https://doi.org/10.51483/IJCCR.2.1.2022.12-18

ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal
of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper

Open Access

Anomaly Detection to Counter DDoS Attacks on Smart Electric Meter Systems

Mohammed. I. Ibrahim[1*], Abeer Salawi[1], Salwa. H. Alghamdi[1], Nada Alkenani[1], Amani Almuntashiri[1], Rawan Alghamdi[1], Yusra Abdullah[1], Amal Ali[1], Wejdan Ahmed Alghamdi[1], and Maram Alkhayyal[2]

[1]College of Computer Science and Information Technology, Department of Engineering and Computer Sciences, Al-Baha University, Saudi Arabia. E-mail: mialmushilah@bu.edu.sa, [AbeerSalawi87@gmail.com, 442021118@stu.bu.edu.sa, 442020945@stu.bu.edu.sa, 442020162@stu.bu.edu.sa, 442020136@stu.bu.edu.sa, 442021272@stu.bu.edu.sa, 442020295@stu.bu.edu.sa]

[2]College of Computer and Information Sciences, Department of Information Systems, King Saud University, Saudi Arabia. E-mail: wejdanalghamdi18@gmail.com

Article Info

Volume 2, Issue 1, June 2022

Received : 01 March 2022

Accepted : 25 May 2022

Published : 05 June 2022

doi: 10.51483/IJCCR.2.1.2022.12-18

Abstract

Bidirectional communication infrastructure of smart systems, such as, smart grids, are vulnerable to network attacks like Distributed Denial of Services (DDoS) and can be a major concern in the present competitive market. In DDoS attack, multiple compromised nodes in a communication network flood connection request, bogus data packets or incoming messages to targets like database servers, resulting in denial of services for legitimate users. Recently, machine learning based techniques have been explored by researchers to secure the network from DDoS attacks. Under different attack scenarios on a system, measurements can be observed either in an online manner or batch mode and can be used to build predictive learning systems. In this paper, a hybrid deep learning model is developed for detecting replay and DDoS attacks in a real-life smart city platform. The performance of the proposed hybrid model is evaluated using real life smart city datasets (environmental, smart river and smart soil), where DDoS and replay attacks were simulated. The proposed model reported high accuracy rates: 98.37% for the environmental dataset, 98.13% for the smart river dataset, and 99.51% for the smart soil dataset. The results demonstrated an improved performance of the proposed model over other machine learning and deep learning models from the literature.

Keywords: *Internet of Things, Deep learning, Cyber security, DDoS attack detection, Replay attack, Smart grid*

1. Introduction

Anomaly detection targets on normal behaviors, instead of attack behaviors. Firstly, these types of systems define what comprises a normal behavior which is normally carried out by an automated training and then intrusion activities are flagged that differ from this normal behavior by a specified threshold. Second, smart grid is an electrical supply network that combines an existing power network with modern information technologies to respond more efficiently to the needs and distribution of energy. It offers several novel features that include bi-directional communication, remote controlling

* *Corresponding author: Mohammed. I. Ibrahim, College of Computer Science and Information Technology, Department of Engineering and Computer Sciences, Al-Baha University, Saudi Arabia. Email: mialmushilah@bu.edu.sa*

of smart home appliances, updates about consumer behavior and keeping track of power grid's stability. Such novel features need integration of new services and devices as well as new standards and protocols for effective and simplified operation. However, the incorporation of all these standards and devices increases the complexity and vulnerability of the smart grid to security threats. Particularly, the bidirectional and software-oriented nature of the smart grid makes it very prone to cyber-attacks. A cyber-attack can have a significant impact on the whole grid that eventually will affect society, therefore, strict security measures are required to safeguard the grid. As a result, cybersecurity in the smart grid has become one of the most important research problems recently.

2. Research Question

Can deep learning methodologies be applied on DDoS attack prediction in smart electric meter systems and outperform the desired accuracy prediction?

2.1. Importance of the Study

The growth of the use of IoT devices, along with the aforementioned issues, have formed an ideal environment for malicious users to commit various cyber-attacks. These attacks may violate users' privacy, aim for economical profit, or just aim to disrupt the normal operation of underlying systems and services. Some of the most significant IoT related cyber-attacks, observed recently, were DDoS attacks. The rise of IoT computing has practically provided the means to enlarge existing DDoS attacks, which were previously committed using normal desktop computers or servers. During September, 2016, a DDoS attack was launched against Brian Krebs' website, the magnitude of which was larger than that of any other previous similar attempt. The attack was conducted by a botnet, composed of approximately one million devices, most of which were Internet Protocol (IP) cameras. In a later stage, the source code of Mirai the botnet that was employed during the attack against the Krebs website, was released and the simple principle upon which Mirai is based was revealed. It scans the internet for accessible devices protected by factory-default usernames and passwords, and it takes control of these devices, in order to form the botnet network. The Mirai attack has brought into daylight the important security implications of IoT computing and the fact that insecure devices, with default credentials, are exposed to the internet in masses.

3. Research Objectives

No attack is insignificant, even the tiniest strike might result in disastrous consequences. And if it is DDoS attack that is a common problem for almost all smart grid systems, the problem becomes more valuable and urgent to solve since there is a security issue that in concerning the users. In this study we will be examining the solution to these attacks via suggested methodologies by researchers.

Her are the key outcomes of our study:

- The application of deep learning models for detecting replay and DDoS attacks in smart city.
- The experimental evaluation is conducted on a real-life smart city dataset.
- Proposed a deep hyper model to improve attack detection accuracy.
- Handle the low number of features introduced in the datasets.
- Consider the time factor in the detection process.

4. Background

To interrupt the normal safe operation of a power grid or gain financial advantage, cyber attackers target different elements of cyber resiliency to manipulate the data being communicated for power system operation and control. These elements include data confidentiality, data integrity, and data availability. Several prevention methods have been implemented and investigated by researchers to protect the network devices and databases from cyber intruders. For an instant, Suo *et al.* (2012) investigated the latest cyber-attack prevention technologies inclusively protecting sensor data, communicational devices security using encryption mechanisms and cryptographic algorithms. Ahanger (2018) classified cyber-attacks into two groups, naming, direct and indirect cyber-attacks and further sub-categorized the direct cyber-attacks into four sub-groups. Among them, data intrusion attacks are considered as the most common group of cyber-attacks and its most significant attack type is Denial of Services (DoS). In these attacks, to disrupt the normal trend of services, the adversary introduces artificial loads to the main service source and causes disruptions to the normal legitimate service. Most current DoS attacks are distributed DDoS where attackers initiate attack from several adversaries simultaneously. Thus, detection and prevention of attack from one node will not stop the attack and make it more complicated to differentiate between legitimate and artificial service requests. To enhance the security of the smart grid, DDoS attacks can be detected by analyzing the patterns of network data. Automatic analysis and detection methods enable in time response and preventive measures which can significantly reduce the damage. However, automatic prediction of DDoS attacks is a challenging problem. The accuracy of a DDoS attack prediction is the most critical factor for timely prevention of the attacks. To enhance the accuracy, the prediction system must learn important features from the network packets in an efficient manner. This challenge can be tackled by employing multiple learning models to enhance the prediction accuracy. However, this introduces another challenge of the automatic unification of multiple learning models.

5. Literature Review

In this Section, there is a review of pertinent literature on DDoS attack detection in smart grid networks using machine learning techniques. Most of the previous methods use shallow learning techniques or a combination of linear and non-linear methods to achieve better results. For example, Ali and Li (2019) classified DDoS attacks using supervised machine learning technique including Random Forests (RF), K-Nearest Neighbors (KNN) and Support Vector Machines (SVM). Tufail *et al.* (2021) gather attacker information by introducing honeypots in Advance Metering Infrastructure (AMI) of the smart grid network and analyzes the interaction between attacker and defender using Bayesian-Nash equilibrium to apply defense strategy accordingly. Ghali *et al*. (2021) prevent and mitigate DDoS attack impacts by reducing data computational burden of AMI using a firewall integrated with the cloud computing-based processing method. Srikantha and Kundur (2015) proposed a collaborative reputation topology configuration based on the auto-healing method for the stability of the overall power network, while one node of the network is under attack. Varalakshmi and Selvi (2013) detects and discards false malicious requests using information divergence scheme.

Specifically used machine learning algorithms for DDoS attack detection are Artificial Neural Networks (ANN), K-nearest neighbor, Support Vector Machine (SVM), decision tree and Naive Bayes. Generally, first, filtered network data is stored in a database. Next, the normalization of extracted features from the stored dataset for a stable training process by machine learning algorithms is achieved. In the end, this trained model is used with data packets of a real-time network for the classification of DDoS attacked and legitimate packets for further processing. Kumar and Selvakumar (2011) used multiple back propagation models for basic results. *Q*-statistics techniques along with Weighted Majority Voting and Weighted Product Rule are used for selecting best back.

For a comparative evaluation, different machine and deep learning models from the literature are selected to compare their performance to the hybrid proposed model. All models explained in the following subsections use SoftMax activation function in their output layer. For all models used for the comparative study alongside with the proposed hybrid model, Adam algorithm is used to optimize weights of the models using cross entropy loss function. In addition to the selected models from the literature, the deep CNN part of the proposed hybrid model is used without applying the RBM part. The reason behind this is to verify our hypothesis that the RBM model contributes to enhance the overall accuracy of the hybrid model. We called the deep CNN part of the proposed model, Deep Convolutional Neural Network (DCNN). The Multi-Layer Perceptron (MLP) is a feed forward neural network with an input layer, one hidden layer, and an output layer. Rectified linear unit activation function is used in the hidden layer units. The hidden and output layers are proceeded by a dropout operation. Deep Multi-Layer Perceptron (DMLP) is a fully connected feed forward model with four layers in total, including the input layer. The three hidden layers applies rectified linear activation function. Each hidden layer and the output layer are proceeded by a dropout operation.

Furthermore, existing literature studies have not focused on data exfiltration caused by DDoS attacks. There is an inadequate clear explanation of the existing methodology of the problem mentioned above. In contrast, the existing literature focuses on the general idea of DDoS attacks.

To address the cybersecurity aspects of smart grid, various approaches have been suggested in the literature, and as the complexity and integration of Artificial Intelligence (AI) increases, more research studies on ways to make the grid more reliable will be conducted. Some research studies also show that the smart grid is also prone to human error, and those errors can be due to social engineering attacks. DDoS attacks with an impact on the user's communication with the sensors have not yet been reported in the literature.

6. Challenges in Data Visualizations

Detecting anomalies on a consumer network has its own set of challenges:

- Lack of data points: Consumer networks do not have subnets containing hundreds of devices generating a multitude of traffic over various protocols which can be analyzed for patterns. For example: In a typical work environment, one can monitor traffic on the DC analyzing user login data or the average overall bandwidth use whose patterns correlate work hours, which cannot be done on a typical consumer network.

- Unavailability of Public Datasets: For commercial networks, publicly available labeled datasets with millions of records and attack types have been made available for research purposes. There has also been work done on the quality of such datasets. However, consumer network data have not been collected or published for privacy reasons.
- Lack of Infrastructure: There are not managed switches or routers with monitoring capabilities in a consumer network. In such networks, packet capturing tools need to be installed on users' computers or a low power device like a Raspberry Pi must be installed on the network to monitor the network.

7. Suggested Methodology

7.1. The Proposed Hybrid Deep Learning Network

Recently, machine learning, specifically deep learning, has been shown to be very effective at detecting cyber-attacks in smart cities. Although simulating cyber-attacks on a real smart city dataset to use it as a benchmark is not a trivial task, our proposed model is developed to detect intrusions using a real dataset with complicated distributions. The proposed model is a hybrid deep learning model, which combines a deep Restricted Boltzmann Machine (RBM) model with a deep Convolutional Neural Network (CNN) model. The RBM part of the proposed model plays an important part in learning high level features from the dataset to provide much better representation of the dataset. The RBM model can overcome the small number of input features and to model the underlying dataset distribution without the need for the associated classes. The deep CNN part of the proposed model is then trained in supervised mode derived by the associated classes. CNN is not only performing the classification task, but it is also learning the local invariance filters that detect local features from input signals.

7.2. Algorithm

In this section, the proposed hybrid deep learning model for replay and DDoS attacks detection is described. A flowchart of the proposed detection model in the context of smart city is shown below (Figure 1). The proposed model consists of an input layer, deep RBM model with two hidden layers, deep CNN with seven hidden layers, a Global Average Pooling (GAP) layer, and a SoftMax output layer. In the next subsections, each step of the proposed hybrid model is explained in detail.

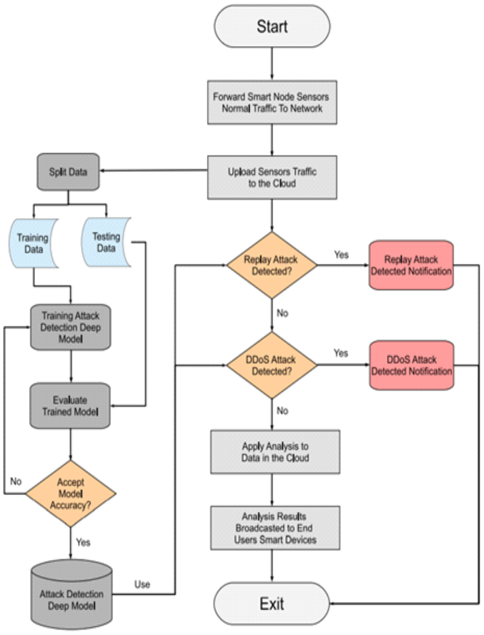
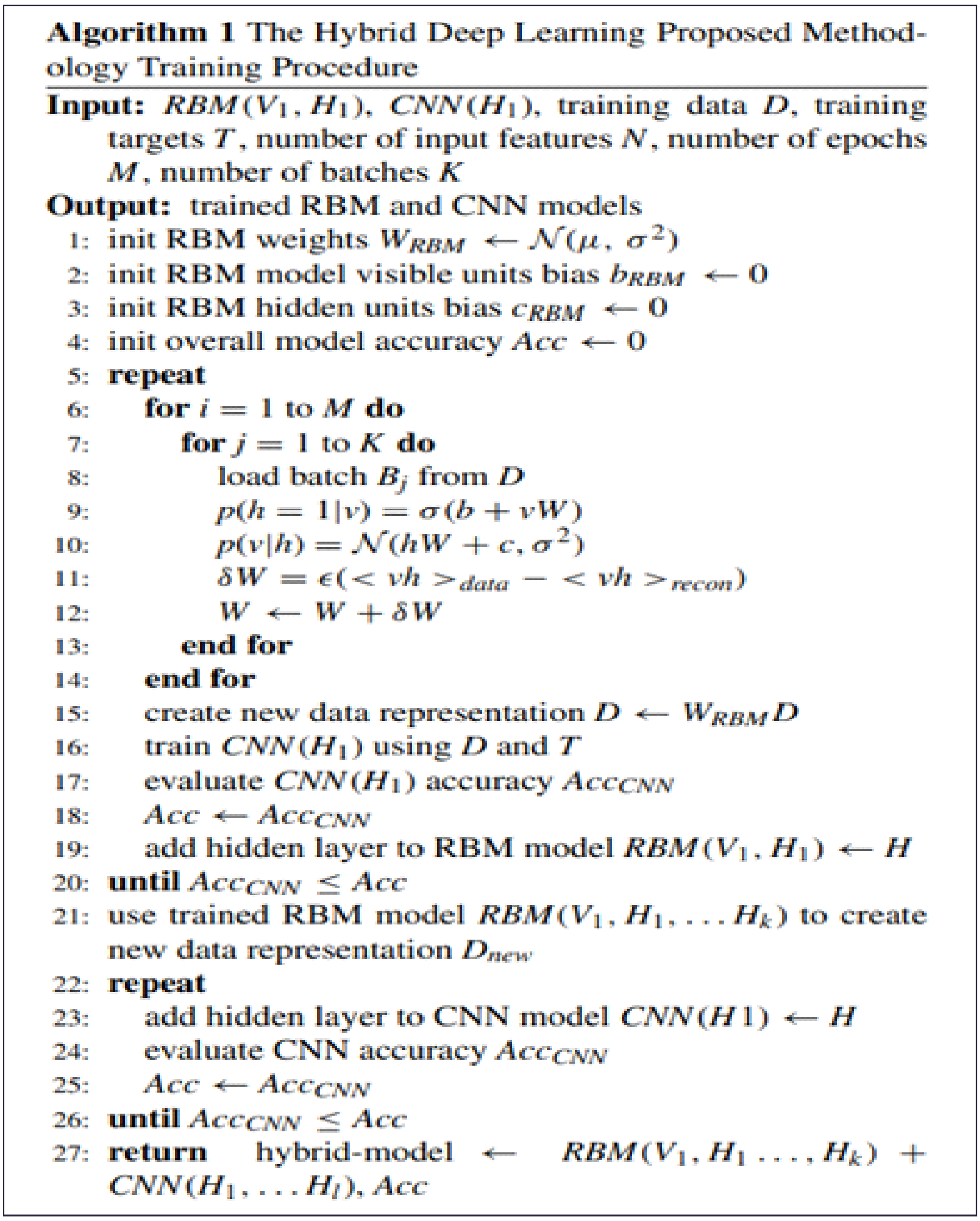

Start
Forward Smart Node Sensors Normal Traffic To Network
Upload Sensors Traffic to the Cloud
Split Data
Training Data
Testing Data
Training Attack Detection Deep Model
Evaluate Trained Model
No
Accept Model Accuracy?
Yes
Attack Detection Deep Model
Use
Replay Attack Detected?
Yes
Replay Attack Detected Notification
No
DDoS Attack Detected?
Yes
DDoS Attack Detected Notification
No
Apply Analysis to Data in the Cloud
Analysis Results Broadcasted to End Users Smart Devices
Exit

Figure 1: Algorithm 1 Describes the Training Procedure for the Proposed Hybrid Model

The inputs are the dataset with its associated classes, an initial RBM model with one hidden layer, an initial CNN model with one hidden layer, maximum number of epochs and number of batches to divide the dataset. Initially, we fixed the CNN model with one hidden layer in order to evaluate the RBM model until we determined the best number of hidden layers to use. The initial RBM model is trained for a maximum number of epochs and batches, then used to create a new data representation. This new data representation is used to train the initial CNN model with one hidden layer to calculate the classification accuracy. If the classification accuracy is getting better, an additional hidden layer is added to the RBM model. Given this new updated RBM model, the training process for RBM is repeated until no further enhancement is introduced to the classification accuracy. The next part of the training procedure is to build the CNN model toward enhancing the overall classification accuracy. The CNN model is trained using the new data representation from the latest RBM deep model. The same incremental approach is used to add more hidden layers to the CNN model, while the classification accuracy is enhancing. When no further improvement in classification accuracy, the training is stopped and the trained hybrid RBM+CNN model and its overall accuracy are recorded.



Algorithm 1 The Hybrid Deep Learning Proposed Methodology Training Procedure

```
Input: $RBM(V_1, H_1)$, $CNN(H_1)$, training data $D$, training
    targets $T$, number of input features $N$, number of epochs
    $M$, number of batches $K$
Output: trained RBM and CNN models
init RBM weights $W_{RBM} \leftarrow \mathcal{N}(\mu, \sigma^2)$
init RBM model visible units bias $b_{RBM} \leftarrow 0$
init RBM hidden units bias $c_{RBM} \leftarrow 0$
init overall model accuracy $Acc \leftarrow 0$
repeat
    for $i = 1$ to $M$ do
        for $j = 1$ to $K$ do
            load batch $B_j$ from $D$
            $p(h = 1|v) = \sigma(b + vW)$
            $p(v|h) = \mathcal{N}(hW + c, \sigma^2)$
            $\delta W = \epsilon(< vh >_{data} - < vh >_{recon})$
            $W \leftarrow W + \delta W$
        end for
    end for
    create new data representation $D \leftarrow W_{RBM} D$
    train $CNN(H_1)$ using $D$ and $T$
    evaluate $CNN(H_1)$ accuracy $Acc_{CNN}$
    $Acc \leftarrow Acc_{CNN}$
    add hidden layer to RBM model $RBM(V_1, H_1) \leftarrow H$
until $Acc_{CNN} \leq Acc$
use trained RBM model $RBM(V_1, H_1, \ldots H_k)$ to create
    new data representation $D_{new}$
repeat
    add hidden layer to CNN model $CNN(H1) \leftarrow H$
    evaluate CNN accuracy $Acc_{CNN}$
    $Acc \leftarrow Acc_{CNN}$
until $Acc_{CNN} \leq Acc$
return hybrid-model $\leftarrow$ $RBM(V_1, H_1 \ldots, H_k)$ +
    $CNN(H_1, \ldots H_l)$, $Acc$
```

As a result, the proposed model reported high accuracy rates: 98.37% for the environmental dataset, 98.13% for the smart river dataset, and 99.51% for the smart soil dataset. The results demonstrated an improved performance of the proposed model over other machine learning and deep learning models from the literature.

8. Conclusion

In the last years, IoT has undergone various attacks by intruders because of the poor design of methods for mitigating malicious attacks such as DDoS. Additionally, the lack of robust security protection has motivated intruders to perform a series of attacks on the IoT network and its devices. These attacks lead to data exfiltration and financial losses. The study performs a rigorous investigation and further proposes a robust framework that withstands the cybersecurity attacks of DDoS in the IoT environment. The study believes that the proposed solution can also help future researchers to tackle the expansion of data exfiltration caused by DDoS attacks in the IoT environment. The hybrid deep learning model proposed in this paper for replay and DDoS attacks detection contributes to the field of securing smart city infrastructure and services. The performance of the proposed methodology in this paper was evaluated by synthetically generating replay and DDoS attack data. Attack data was generated from real-life normal behavior recorded in the smart city of Queanbeyan, Australia. The performance of the proposed methodology was compared with machine and deep learning models from the literature. The experimental results showed that our proposed model outperforms all other models with high detection accuracy. The experimental results showed the importance of the RBM part of the proposed model. It overcomes the small number of features, and the complicated probability distributions presented in the datasets. The reported results showed a significant enhancement to the proposed methodology by adding the RBM part, compared to the results obtained from the deep CNN part of the proposed methodology applied alone. Modeling the river dataset was more complicated than other datasets due to the small number of data instances and the complicated probability distributions.

9. Future Work

Numerous difficulties occur from numerous attacks on the security of smart grid systems, as the smart grid's safety requirements and objectives are dispersed across large areas. Due to the critical importance of power infrastructure and the socioeconomic impact of blackouts, the smart grid may be a primary target of cyber terrorism. Cyber defense solutions should be used to safeguard all components of smart grid systems. Defensive solutions should incorporate a variety of defense technologies, including machine, proactive IDS/IPS systems, wireless controlled propagation, authorization, authentication, and certification. The solutions should incorporate scalable, resilient, and adaptive cybersecurity/defense approaches for intelligent grid operations that do not jeopardize genuine smart grid operations.

References

Ali, S. and Li, Y. (2019). Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network. in *IEEE Access*, 7, 108647-108659, 2019, doi: 10.1109/ACCESS.2019.2933304.

Ahanger, T. (2018). Defense Scheme to Protect IoT from Cyber Attacks using AI Principles. *International Journal of Computers Communications & Control, 13*(6), 915-926. Retrieved from http://univagora.ro/jour/index.php/ijccc/article/view/3356

Ghali, A.A., Ahmad, R. and Alhussian, H. (2021). A Framework for Mitigating DDoS and DOS Attacks in IoT Environment Using Hybrid Approach. *Electronics*, 10(11), 1282.

Huraj, L., Šimon, M. and Horák, T. (2020). Resistance of IoT Sensors Against DDoS Attack in Smart Home Environment. *Sensors*, 20(18), 5298, https://doi.org/10.3390/s2018529.

Magaia, N., Fonseca, R., Muhammad, K., Segundo, A.H.F.N., Neto, A.V. L. and de Albuquerque, V.H.C. (2020). Industrial Internet-of-Things Security Enhanced with Deep Learning Approaches for Smart Cities. *IEEE Internet of Things Journal, 8*(8), 6393-6405.

Patel, D., Srinivasan, K., Chang, C.Y., Gupta, T. and Kataria, A. (2020). Network Anomaly Detection Inside Consumer Networks—A Hybrid Approach. *Electronics*, 9(6), 923.

Shitharth, S. and Winston, D. (2015). A Comparative Analysis Between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network. *Procedia Technology*, 21, doi: 10.1016/j.protcy.2015.10.086.

Spathoulas, G., Giachoudis, N., Damiris, G.P. and Theodoridis, G. (2019). Collaborative Blockchain-Based Detection of Distributed Denial of Service Attacks Based on Internet of Things Botnets. *Future Internet*, 11(11), 226.

Tufail, S., Parvez, I., Batool, S. and Sarwat, A. (2021). A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies*, 14(18), 5894.

Cite this article as: Mohammed. I. Ibrahim, Abeer Salawi, Salwa. H. Alghamdi, Nada Alkenani, Amani Almuntashiri, Rawan Alghamdi, Yusra Abdullah, Amal Ali, Wejdan Ahmed Alghamdi, and Maram Alkhayyal. (2022). Anomaly Detection to Counter DDoS Attacks on Smart Electric Meter Systems. *International Journal of Cryptocurrency Research,* 2(1), 12-18. doi: 10.51483 / IJCCR.2.1.2022.12-18.