Computers, Materials & Continua
DOI: 10.32604/cmc.2022.024794
Article

Tech Science Press

Intelligent Deep Learning Model for Privacy Preserving IIoT on 6G Environment

Anwer Mustafa Hilal[1,*], Jaber S. Alzahrani[2], Ibrahim Abunadi[3], Nadhem Nemri[4], Fahd N. Al-Wesabi[5,6], Abdelwahed Motwakel[1], Ishfaq Yaseen[1] and Abu Sarwar Zamani[1]

[1]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj, 16278, Saudi Arabia
[2]Department of Industrial Engineering, College of Engineering at Alqunfudah, Umm Al-Qura University, Saudi Arabia
[3]Department of Information Systems, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[4]Department of Information Systems, King King Khalid University, Muhayel Aseer, 62529, Saudi Arabia
[5]Department of Computer Science, King King Khalid University, Muhayel Aseer, 62529, Saudi Arabia
[6]Faculty of Computer and IT, Sana'a University, Sana'a, 61101, Yemen
*Corresponding Author: Anwer Mustafa Hilal. Email: a.hilal@psau.edu.sa
Received: 31 October 2021; Accepted: 20 December 2021

Abstract: In recent times, Industrial Internet of Things (IIoT) experiences a high risk of cyber attacks which needs to be resolved. Blockchain technology can be incorporated into IIoT system to help the entrepreneurs realize Industry 4.0 by overcoming such cyber attacks. Although blockchain-based IIoT network renders a significant support and meet the service requirements of next generation network, the performance arrived at, in existing studies still needs improvement. In this scenario, the current research paper develops a new Privacy-Preserving Blockchain with Deep Learning model for Industrial IoT (PPBDL-IIoT) on 6G environment. The proposed PPBDL-IIoT technique aims at identifying the existence of intrusions in network. Further, PPBDL-IIoT technique also involves the design of Chaos Game Optimization (CGO) with Bidirectional Gated Recurrent Neural Network (BiGRNN) technique for both detection and classification of intrusions in the network. Besides, CGO technique is applied to fine tune the hyperparameters in BiGRNN model. CGO algorithm is applied to optimally adjust the learning rate, epoch count, and weight decay so as to considerably improve the intrusion detection performance of BiGRNN model. Moreover, Blockchain enabled Integrity Check (BEIC) scheme is also introduced to avoid the misrouting attacks that tamper the OpenFlow rules of SDN-based IIoT system. The performance of the proposed PPBDL-IIoT methodology was validated using Industrial Control System Cyber-attack (ICSCA) dataset and the outcomes were analysed under various measures. The experimental results highlight the supremacy of the presented PPBDL-IIoT technique than the recent state-of-the-art techniques with the higher accuracy of 91.50%.

Keywords: 6G networks; industrial iot; blockchain; security; intrusion detection; artificial intelligence

1 Introduction

The advancements made in industries, especially large-scale, in recent years have been rapid in the areas of surveillance, transportation, security, and factory automation. In this scenario, Industrial IoT (IIoT) [1] has drawn a considerable attention by integrating dense wireless devices like Radio Frequency Identification (RFID) tags [2] to identify the machines and sensor nodes for fault diagnosis, asset monitoring, large scale equipment monitoring, manufacturing, production, and other such applications for water supplies, power plants, gas, and oil refineries. Industrial Control System (ICS) is employed to describe distinct systems like Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). SCADA analyses and collects the data from substations on a real-time basis. All substations have control devices such as Intelligent Electronic Device (IED), Remote Terminal Unit (RTU) and Programmable Logic Controller (PLC) that handle field devices, for instance, meters, actuators, sensors, etc.

Having been considered as a fundamental enabler of Industry 4.0 and a developing offshoot of IoT, Industrial IoT (IIoT) systems are being rapidly deployed in numerous social and commercial fields like manufacturing, retail, pervasive monitoring, logistics, home automation, security surveillance, and healthcare [3]. Furthermore, with astonishing advancements made in sensor network technologies and wireless communications, considerable number of devices are being presented to IIoT environment in which the raw data is processed and captured locally for data-driven decision-making process. This device has the potential to interact and communicate with one another, process and share the data and is independent of human interference [4]. Hence, these devices should be safeguarded enough to preserve the data integrity and guarantee computing reliability and resource availability. Blockchain technologies introduced a novel model for the next-generation transaction-based applications, alongside a shared and distributed private or public ledger and a collective consensus method that enables accountability, trust, and transparency in the network. Fig. 1 illustrates the evolution of 1G-6G.

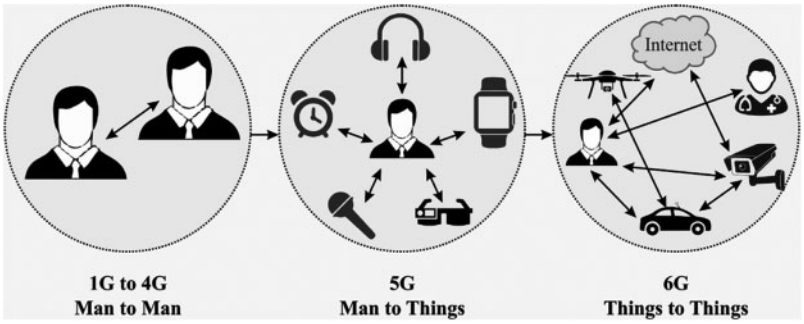

Figure 1: Evolution of 1G-6G

Blockchain technique is transparent in nature owing to which it has been emphasized by the research community and industries as a possible solution to manage huge IIoT networks in an effective manner [5]. Furthermore, trust-less network architectures and decentralized IIoT devices are anticipated to perform a significant part in the development of IIoT networks. These networks treat the data locally, from where it is generated and not in a centralized way. Also, it can enable device connectivity and create trustless data storage via sensors and devices which could function independent of central authorities. Also, a secured framework is generally provided by a blockchain i.e., strong against single point of failure [6]. Since decentralized networks have several entry points, it adheres to fault tolerance and resilience of the network. Besides, IIoT infrastructure could be highly available with the help of distributed ledger technology.

IIoT system is highly vulnerable and gets exposed to numerous security attacks, for instance, Distributed Denial-of-Service (DDoS) and Denial-of-Service (DoS). This attack could incur a significant loss for IIoT service and smart environmental application in the IIoT system. As a result, it becomes inevitable to protect the IIoT system from all types of cyber attacks [1]. Intrusion Detection System (IDS) is a security system that mostly functions in the network layers of IIoT system. When IDS is installed in an IIoT network, it should be capable of analysing the data packets and produce the responses on a real-time basis. Furthermore, it should analyse the data packets present in distinct layers of IIoT system using distinct protocol stacks and adapt to different techniques used in IIoT framework [7]. An IDS i.e., developed for IIoT-based smart environment, must function under stringent conditions in terms of fast response, high volume data processing, and low-processing capability. Hence, traditional IDS mayn't be adequate to meet the needs of IIoT environment. IIoT security is a serious and continuous problem that needs to be addressed with priority; therefore, it becomes an inevitable need to have a clear and current understanding of security susceptibilities in IIoT systems and the growth of respective mitigation methods. Though blockchain and artificial intelligence are known to exhibit numerous advantages, they still have their own share of disadvantages too. Blockchain has a problem with scalability, energy consumption, privacy, efficiency, and security whereas AI overcomes a few problems like effectiveness and interpretability. Though both techniques are distinct areas of research, it could be associated with one another so as to have the advantage of natural incorporation. These two techniques have common requirements for security, trust, and data analysis due to which one could authorize the other.

The current research paper develops a new Privacy Preserving Blockchain with Deep Learning model for Industrial IoT (PPBDL-IIoT) on 6G environment in order to identify the presence of intrusions in network. PPBDL-IIoT technique incorporates Chaos Game Optimization (CGO) with Bidirectional Gated Recurrent Neural Network (BiGRNN) technique for detection and classification of intrusions in the network. Additionally, CGO algorithm is applied in fine tuning the hyperparameters of BiGRNN model too. Furthermore, Blockchain Enabled Integrity Check (BEIC) scheme is introduced to avoid the misrouting attacks that tamper the OpenFlow rules of SDN-based IIoT system. For validating the supremacy of the proposed PPBDL-IIoT technique, a series of simulations was executed on ICSCA dataset and the outcomes were discussed under distinct parameters.

The paper is structured in the following. Section 2 shows a comprehensive review of security based solutions for IIoT environment and Section 3 elaborates the detailed processes involved in the proposed model. Next, Section 4 shows a brief experimental validation process and Section 5 draws the conclusion.

2 Related Works

Derhab et al. [8] proposed a security framework in which SDN and blockchain techniques are incorporated. The presented method was made up of an IDS scheme that integrates RSL and KNN algorithms to defend against the forged command and BICS so that the misrouting attacks can be avoided. Rahmadika et al. [9] proposed a smart system incorporating 5G edge network, FL, and blockchain technology so as to generate an effective and secured architecture for performing transaction. FL allows the UE to train AI paradigm without revealing the beneficial data of UEs to either model or the public provider. The recorded transaction could not be maliciously changed or in other words, they remain the same. Further, the researcher also proposed few dynamic verification protocols to UE for the purpose of interacting with different BSs. In addition to this, blockchain was also employed as a rewarding method in FL to allow the computation offloading in wireless networks.

Qu et al. [10] proposed an architecture that is composed of BCS, layers, and intersect. In this novel structure, every BCS is configured using blockchain technique. The authors described about the credibility authentication approach in this study and also showed how it can authenticate the procedure. Further, security analyses was conducted to test the efficiency based on authentication, response time, and storage efficacy. Alkadi et al. [11] proposed the development of a DBF to provide security-based distributed IDS and security-based blockchain with the help of an intelligent contract in IoT network. IDS scheme makes use of BiLSTM DL method to handle consecutive network data and is measured by BoT-IoT and UNSW-NB15 datasets. Both privacy-based blockchain and smart contracts method were a result of Ethereum library and it aims at providing privacy to the distributed IDS.

Ferrag et al. [12] proposed a new DL and blockchain-based energy structure i.e., enabled DeepCoin for Smart Networks. DeepCoin structure employs two systems such as a DL based and blockchain based systems. The blockchain-based system includes five stages such as agreement, setup, view change, consensus making phases, and creating a block. It integrates a new consistent peer-to-peer energy scheme i.e., depending on real-time Byzantine fault-tolerance approach. Further, the method attains a high throughput. In Guha Roy et al. [13], a decentralized security method was proposed with the incorporation of an SDN using blockchain for IoT in fog computing and mobile edges. Here, SDN repeatedly analyses and monitors the traffic system to render an attack detection method. Blockchain was employed in this study to overcome the problems faced in the present model. This was done so, by sending the decentralized attack detection system that identifies attacks in fog and decreases the same in edge node.

Skwarek [14] proposed an approach for IoT devices to attain industry-grade consistency in data transfer from WSN to production system via blockchain technology. It is possible to obtain improved reliability and security of the acquired data within sensor networks on application levels. Hence, a lightweight, higher-level transmission protocol, depending on blockchain technology, has been developed in this study. Blockchain mechanisms could protect the wireless transmission of IoT in a scalable, lightweight model. Lee et al. [15] proposed a novel method that leverages the distributed watchdog using blockchain system in defending the software supply chain. Furthermore, the researchers introduced a set of thorough specifications to determine the behavior of system in a clear manner and employ module checking.

3 The Proposed Model

The current study presented a new framework for ICS that allows network virtualization by transferring the control layer to cloud so that a centralized management is enabled. The proposed PPBDL-IIoT technique is a two-stage process namely intrusion detection and BEIC. For a long known time, WAN is generally considered as complex and costly only. The proposed framework decreases the network cost by providing zero-touch placement, viz., it is not necessary to construct the network device by plugging it in. Rather, the devices are constructed from SDN controller. The presented framework is made up of the modules discussed herewith.

Private cloud: It hosts every component that provides a central control for ICS alike VMs such as SDN controller, SCADA, and DCS servers.

IP network: Rather than employing a devoted WAN to replace the ICS, public internet connections are used among SDN and distinct substations. Every device is validated and end-to-end encryptions are performed through networks.

SDN controller: It can be considered as an application that handles the flow control with the help of protocols like OpenFlow. In this setup, the switches are used for the transmission of data packets. Open Flow protocol is a southbound interface amongst the forwarding and controller mechanisms like switches. Here, the northbound interface assumes the communication amongst the applications and controller.

Virtual Switch: It can be an application that interconnects different VMs of different/same hypervisor(s). Furthermore, it interconnects the VMs with other physical switch.

3.1 Design of Intrusion Detection Technique

In intrusion detection process, CGO-BiGRNN technique is applied to determine the occurrence of intrusions in the network. Multilayer RNNs are amongst one of the generally utilized techniques in DL. These kinds of networks are capable of memorizing the realized data. Further, RNN is a powerful technique for sequential data (time series) analysis. It utilizes the preceding output to predict the next output. These loops i.e., hidden neurons allow one to save the preceding input data. But, the model is forecasted based on the future output. The hidden layer outcome is retransmitted for t times to the hidden layer [16]. Then the output becomes complete and the preceding data is retained for too long. Eventually, the errors are returned back for updating the weight. During this case, four obtainable RNN structures are utilized.

Simple RNN is fundamentally a group of general NNs which have the same task to accomplish i.e., transfer the message from one node to another. Specifically, this is a memory network that saves knowledge on the data server. However, its memory is short-term and could not continue as a long-term time series. A simple recurrent network is the one internal memory$-h_t-$ calculated through Eq. (1):

$$h_t = g(Wx_t + U_f h_{t-1} + b) \tag{1}$$

where $g()$ refers to activation function, U and W denote the variables in the weight matrices of h layer, b represents the bias and X signifies the input vector.

GRU is an easy LSTM, proposed by Cho et al. [17]. The difference with LSTM is that GRU combines both input as well as output gates and upgrades the same. The output value of h_t in GRU is calculated as follows.

$$z_t = \sigma(W_z X_t + U_z h_{t-1} + b_z) \tag{2}$$

$$r_t = \sigma(W_r X_t + U_r h_{t-1} + b_r) \tag{3}$$

$$\widetilde{h_t} = \tanh(W_h X_t + (r_t * h) U_h) \tag{4}$$

$$h_t = (1 - z_t) * h_{t-1} + z_t * \widetilde{h_t} \tag{5}$$

where r implies reset gate, and z represents the upgrade gate. Reset gate represents the integration of novel input with earlier memory. An upgrade gate also represents the retention of the preceding memory. When the update gate is one, the preceding memory gets completely preserved. When it can be zero, the preceding memory goes totally forgotten. There is a forget gate in LSTM which manually defines the preceding memory as continuous. But in case of GRU, every preceding memory is either

preserved or entirely forgotten. Though GRU can be compared with LSTMs in terms of efficiency, it requires low memory.

Bi-directional framework methods have the capability of learning data from preceding and following data, if the current data is managed well. Fig. 2 illustrates the framework of GRU technique. BiGRNN method has been defined as a dependent method that relies upon the state of two unidirectional and oppositely-placed GRUs [18]. This allows the data in both future as well as past to impact the current state. *bi*-GRU is determined as follows.

$$\overrightarrow{h_t} = GRU_{fwd}(x_t, \overrightarrow{h_{t-1}})$$

$$\overleftarrow{h_t} = GRU_{bwd}(x_t, \overleftarrow{h_{t+1}}) \tag{6}$$

$$h_t = \overrightarrow{h_t} \oplus \overleftarrow{h_t}$$

where $\overrightarrow{h_t}$ implies the condition of forwarding GRU, $\overleftarrow{h_t}$ refers to backward GRU, $\oplus$ defines the function of concatenating two vectors.

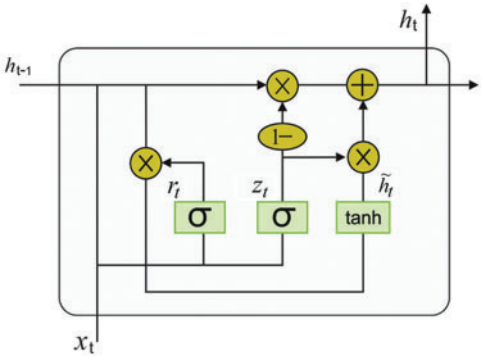

Figure 2: GRU structure

In order to fine tune the hyperparameters of BiGRNN technique, CGO algorithm is applied. The key concept of CGO algorithm is depending on chaos theory, in which the fractals are configured by using chaos game concept. The theory of chaos game is used as the key principle behind CGO algorithm method. A quantity of solution candidates (X), represent the seed, is considered as CGO approach. Every (X) candidate solution includes a few tuneable variables (X) which represent the location of the seed. The triangle of Sierpinski is assumed as the exploration fields on the lookout for solution. The mathematical form for the above scenario is represented herewith.

$$X = \begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_i \\ \vdots \\ X_n \end{bmatrix} = \begin{bmatrix} x_1^1 & x_1^2 & \cdots & x_1^j x_2^j & \cdots & x_1^d \\ x_2^1 & x_2^2 & \cdots & \vdots & \cdots & x_2^d \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_i^1 & x_i^2 & \cdots & x_i^j & \cdots & x_2^d \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n^1 & x_n^2 & \cdots & x_n^j & \cdots & x_n^d \end{bmatrix}, \begin{cases} i = 1, 2, \ldots, n. \\ i = 1, 2, \ldots, d. \end{cases} \tag{7}$$

In which n denotes the population size of exploration, whereas d indicates dimensional problem. The seed is randomly initialized by [19]

$$x_i^j(0) = x_{i,\min}^j + rand.(x_{i,\max}^j - x_{i,\min}^j), \begin{cases} i = 1, 2, \ldots, n. \\ i = 1, 2, \ldots, d. \end{cases} \tag{8}$$

where $x_i^j(0)$ represent the first population, $x_{i,\min}^j$ and $x_{i,\max}^j$ indicates min. and max. values of *jth* dimension, and rand represent an arbitrary value in the range of zero and one. To finalise the structure of a triangle, the arithmetical method makes distinct seeds in their upper and lower bounds. A temporary triangle using three seeds are shown below.

- The Global Best (GB) established until now;
- The Mean Group (MGi) is the mean value of arbitrary seed;
- The ith solution candidate (X_j).

The vertices of the triangle are X_j. *GB*, and MGi A temporary triangle is created for every first seed so that it can produce novel seed to finish a novel triangle. The ith iteration comprises 3 corners of a Sierpinski triangle and the seed attained in prior iterations. For novel seed, the temporary triangle is employed and the dice is again rolled. The seeds in X_i are transferred to GB or MGi based on the resultant colour. It can be modelled by an arbitrary integer value. It creates two integers i.e., zero/one, that allows the selection of green or red faces. As per the chaos game, seed motion must be minimum. in this regard, some of the factorials generated, are employed. The determined procedure for the initial seed can be mathematically expressed as

$$Seed_i^1 = X_i + \alpha_i \times (\beta_i \times GB - \gamma_i \times MG_i),\ i = 1, 2, \ldots, n \tag{9}$$

whereas X_i denotes *ith* candidate, α_i signifies an arbitrary factorial that restricts the motion of seeds, and β_j and γ_j denotes arbitrary integers of zero/one to represent the probabilities of rolling some dice. The dice of three red and blue faces are employed to the succeeding seeds (GB). The dice is rolled while the GB is moved to X_i or *MGi*, based on the resultant colour. The seed move to the X_i, once a blue face is attained; when red face is attained, the seeds move to *MGi*. The 2nd seeds go toward a point on linking lines among X_i & *MGi*. It can be expressed mathematically by

$$Seed_i^2 = GB + \alpha_i \times (\beta_i \times X_i - \gamma_i \times MG_i),\ i = 1, 2, \ldots, n \tag{10}$$

Based on the 3rd seeds, the dice is rolled. As per the resultant colour, the seed move to X_i or *GB*, that generates 2 integrals i.e., zero and one. As per the certain factor, the seed travel to the connected lines among X_i & GB can be formulated by

$$Seed_i^3 = MG_i + \alpha_i \times (\beta_i \times X_j - \gamma_i \times GB),\ i = 1, 2, \ldots, n \tag{11}$$

Also, alternative technique is employed for creating the 4th seed to present a mutation step in the position update of seeds. The position is modified according to specific changes in the chosen decision. The arithmetical expression for the abovementioned procedure can be given in the following.

$$Seed_i^4 = X_i(x_i^k = x_i^k + R),\ k = [1, 2, \ldots, d] \tag{12}$$

whereas k denotes an arbitrary integer among 1 & d, as well as R signifies the range of arbitrary value between zero and one.

The four distinct formulations for α_i that control the movement limitation of the grain are proposed herewith to change and monitor the exploitation and exploration rates of CGO method.

$$\alpha_i = (x_i^k = x_i^k + R) \begin{cases} Rand \\ 2 \times Rand \\ (\delta \times Rand) + 1 \\ (\varepsilon \times Rand) + (\sim \varepsilon) \end{cases} \tag{13}$$

where Rand denotes a random number in the range of zero and one, as well as δ & ε represent arbitrary factors among [0, 1].

The fitness of novel candidate is related to the existing one and higher fitness are saved. In the meantime, the candidate with lower fitness gets rejected.

3.2 Design of BEIC Scheme

Blockchain is a kind of chain formation that integrates data blocks in a sequential order. It is non-forgeable, tamper-proof distributed ledger that is assured by cryptography. Each blockchain participant maintains the data for blockchain node. Hence, every data in blockchain is open and transparent. When the data is published, it is retained permanently and could not be tampered with. Tamper-proof and open authentication features of the blockchain enable one to perform as a trusted 3rd parties for addressing the concern of a user in Cloud Computing (CC) platform. Each result could be released to blockchain for verification and can be retained by every user in the blockchain. Thus, when blockchain is incorporated in CC environment, it benefits by resolving the drawbacks of CC platform and could increase the efficiency of services to users with high data security.

Being a significant model of Bitcoin and a decentralized database, blockchain serves as a primary framework of Bitcoin simultaneously. A blockchain is a sequence of data blocks that are produced with the help of cryptography. Fig. 3 illustrates the block diagram of blockchain technology. Every block has data about bitcoin network transaction which is employed to verify the validity of the data and produce succeeding blocks. In other terms, blockchain is a chained data structure that successively integrates data blocks based on time series. Being a distributed ledger, it could not be forged through or tampered with cryptography. Blockchain technologies, in general, use blockchain data structure to store and verify the information. Further, it employs distributed node consensus to update and generate the information. In addition, it also employs cryptography for the purpose of data access and transmission. It also employs smart contract, made up of automatic script code, for programming and data manipulation purposes. Blockchain contains few features such as immutability, decentralization, collective maintenance, traceability, transparency, and openness. This characteristic ensures the transparency and honesty of blockchain and lays the basis for blockchain to create trust. Blockchain-rich application scenario depends on the fact that blockchain could resolve data asymmetry and attain concerted action and collaborative trust amongst different subjects.

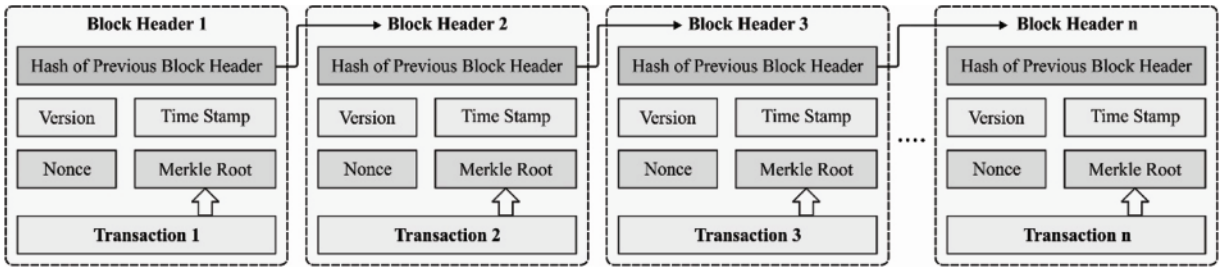

Figure 3: Framework of blockchain

Before determining the security solutions, some assumptions are to be made.

- Consider that ICS isn't compromised (viz., free from malicious codes prior to the installation of BEIC scheme). Or else, forged rule could be deliberated as legitimate.
- BEIC scheme focuses only on southbound transmission. Consider that the northbound communications are secure between DCS and SCADA servers and IDSs from one side as well as SDN controllers from another side.
- Consider that SDN controllers are placed in a private cloud and are available from an individual host using access control and authentication method.

Blockchain [20] is an essential component in the proposed integrity checking system. The fundamental concept is to offer a solution in which every flow rule that can be produced from the controller, is saved in immutable and verifiable databases. Blockchain is a series of blocks i.e., connected with hash values. In blockchain networks, every user contains: single public key signifies its exclusive address and single private key to sign the blockchain transactions. After authenticating the transmission blocks, the transaction is processed and then added to the blockchain. After recording, the data in the provided blocks could not be altered without changing every succeeding block. Additionally, the data exist in several hosts in a gradual manner. So, any modifications will be denied by hosts of the peers. In this study, a private (or permission) blockchain is presented. Therefore, consensus methods like Proof of Work are not essential herewith. This blockchain is made up of SDN firewall and controller. SDN controllers create the block and share it with firewall through blockchain. The initial nodes have full permission, viz., to send, read, and write, whereas the firewall could only receive and read. The BEIC systems are brought in the succeeding series.

- Once the requests are received from northbound applications, the SDN controllers are developed to transmit the respective flow rules to vSwitches. In this model, SDN controllers are also considered as members of a blockchain. It hashes the flow rule and places it in block i.e., dispersed to another node of the blockchain. The SDN controllers are the node in blockchain that had the authority to construct a block whereas the remaining nodes could only read the blockchain.
- Once the flow rule reaches vSwitch nodes, save the rule in record files and latter upgrades its flow table.
- The firewall gathers the vSwitch log and access the BlockChain for obtaining the flow rules, transmitted through the controller.
- When the firewall detects the 2 rules that are present in blockchain and vSwitch, it informs the management to take a proper counter measure for fixing this mismatch.

4 Performance Validation

The present subsection validates the efficiency of the proposed PPBDL-IIoT technique against benchmark dataset [21]. In this study, binary and multi-class datasets were considered for simulation purposes. The dataset has 128 attributes in total. Besides, the binary class dataset has two classes of instances namely, Natural and Attack classes. The binary class dataset has 15 sub-datasets out of which only five sub-datasets are used in the experimentation procedure. Sub-dataset 1 comprises of 1100 instances under natural class and 3866 instances under attack class. Besides, sub-dataset 2 has 1544 instances under natural class and 3525 instances under attack class. Similarly, sub-dataset 3 comprises of 1604 instances under natural class and 3811 instances under attack class. Likewise, sub-dataset 4 comprises of 1800 instances under natural class and 3402 instances under attack class. Lastly, sub-dataset 5 comprises of 1481 instances under natural class and 3680 instances under attack class. On

the other hand, multi-class dataset includes 15 sub-datasets under three categories namely, No event, Natural, and Attack.

Fig. 4 shows the confusion matrix generated by PPBDL-IIoT technique under five sub-datasets present in the binary dataset. The proposed PPBDL-IIoT technique classified data-1 with 1067 instances under natural class and 3834 instances under attack class. Further, PPBDL-IIoT approach classified data-2 with 1488 instances under natural class and 3793 instances under attack class. Besides, PPBDL-IIoT manner classified data-3 with 1541 instances under natural class and 3764 instances under attack class. Additionally, PPBDL-IIoT method has classified data-4 with 1737 instances under natural class and 3350 instances under attack class. Lastly, PPBDL-IIoT algorithm classified data-5 with 1429 instances under natural class and 3642 instances under attack class.

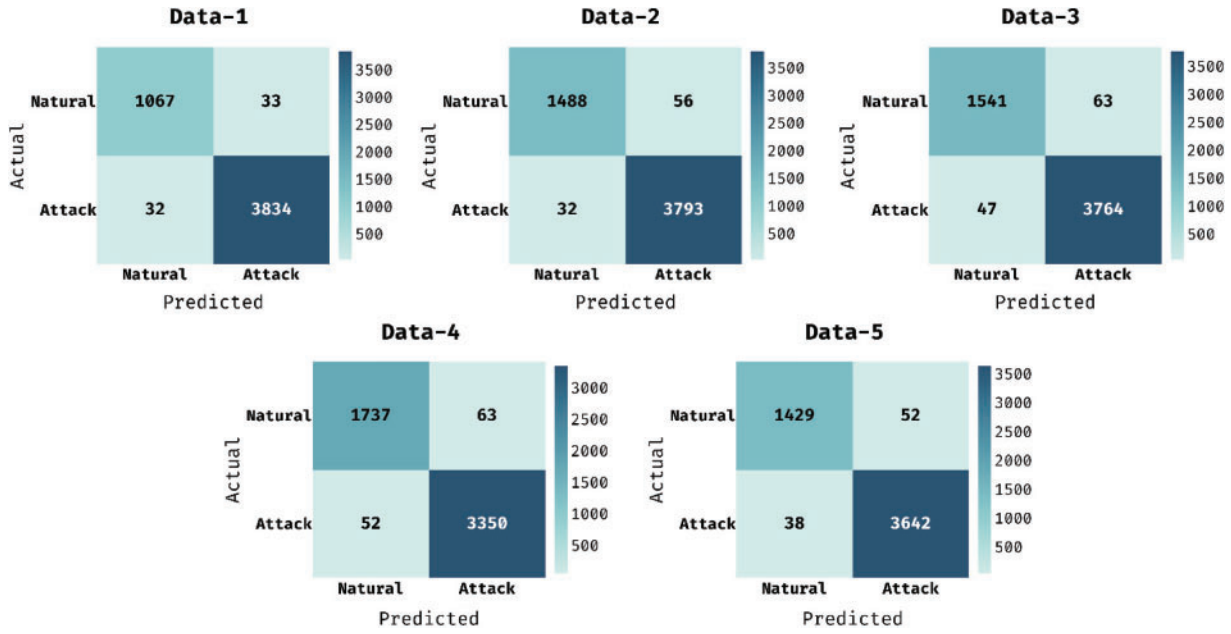

Figure 4: Confusion matrix analysis of PPBDL-IIoT model on binary dataset

Tab. 1 provides the classification results of PPBDL-IIoT technique under different sub-datasets of binary class datasets. The results demonstrate that PPBDL-IIoT technique gained effectual outcomes on the applied sub-datasets. For instance, on the applied data-1, PPBDL-IIoT technique achieved a high precision of 0.971, recall of 0.970, specificity of 0.992, accuracy of 0.987, and F-score of 0.970. Moreover, on the applied data-3, the proposed PPBDL-IIoT method gained a high precision of 0.970, recall of 0.961, specificity of 0.988, accuracy of 0.980, and F-score of 0.966. Furthermore, on the applied data-5, PPBDL-IIoT algorithm accomplished a superior precision of 0.974, recall of 0.965, specificity of 0.990, accuracy of 0.983, and F-score of 0.970.

Fig. 5 demonstrates the results from ROC analysis of PPBDL-IIoT method on the applied binary class dataset. The figure portrays that the proposed PPBDL-IIoT technique produced a high ROC of 99.0933.

Table 1: Results of the analysis of the proposed PPBDL-IIoT model for binary class dataset

Binary dataset	Precision	Recall	Specificity	Accuracy	F-score
Data-1	0.971	0.970	0.992	0.987	0.970
Data-2	0.979	0.964	0.992	0.984	0.971
Data-3	0.970	0.961	0.988	0.980	0.966
Data-4	0.971	0.965	0.985	0.978	0.968
Data-5	0.974	0.965	0.990	0.983	0.970
Average	0.973	0.965	0.989	0.982	0.969

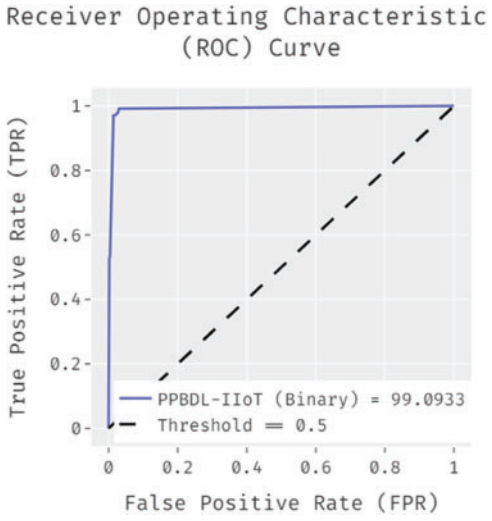

Figure 5: ROC analysis of PPBDL-IIoT model on binary class dataset

Fig. 6 showcases the results of confusion matrices produced by PPBDL-IIoT technique on the applied multi-class dataset. The proposed PPBDL-IIoT technique classified a set of 162 instances into No events class, 3381 instances into Attack class, and 770 instances into Natural class. Meanwhile, PPBDL-IIoT approach classified a set of 312 instances into No events class, 3063 instances into Attack class, and 1038 instances into Natural class. Eventually, the proposed PPBDL-IIoT method classified a set of 338 instances into No events class, 3337 instances into Attack class, and 1080 instances into Natural class. Concurrently, PPBDL-IIoT method classified a set of 391 instances into No events class, 2956 instances into Attack class, and 1182 instances into Natural class. Simultaneously, the proposed PPBDL-IIoT algorithm classified a set of 253 instances into No events class, 3224 instances into Attack class, and 1035 instances into Natural class.

Tab. 2 shows the classification results attained by PPBDL-IIoT approach on the applied multi-class dataset. The proposed PPBDL-IIoT technique obtained the maximum classification performance on the applied sub-datasets. For sample, with data-1, the PPBDL-IIoT technique reached a recall of 0.889, precision of 0.750, specificity of 0.922, accuracy of 0.926, and F-score of 0.761. Likewise, with data-2, PPBDL-IIoT method gained a precision of 0.789, accuracy of 0.927, recall of 0.905, specificity of 0.953, and F-score of 0.833. Similarly, with data-3, PPBDL-IIoT approach obtained a recall of 0.907, precision of 0.828, accuracy of 0.931, specificity of 0.935, and F-score of

0.861. In line with this, for data-4, PPBDL-IIoT algorithm obtained a accuracy of 0.927, recall of 0.905, precision of 0.820, specificity of 0.934, and F-score of 0.839. In line with this, for data-5, the proposed PPBDL-IIoT approach achieved a recall of 0.916, precision of 0.856, accuracy of 0.955, specificity of 0.946, and F-score of 0.873.

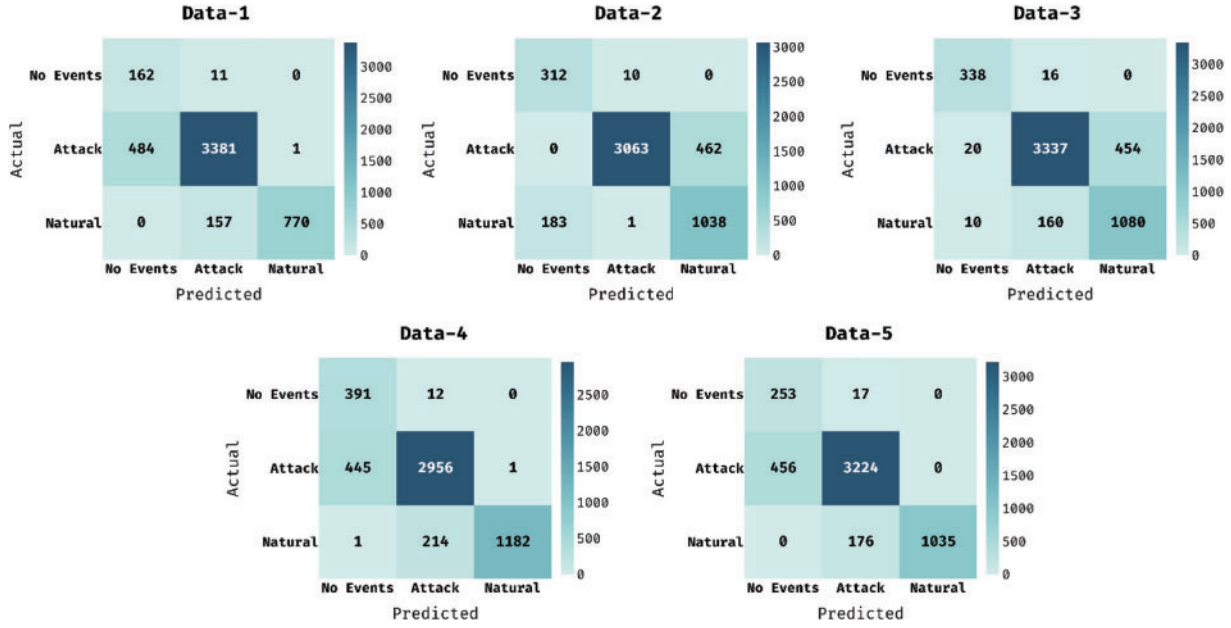

Figure 6: Confusion matrix analysis of PPBDL-IIoT model on multi-class dataset

Table 2: Results analysis of proposed PPBDL-IIoT model on multiclass dataset

Multiclass dataset	Methods	Precision	Recall	Specificity	Accuracy	F-Score
Data-1	No events	0.297	0.936	0.920	0.921	0.451
	Attack	0.954	0.900	0.847	0.889	0.926
	Natural	0.999	0.831	1.000	0.968	0.907
	Average	0.750	0.889	0.922	0.926	0.761
Data-2	No events	0.630	0.969	0.961	0.962	0.764
	Attack	0.997	0.897	0.993	0.926	0.944
	Natural	0.741	0.849	0.906	0.892	0.792
	Average	0.789	0.905	0.953	0.927	0.833
Data-3	No events	0.722	0.955	0.974	0.973	0.822
	Attack	0.951	0.902	0.890	0.898	0.926
	Natural	0.810	0.864	0.939	0.922	0.836
	Average	0.828	0.907	0.935	0.931	0.861
Data-4	No events	0.531	0.970	0.928	0.931	0.686
	Attack	0.931	0.898	0.874	0.890	0.914
	Natural	0.999	0.846	1.000	0.959	0.916
	Average	0.820	0.905	0.934	0.927	0.839

(Continued)

Table 2: Continued

Multiclass dataset	Methods	Precision	Recall	Specificity	Accuracy	F-Score
Data-5	No events	0.619	0.937	0.968	0.967	0.745
	Attack	0.948	0.958	0.870	0.932	0.953
	Natural	1.000	0.855	1.000	0.966	0.922
	Average	0.856	0.916	0.946	0.955	0.873

Fig. 7 exhibits the result of ROC analysis accomplished by PPBDL-IIoT methodology on the employed multi class datasets. The figure exhibits that the proposed PPBDL-IIoT method produced a high ROC of 97.1620.

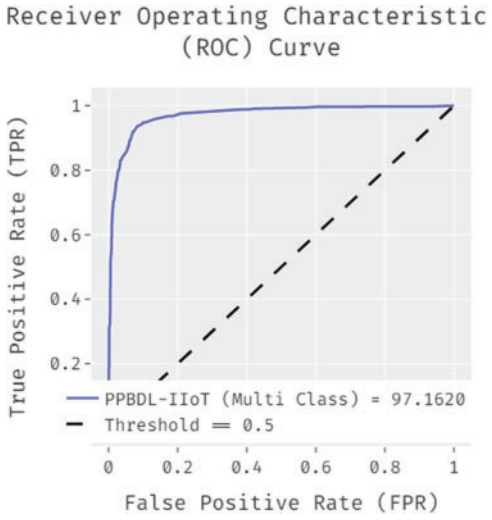

Figure 7: ROC analysis of PPBDL-IIoT model on multi-class dataset

For ensuring the enhanced classification performances of PPBDL-IIoT process, a thorough comparison study was conducted and the results are shown in Tab. 3. Fig. 8 illustrates the results of binary class outcome analysis accomplished by PPBDL-IIoT technique against existing techniques. The figure illustrates that NB-K, BN, and LSVM techniques achieved low performance with its accuracy values being 75.7%, 77.9%, and 78.3% respectively. Along with that, DT and Bagging methods showcased slightly enhanced performance with accuracy values being 92.9% and 92.9% respectively. Moreover, AdaBoostM1, KNN, and RF techniques accomplished moderately reasonable outcomes with its accuracy values being 94.1%, 95.5%, and 96%. However, the proposed PPBDL-IIoT technique produced superior outcomes with a high accuracy of 98.2%.

Table 3: Results analysis of existing with proposed model with respect to accuracy

Methods	Binary class	Multi class
PPBDL-IIoT	98.20	91.50
RF	96.00	79.60
KNN	95.50	87.70
AdaBoostM1	94.10	29.40
DT	92.90	83.20
Bagging	92.90	79.60
LSVM	78.30	30.40
BN	77.90	74.60
NB-K	75.70	19.70

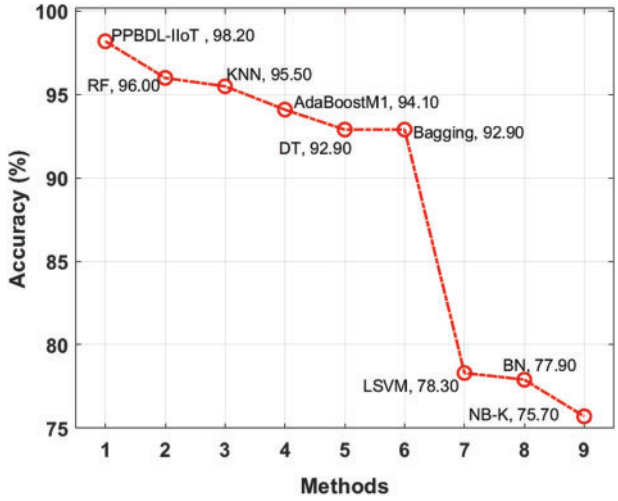

Figure 8: Accuracy analysis of PPBDL-IIoT model on binary class dataset

Fig. 9 depicts the results of multi-class outcome analysis of the proposed PPBDL-IIoT approach against existing methods. The figure demonstrates that NB-K, AdaBoostM1, LSVM, and BN methods achieved less performance with its accuracy values being 19.7%, 29.4%, 30.4%, and 74.6% correspondingly. Likewise, RF and bagging techniques outperformed other techniques and achieved the same accuracy of 79.6%. Followed by, DT and KNN methods accomplished moderately reasonable outcomes with accuracy values such as 83.2% and 87.7%. Eventually, the proposed PPBDL-IIoT method produced a high accuracy of 91.5%.

From the abovementioned figures and tables and respective discussion, it is clear that the proposed PPBDL-IIoT methodology is an appropriate tool to provide security in 6G-enabled IIoT environment.

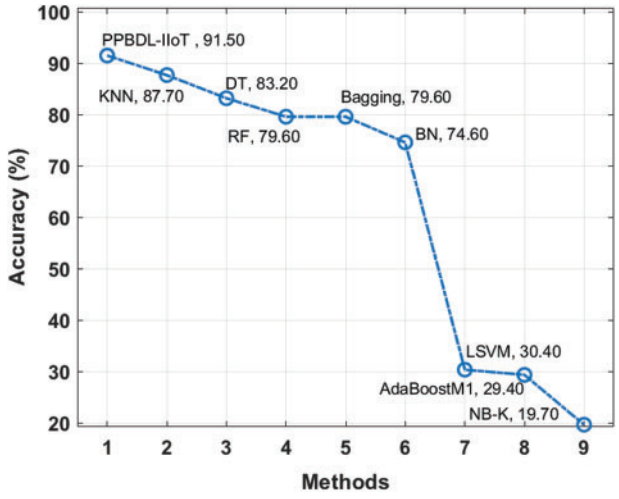

Figure 9: Accuracy analysis of PPBDL-IIoT method on multiclass dataset

5 Conclusion

In current study, a new PPBDL-IIoT technique has been proposed for the detection of intrusions in 6G-enabled IIoT environment. The proposed PPBDL-IIoT technique encompasses a two-stage process namely, intrusion detection and BEIC. DL-based BiGRNN technique with CGO-based hyperparameter optimization is used to detect and classify the intrusions in network. CGO algorithm is applied to optimally adjust the learning rate, epoch count, and weight decay so as to improve the intrusion detection performance of BiGRNN model up to a considerable manner. Moreover, BEIC technique is designed to circumvent the misrouting attacks that tamper the OpenFlow rules of SDN-based IIoT system. For ensuring the supremacy of PPBDL-IIoT technique, a series of simulations was executed on ICSCA dataset. The experimental results highlight the supremacy of PPBDL-IIoT technique over an advanced technique with the higher accuracy of 91.50%. In future, the design of PPBDL-IIoT methodology can be extended further to perform fault diagnosis and power management systems in blockchain-enabled IIoT environment.

Acknowledgement: The authors would like to acknowledge the support of Prince Sultan University, Riyadh, Saudi Arabia for partially supporting this project to paying the Article Processing Charges (APC) of this publication.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP 2/23/42). www.kku.edu.sa.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. D. Xu, W. He and S. Li, "Internet of Things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[2] D. Zuehlke, "SmartFactory—towards a factory-of-things," *Annual Reviews in Control*, vol. 34, no. 1, pp. 129–138, 2010.

[3] A. Shahzad, Y. G. Kim and A. Elgamoudi, "Secure IoT platform for industrial control systems," in *2017 Int. Conf. on Platform Technology and Service (PlatCon)*, Busan, Korea, pp. 1–6, 2017.
[4] H. Farhady, H. Lee and A. Nakao, "Software-defined networking: A survey," *Computer Networks*, vol. 81, pp. 79–95, 2015.
[5] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.
[6] O. Michel and E. Keller, "SDN in wide-area networks: A survey," in *2017 Fourth Int. Conf. on Software Defined Systems (SDS)*, Valencia, Spain, pp. 37–42, 2017.
[7] M. M. Hasan and H. T. Mouftah, "Optimal trust system placement in smart grid SCADA networks," *IEEE Access*, vol. 4, pp. 2907–2919, 2016.
[8] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag *et al.,* "Blockchain and random subspace learning-based ids for sdn-enabled industrial iot security," *Sensors*, vol. 19, no. 14, pp. 3119, 2019.
[9] S. Rahmadika, M. Firdaus, S. Jang and K. -H. Rhee, "Blockchain-enabled 5g edge networks and beyond: An intelligent cross-silo federated learning approach," *Security and Communication Networks*, vol. 2021, pp. 1–14, 2021.
[10] C. Qu, M. Tao, J. Zhang, X. Hong and R. Yuan, "Blockchain based credibility verification method for iot entities," *Security and Communication Networks*, vol. 2018, pp. 1–11, 2018.
[11] O. Alkadi, N. Moustafa, B. Turnbull and K. K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2021.
[12] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1285–1297, 2019.
[13] D. G. Roy and S. N. Srirama, "A blockchain-based cyber-attack detection scheme for decentralized internet of things using software-defined network," *Software: Practice and Experience*, vol. 51, no. 7, pp. 1540–1556, 2021.
[14] V. Skwarek, "Blockchains as security-enabler for industrial IoT-applications," *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, no. 3, pp. 301–311, 2017.
[15] J. Lee and T. Kwon, "Distributed watchdogs based on blockchain for securing industrial internet of things," *Sensors*, vol. 21, no. 13, pp. 4393, 2021.
[16] H. Apaydin, H. Feizi, M. T. Sattari, M. S. Colak, S. Shamshirband *et al.,* "Comparative analysis of recurrent neural network architectures for reservoir inflow forecasting," *Water*, vol. 12, no. 5, pp. 1500, 2020.
[17] K. Cho, B. V. Merrienboer, C. Gulcehre, F. Bougares, H. Schwenk *et al.* "Learning phrase representations using RNN encoder-decoder for statistical machine translation," arXiv preprint, arXiv:1406.1078, 2014.
[18] R. Fu, Z. Zhang and L. Li, "Using LSTM and GRU neural network methods for traffic flow prediction," in *2016 31st Youth Academic Annual Conf. of Chinese Association of Automation (YAC)*, Wuhan, China, pp. 324–328, 2016.
[19] I. Alsaidan, M. A. M. Shaheen, H. M. Hasanien, M. Alaraj and A. S. Alnafisah, "Proton exchange membrane fuel cells modeling using chaos game optimization technique," *Sustainability*, vol. 13, no. 14, pp. 7911, 2021.
[20] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras *et al.,* "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2019.
[21] U. Adhikari, S. Pan and T. Morris, "Dataset": https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets. 2020.