in an SG network. Furthermore, it provides mutual authentication using the SM2 algorithm which helps in avoiding various cyber-attacks such as intrusion inclusion, FDI, malicious data injection, the addition of erroneous values by manipulating the readings of sensors embedded in smart meter and connected with the internet. In [15], the authors proposed an advanced novel lightweight authentication scheme for secure communication using Elliptic Curve Cryptography (ECC) in a smart grid network. The scheme was designed for privacy preservation to avoid cyber-threats on transmitted messages. The work was able to provide safe communication, mutual authentication with a robust connection over the smart grid network Moreover, there was also a session key exchange phase to minimize the communication overhead. The security testing was provided using the BAN-logic and the model was validated using the NS-2simulator.

In [1] the authors conducted in-depth research analysis for cyber-attacks and threats in an SG network. They further discuss the various types of CPS attacks on the SG and smart meter. They highlighted the key points and provided a suggestion to make the network of the SG less vulnerable. A detailed comprehensive survey was presented which was further supported by potential solutions mentioned in their review paper. The paper mainly focused the network vulnerabilities and security requirement. In [16], the authors proposed a novel methodology called Smart Gird Security Classification (SGSC) for SG network security. The methodology was based on the specification of the Advanced Metring Infrastructure (AMI) system. The proposed methodology was linked to risk analysis. The main purpose is to assign the system to a security class based on the score matrix given to the respective protection mechanism. The system worked well in decision making for smart meter and SG.

In [5], the authors designed and developed the concept of attack trees to analyse the path of outsider attacks for intrusion and injection of false data in the smart meter. Next, they have used a game theory approach for modelling the interaction between attackers and defenders. They were able to provide an optimal allocation of security resources in a smart meter network. Similarly, in [17], the authors proposed a double-blockchain assisted secure and anonymous data aggregation scheme using FC nodes deployed at the edge of an SG network. The scheme was able to provide stable and reliable services. Furthermore, they designed a 3-tier architecture-based data aggregation framework by integrating FC and blockchain. The data aggregation mechanism was able to provide a low computational overhead for the SG network.

III. PROPOSED SYSTEM MODEL FOR SMART METER

In this section, we discussed the proposed model for secure communication in the smart meter. See Figure 1 for the advanced blockchain-based model in the FC environment.

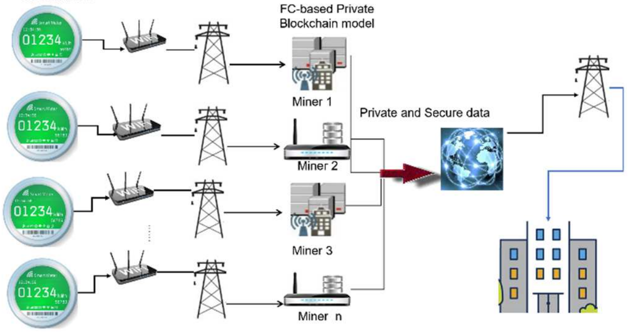

Figure 1: Advanced blockchain-based system model for secure communication

Figure 1 is the proposed system model for secure communication in the smart meter network. It consists of various fog nodes acting as a miner at the edge of smart meters over HAN to record the transaction with the attached timestamp while transmitting the bi-directional data between a smart meter to fog, and the utility office. Electric data is transmitted through data connectors which are further connected to fog nodes. The communication of data is secured inside the fog nodes where data is encrypted using Elliptic Curve Cryptography (ECC) and digital signature. The proposed Advanced Elliptic Curve Cryptography Digital Signature (AECCDS) algorithm is designed and developed to work with fog nodes. Here fog nodes will work in a distributed environment to close the entry points for the outside intruders by acting on HAN, NAN, BAN, and LAN. The system works on cryptographic operations. Once the data is encrypted and secured it can be decrypted by users and the meter management system. In this proposed model no third party is involved in the communication and transmission of electrical data. The user can access the secured data and readings in a single hop count. This will further reduce the overhead cost related to energy and deployment of the system model in the real-world environment. Moreover, the model uses the concept of the distributed system acting at the edge of smart meter networks. Where FC nodes act as a middleware layer along with the decentralized application of blockchain techniques. This makes the SG network much more trustworthy and secure for electric data transmission and communication when compares with the existing model of electric data transmission in smart meters. The existing models are vulnerable to various cyber-attacks and crimes related to the stealing of user information in a Cyber-Physical System (CPS) like smart meters.

IV. NETWORK MODEL

In this section, we discussed the networking model for secure electric data transmission in smart meters, service provider, and trusted authority using the master fog node. See Figure 2 for the networking model.

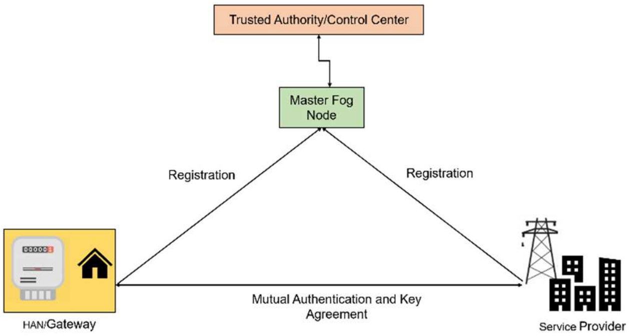
Trusted Authority/Control Center
Master Fog Node
Registration
Registration
Mutual Authentication and Key Agreement
HAN/Gateway
Service Provider

Figure 2: Networking model for the proposed work

The networking model shown in Figure 2 consists of the home-based smart meter with HAN/ gateway, service provider, data connectors, master fog node, and the trusted authority or the Control Centre (CC). Furthermore, there is mutual authentication and key arrangement between the consumers using smart meter and electric power service provider. There is also a registration between the smart meter users and master fog node along with the trusted authority or control centre. The power service provider also has a registration with the master fog node and trusted authority i.e. the control centre to manage the metering system. Here the communication is conducted over a communication channel between the different endpoints such as BAN-gateway and HAN-gateway.

Next, the trusted authority plays the role of creating trust using a CC. The mutual authentication is conducted to authenticate the electric data using the cryptographic operations of blockchain i.e the encryption and decryption with public-private key arrangement along with an inclusion of digital signature and ECC in master fog node. The fog node further registers the request to authenticate the smart meters and service providers by working as middleware and acting as miners. The master fog node makes the final decision on the authenticity, confidentiality, identity, and integrity of electric data sent by smart meters, and service providers through HAN, NAN, BAN, and LAN. However, the real-world implementation of the blockchain-based smart meter system in the FC environment with sensors and actuators is still in infancy many theories have been suggested and given earlier but they are unable to meet the QoS requirement for secure communication in the SG network. The proposed system model and novel AECCDS algorithm were able to minimize the packet error during electric data transmission. The future work requires the real-world implementation of the proposed advanced system model for the SG network.

V. PROPOSED ADVANCED ELLIPTIC CURVE CRYPTOGRAPHY DIGITAL SIGNATURE (AECCDS)

In this section, we discussed the proposed advanced novel AECCDS algorithm. The algorithm works in an FC environment for secure electric data transmission in smart meters using ECC and digital signature. A ring-based signature is used to select from a pool of public keys which further helps in making the electric data identification. The digital signature is designed using the Hash and private key. Asymmetric public-private key pairs are also used in the development of an algorithm. And at the last signatures are mixed to form a Ring. The algorithm uses the Diffie-Hellman method for the exchange of key among different smart meter devices and nodes. ECC based point multiplication is applied for SG services to achieve better performance along with a central point. Furthermore, the algorithm is implemented using a hybrid of Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature (ECDS) techniques for secure communication in smart meters.

Symbol Notations

$ASYM_E$: Asymmetric encryption
A_{PUB_K}: Asymmetric public key
A_{PRVT_K}: Asymmetric private key
C_T: Ciphertext
C_K : Cipher key
C_S: Cloud server
$C(\,x, y)$: C is the chosen point with x and y as coordinates
D_f : Data format

d: Decryption

e: Encryption

E_{dp} : Electric data packet

E_{dpa}: Electric data packet allocation

E_{ds} : Electric data set

$ECDH$: Elliptic Curve Diffie-Hellman

$ECDS$: Elliptic Curve Digital Signature

FC_n: Fog computing nodes

F_s : Fog server

FC_nPRVT_K : Fog node private key

FC_nPUB_K : Public key of the fog node

G: Generator point

H_c : Hash code

k: Key

K_{sym} : Symmetric key

M : Miners

$PRVT_K$: Private key

PUB_K : Public key

S_{mu} : Smart meter users

S_m : Smart meter

S_{md} : Smart meter data

S_mPUB_K : Smart meter public key

$SPRVT_K$: Signed private key

$SPUB_K$: Signed public key

SYM_E : Symmetric encryption

T_s : Timestamp

U_O : Utility Office

V: Value

Algorithm Steps:

Requirement: E_{dp}, S_m , FC_n, and C_s devices.

Step 1: Random value selection.

Step 2: FC-based blockchain system creation.

Step 3: Electric data classification.

Step 4: Next, electric data packet allocation, E_{dPa} at FC_n using a private blockchain.

Step 5: FC_n are used to store the electric data packet, E_{dp}.

Step 6: A timestamp T_s is attached to the block of E_{dp}.

Step 7: S_m send the E_{dp} to FC_n using ledgers.

Step 8: FC_n allocates the E_{dp}.

Step 9: Next to perform E_{dpa} and mining at the individual FC_n.

Step 10: Generation of keys.

Step 11: Start of encryption process using a hybrid technique of ECDH and ECDS technique.

Step 12: S_m sends a key K and E_{dp} to the FC_n.

Step 13: FC_n verifies the key K.

Step 14: Generation of digital signature and use of Diffie-Hellman key exchanges.

Step 15: Generate the H_C.

Step 16: Next, send the H_C to FC_n acting as miners, M.

Step 17: Next, start the decryption process.

Step 18: FC_n status is checked.

Step 19: Verification of S_m and FC_n.

AECCDS Algorithm:

Input: E_{dp} is the electric data packet and S_mPUB_K, the public key of the smart meter. Fog node private key, FC_nPRVT_K $C(x,y)$, where C is the chosen point, and E_{ds} is the electrical dataset.

Output: Decrypted E_{dp}

```
START
$FC_n$ <- $[FC_nPRVT_K].S_mPUB_K$
Return ($FC_{nx}$)
Choose random value $V[1,....n-1]$
$C <- [V].G$
$FC_n$ <- [V]. $S_mPUB_K$
(FC-based blockchain system is created)
Data classification
if ($S_m = Unauthorized\ electric\ data$) then
get geo-location and send the data for verification to $FC_n$ using $SPARK$
else if ($S_m == Authorized\ electric\ data$)
then
$E_{dp}$ send to $FC_n$ to $C_s$
end if
$FC_n$ allocates the $E_{dp}$ to $F_s$
for each $E_{dp}$ do ( $S_m <- C_T$)
    $C_T + T_s$ <- $E_{dp}$
    if $F_s$ == Available then
        allocate the $E_{dp}$
            else no allocation
    end if
end
function Encryption ($E_{dp}$ )
    if $S_m$ confirms $E_{dP}$ storage over blockchain then
        Generate a $K_{sym}$
        $C <- SYM_E(E_{dp}, K_{sym})$
        $C_k <- ASYM_E(K_{sym}, FC_nPUB_K)$
        e <- ($FC_{nx}$* Decimal ($E_{dp}$) modulo $S_mPUB_K$
Return (e, C)
        else
    do no operation
    end if
end function
function SIGNATURE ($E_{dp}$ )
    if the user chose anonymity over blockchain then
            Generate an asymmetric public-private key pair ($A_{PUB_K}, A_{PRVT_K}$)
            $H_c$ <- Estimate hash of $E_{dp}$
Design the digital signature using the $H_c$ and signed private key $SPRVT_K$
Share the public key $SPUB_K$ to the $FC_n$ and receiver using Diffie-Hellman key exchanges
Mix the signature with other $FC_n$ and devices to form a ring
        else
    no operation
    end if
end function
function $DECRYPTION$ (C, $C_k$, $FC_nPRVT_K$, $K_{sym}$)
    $K_{sym} < -Decryption_{Asym}(C_k, FC_nPRVT_K)$
    $E_{dp}$ $< - Decryption$ (C, $K_{sym}$)
    d < – (e * (${FC_{nx}}^{-1}$) modulo $S_mPUB_K$
Return ($E_{dp}$)
end function
END
```

VI. RESULTS AND DISCUSSION

In this section, we discussed the results and simulation of the AECCDS algorithm in the iFogSim Simulator. Next, we have used Anaconda (Python), Geth version 1.9.25, Ganache, Truffle (Compile) and ATOM as a text editor for creating smart contracts. The algorithm usage the elliptic curve cryptography and ring-based digital signature for secure electric data transmission. Moreover, the time complexity of the proposed AECCDS 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 AECCDS algorithm is $T(C) = O(N)^2 + O(N)^3$.

We have used iFogSim software which 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 [18, 19]. It is a Graphical User Interface (GUI) based on an open-source platform for fog-based simulation. Next Geth version 1.9.25 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. 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, the 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^{TM} i9-8750H
CPU	5.30 GHz
RAM	32GB
System Type	64-bit Windows 10
Platform	iFogSim, Ganache, Truffle, ATOM and Spyder
Language	Java and Python

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

See Figure 3 represent the 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 with sensors and actuators.

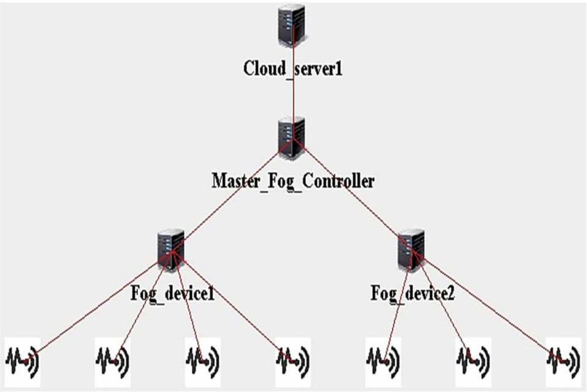

Figure 3: GUI configuration

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

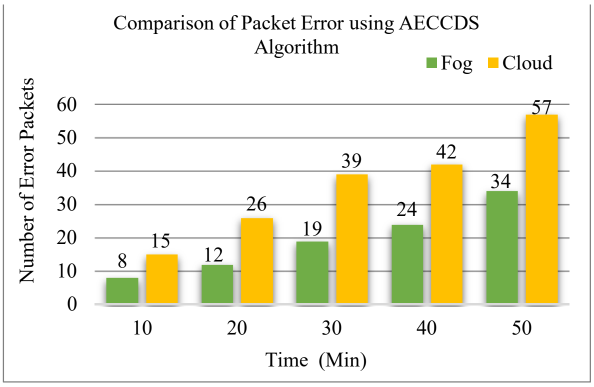

Figure 4: Comparison of packet error

Figure 4 shows the comparisons of packet error using the AECCDS algorithm between fog nodes and cloud servers at different time intervals. Furthermore, 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.

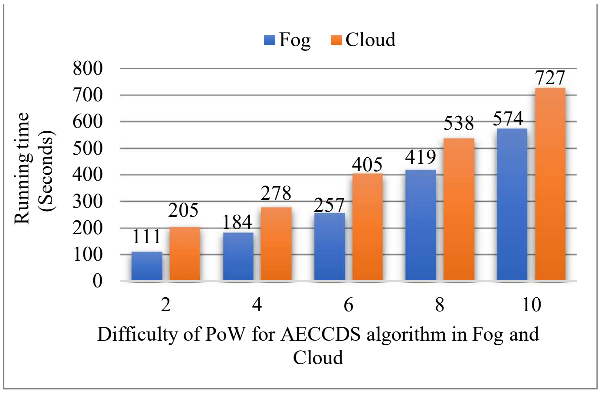

Figure 5: Running time of AECCDS algorithm for PoW with the difficulty level

Figure 5 shows the running time of the AECCDS algorithm for Proof of Work (PoW) with varying difficulty level in fog and cloud. The figure shows that the difficulty level in fog nodes is much lesser when compared to the cloud.

The proposed AECCDS algorithm in the FC environment easily outperforms the cloud when compares to packet error and running time for PoW with the varying difficulty level in Figures 4 and 5.

VII. CONCLUSION

SG network has a major role to play in smart cities. The energy and power are generated, transmitted, distributed, and at last, consumed at the site of smart meter users. With the advancement in technology and Industrial Revolution (IR) 4.0, the SG network becomes vulnerable to outside hackers and cyber-physical attacks. The complexity of the SG system makes it vulnerable to outside attackers.

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. Next, we have proposed a novel AECCDS algorithm that uses the technique of ECC and ring-based digital signature in an FC environment using a blockchain model. The algorithm was able to secure the electrical data transmission in the SG network. The future work includes the evaluation of performance metrics, comparison, and benchmarking with other existing state of the art techniques and related work. Furthermore, future works also require enhancing the proposed system model using a mathematical framework for verification.

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 also 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] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer networks, vol. 169, p. 107094, 2020.

[2] M. B. Mollah et al., "Blockchain for future smart grid: A comprehensive survey," IEEE Internet of Things Journal, 2020.

[3] R. Moghaddass and J. Wang, "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data," IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 5820-5830, 2017.

[4] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," IEEE Systems Journal, 2019.

[5] S.-Z. Liu, Y.-F. Li, and Z. Yang, "Modelling of cyber-attacks and defenses in local metering system," Energy Procedia, vol. 145, pp. 421-426, 2018.

[6] M. Forcan and M. Maksimović, "Cloud-fog-based approach for smart grid monitoring," Simulation Modelling Practice and Theory, vol. 101, p. 101988, 2020.

[7] S. Misra, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan, "Blockchain at the edge: Performance of resource-constrained IoT networks," IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 1, pp. 174-183, 2020.

[8] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," Journal of Information Security and Applications, vol. 52, p. 102500, 2020.

[9] Y. Yang, M. Liu, Q. Zhou, H. Zhou, and R. Wang, "A Blockchain Based Data Monitoring and Sharing Approach for Smart Grids," IEEE Access, 2019.

[10] M. Goudarzi, H. Wu, M. S. Palaniswami, and R. Buyya, "An application placement technique for concurrent iot applications in edge and fog computing environments," IEEE Transactions on Mobile Computing, 2020.

[11] C. Gavriluta, C. Boudinet, F. Kupzog, A. Gomez-Exposito, and R. Caire, "Cyber-physical framework for emulating distributed control systems in smart grids," International Journal of Electrical Power & Energy Systems, vol. 114, p. 105375, 2020.

[12] T. Zou, A. S. Bretas, C. Ruben, S. C. Dhulipala, and N. Bretas, "Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks," Electric Power Systems Research, vol. 187, p. 106490, 2020.

[13] C. Alcaraz, J. E. Rubio, and J. Lopez, "Blockchain-assisted access for federated Smart Grid domains: Coupling and features," Journal of Parallel and Distributed Computing, vol. 144, pp. 124-135, 2020.

[14] K. Wu, R. Cheng, W. Cui, and W. Li, "A lightweight SM2-based security authentication scheme for smart grids," Alexandria Engineering Journal, vol. 60, no. 1, pp. 435-446, 2021.

[15] D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography," Journal of Systems Architecture, p. 101938, 2020.

[16] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A methodology for security classification applied to smart grid infrastructures," International Journal of Critical Infrastructure Protection, vol. 28, p. 100342, 2020.

[17] S. Chen, L. Yang, C. Zhao, V. Varadarajan, and K. Wang, "Double-blockchain Assisted Secure and Anonymous Data Aggregation for Fog-enabled Smart Grid," Engineering, 2020.

[18] S. Shukla, M. F. Hassan, M. K. Khan, L. T. Jung, and A. Awang, "An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment," PloS one, vol. 14, no. 11, p. e0224934, 2019.

[19] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments," Software: Practice and Experience, vol. 47, no. 9, pp. 1275-1296, 2017.