Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 9(4): 8868–8884.
DOI: 10.3934/math.2024432
Received: 06 January 2024
Revised: 08 February 2024
Accepted: 18 February 2024
Published: 04 March 2024

Research article

Ensuring data integrity in deep learning-assisted IoT-Cloud environments: Blockchain-assisted data edge verification with consensus algorithms

Fahad F. Alruwaili*

Department of Computer & Network Engineering, College of Computing & Information Technology, Shaqra University, Shaqra, Saudi Arabia. alruwaili@su.edu.sa

* **Correspondence:** Email: alruwaili@su.edu.sa.

Abstract: Ensuring the reliability and trustworthiness of massive IoT-generated data processed in cloud-based systems is paramount for data integrity in IoT-Cloud platforms. The integration of Blockchain (BC) technology, particularly through BC-assisted data Edge Verification combined with a consensus system, utilizes BC's decentralized and immutable nature to secure data at the IoT network's edge. BC has garnered attention across diverse domains like smart agriculture, intellectual property, and finance, where its security features complement technologies such as SDN, AI, and IoT. The choice of a consensus algorithm in BC plays a crucial role and significantly impacts the overall effectiveness of BC solutions, with considerations including PBFT, PoW, PoS, and Ripple in recent years. In this study, I developed a Football Game Algorithm with Deep learning-based Data Edge Verification with a Consensus Approach (FGADL-DEVCA) for BC assisted IoT-cloud platforms. The major drive of the FGADL-DEVCA algorithm was to incorporate BC technology to enable security in the IoT cloud environment, and the DL model could be applied for fault detection efficiently. In the FGADL-DEVCA technique, the IoT devices encompassed considerable decentralized decision-making abilities for reaching an agreement based on the performance of the intrablock transactions. Besides, the FGADL-DEVCA technique exploited deep autoencoder (DAE) for the recognition and classification of faults in the IoT-cloud platform. To boost the fault detection performance of the DAE approach, the FGADL-DEVCA technique applied FGA-based hyperparameter tuning. The experimental result analysis of the FGADL-DEVCA technique was performed concerning distinct metrics. The experimental values demonstrated the betterment of the FGADL-DEVCA approach with other existing methods concerning various aspects.

Keywords: blockchain; edge verification; fault detection; deep learning; Football Game Algorithm
Mathematics Subject Classification: 11Y40

1. Introduction

Conventional cloud computing (CC) is employed to attain demand-based resource distribution due to its higher scalability and flexibility. With the fast expansion of the Internet of Things (IoTs) over the past few years, the exponential development of data takes great real-time needs for the exchange, processing, and storage of data that are much higher than the carrying ability of standard CC [1].The IoT is a cutting-edge technology that can be created by several researchers. Despite having an extensive of proposals in the present study, the utilization of IoT is not flexible or simple. Among the numerous works to address the restrictions of IoT utilization, major developing solutions are dependent upon service-based techniques [2]. This method reflects some IoT nodes as smart objects, which could be offered widespread services across any network. When this technique is engaged, the developers can acquire the flexibility of considering the level of services and data than the devices and communication network. Therefore, it will efficiently overcome the problems of IoT utilization, being consistent, flexible, effective, and comparatively simple [3]. With the constant expansion of blockchain (BC) technology, it started to be progressively implemented in stocks and bonds in the financial domain. In transactions, persons introduce "smart contracts" via programs and methods, and implement BC technology to ensure the dependability and integrity of financial transactions [4].

In the existing phase of development, BC technology has come into a time of fast development of technologies like artificial intelligence (AI), and big data has used modifications in Internet technology, and the IoT solution of the autonomous self-assembled network is steadily entered into all phases of social interactions [5]. The link between the IoTs and advanced technologies, namely big data and AI, is continuously developing. The major features of BC can be stated, such as computational logic, irreversibility of records, allocated database, transparency with pseudonymity, and peer-to-peer (P2P) communication, safeguarding access to new data after being accessible through the network. Employing BC can ensure that the data cannot be removed or updated unintentionally [6]. Confidentiality, security, and privacy to the IoT networks provide reliance, and BC is deliberated inherent security technology. This provides solutions to resolve several challenges that occur in conventional allocated database systems. The hack-proof form of BC offers security features for information generated by IoT devices [7]. Mining of the most extensively employed consensus technique, like PoW, is an energy consumption method [8]. Consensus methods have been employed by BC for validating transactions and providing data integrity [9]. Therefore, with an integration of the two, such as BC technology and microservice, it is possible to design and utilize robust independent and protective microservices. Although this sounds promising, safeguarding cyber security comes in the form of a real-life difficulty [10]. Since the reliance on cyber connections is improving, the possible effect of cyberattacks must be significantly large such as shutting down the power grid for a whole blackout.

I develop a Football Game Algorithm with DL-based Data Edge Verification with a Consensus Approach (FGADL-DEVCA) for a BC-assisted IoT-cloud platform. The major drive of the FGADL-DEVCA approach is to incorporate BC technology to enable security in the IoT cloud environment, and the DL model can be applied for fault detection efficiently.

- The FGADL-DEVCA technique utilizes deep autoencoder (DAE) for fault recognition and classification in the IoT-cloud platform.

- FGA-based hyperparameter tuning is applied to enhance the fault detection performance of the DAE approach within the FGADL-DEVCA technique.
- An experimental evaluation of the FGADL-DEVCA approach is conducted, assessing its performance across distinct metrics

The remaining sections of the article are arranged as follows: Section 2 offers the literature review, and Section 3 represents the proposed method. Then, section 4 elaborates on the results evaluation, and section 5 completes the work.

2. Literature survey

Vaiyapuri et al. [11] designed an innovative BC-based Data Edge Verification with a Consensus Algorithm for ML (BDEVCA-ML) methodology. This method combines the benefits of BC, IoT, and ML algorithms for improving the IoT platform. The deep BiGRU (DBi-GRU) algorithm was employed for detecting fault. At last, the African vulture optimizer algorithm (AVOA) method was employed for the boost parameter tuning of the DBi-GRU architecture. In [12], a method named Score Grouping-practical Byzantine fault tolerance (SG-PBFT), a protective and effective dispersed consensus method for applications of BC in the IoV, was developed. The SG-PBFT consensus method enhances the standard PBFT consensus technique by enhancing the PBFT consensus method as well as employing a score group method for attaining greater consensus proficiency. Fan et al. [13] presented a two-layer BC-based architecture, and an innovative Dynamic Random BFT (DR-BFT) consensus method was developed. Next, the method obtains consensus under the data with a binary consensus sub-method that can be a substitute for Ben-Or and Michael's Random Consensus. The architecture also develops an increased minimum technique.

In [14], a BC-based data integrity verification method was developed. According to this technique, a comprehensive BC-assisted data integrity verification method without a reliable third party was established with data verification and data update stages. An innovative developed model was built under Hyperledger Sawtooth and experimental assessment against 2 recent models in a simulation cloud–based platform. Du et al. [15] projected a 2-stage trading method. Primarily, a smart contract-based identical method was introduced to form the renting connections between the DSOs and ECNs with the target of increasing social services. Secondarily, a social welfare improved double auction (SWIDA) technique was introduced for the development of the rental connection between the DSOs and UTs. In [16], -BC-based protected ES deployment architecture named ETS_GA was designed that is dependent on the elite-preserving GA (EGA). The early issue of standard GA was successfully resolved by employing niche sharing (NS) and tabu search (TS). BC-assisted privacy safeguard techniques were further utilized in the engaged servers.

Poongodi et al. [17] presented an efficient batch authentication and key exchange method. Additionally, 3 categories of techniques have been developed, namely MAC-based, ID-assisted, and PKI. The neuro-fuzzy interpretation algorithm could be exploited for predicting VANET security grades. In addition, I made an effort from a BC viewpoint integrated with MEC. In [18], a lightweight architecture-based evolutionary consensus algorithm called the Proof of Evolutionary Model (PoEM) technique was projected. PoEM repeatedly trains an ML method for attaining a consensus. Besides IoT platforms' dynamics, an innovative method was developed to control nodes combining and leaving dynamically.

Chen et al. [19] present a novel consortium blockchain framework for MCS, featuring the development of a Credit-based Proof-of-Work (C-PoW) model for enhanced reliability. It also introduces a scalable Deep Reinforcement Learning-based Computation Offloading (DRCO) method to handle computation-intensive tasks in the C-PoW context. In [20], an innovative Deep Reinforcement Learning (DRL) framework designed to offload computation-intensive Proof-of-Work (PoW) tasks onto edge servers within a blockchain-based Mobile Crowd Sensing (MCS) system is introduced. The objective of this framework is to establish an optimal offloading policy for PoW tasks, specifically addressing the complexities and dynamics inherent in the MCS environment.

3. The proposed model

In this study, an FGADL-DEVCA approach for a BC-assisted IoT-cloud platform is introduced. The major driver of the FGADL-DEVCA approach is to incorporate BC technology to enable security in the IoT cloud environment, and the DL model can be applied for fault detection efficiently. In the FGADL-DEVCA technique, the IoT devices encompass considerable decentralized decision-making abilities for reaching an agreement based on the performance of the intrablock transactions. Figure 1 illustrates the flow of the presented FGADL-DEVCA approach.

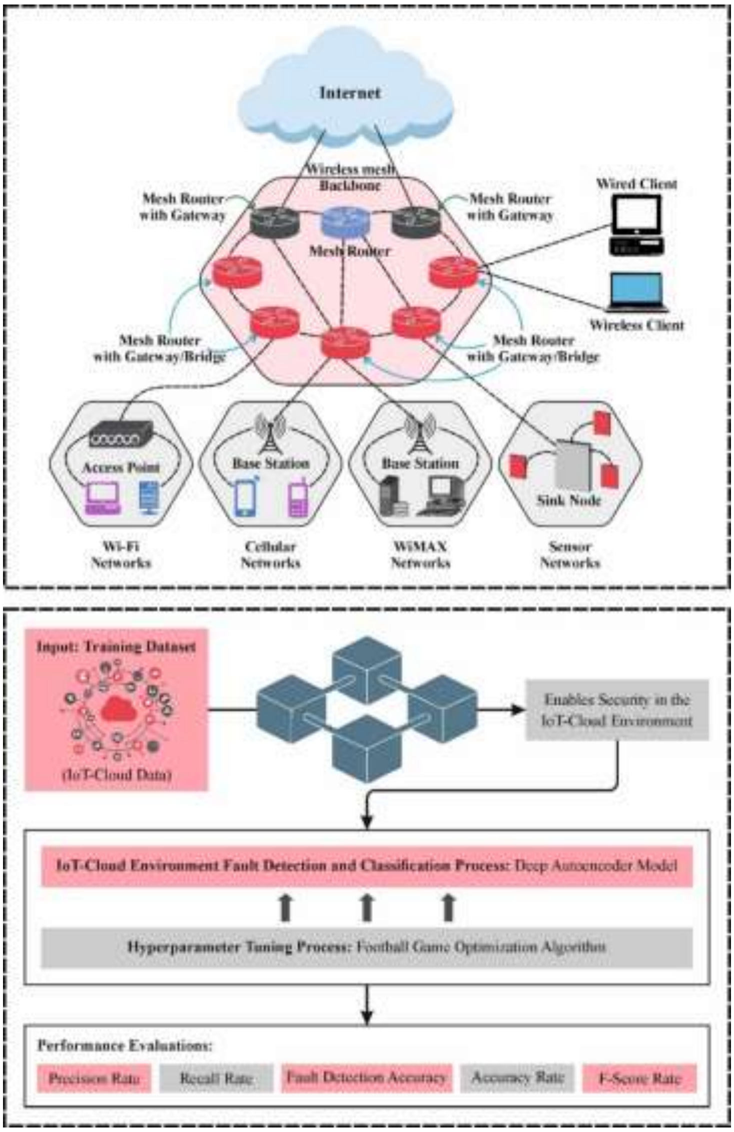

Figure 1. Overall flow of the FGADL-DEVCA approach.

3.1. Blockchain technology

In 2009, BC technology was presented by Satoshi Nakamoto over the establishment of the primary decentralization of digital exchange [21]. Currently, Bitcoin has gained important attention from both trade experts and researchers for its ability to transform a huge array of uses over the formation of decentralization and safe methods.

BC technology can be employed to find inadequacies and enhance data safety over mysterious and reliable transactions. Transactions noted on a BC are included in a decentralized archive by time stamps, averting any single right from authorizing actions in privacy. This consensus-driven technique aids in guaranteeing the reliability and safety of the BC, as some effort to change the archives would need to be organized through a mainstream of the system to accomplish. A BC includes a sequence of interrelated blocks; each holds the highest of manifold transactions and an exclusive cryptographic hash. These hashes have been produced utilizing difficult mathematical procedures that are employed to classify and confirm the reality of every block. Every block contains header data like the preceding block's hash, a time stamp, block number, other meta-data, and a body having the transaction logged on the system.

3.2. Fault detection using DAE

In this work, the FGADL-DEVCA technique exploits DAE for the recognition and classification of faults in the IoT-cloud platform. The technique utilizes autoencoders (AE), which is common in deep learning (DL) [22]. An AE is nothing but an unsupervised NNs-based feature extractor model that acquires the finest possible features to imitate its outcome assuming some input. One of the major attractive features is its probability of delivering a nonlinear and effective generalized PCA. It attains this outcome through backpropagation (BP) by inputting equal values of the target. To restate, it attempts to address how to forecast the presence as much as possible. The AE architecture contains 3 layers such as an output layer, a hidden layer (HL), and an input layer. The HL sizes are smaller than the input. Figure 2 represents the framework of the DAE model.

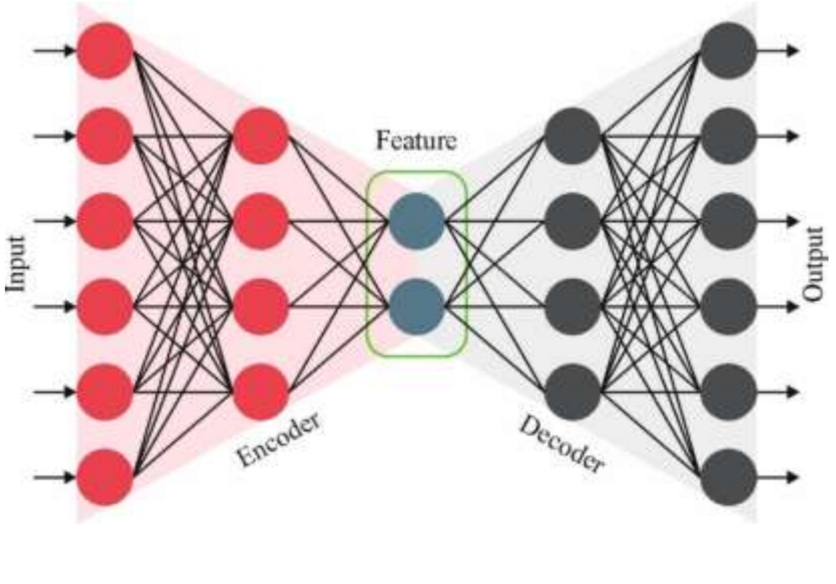

Figure 2. Architecture of DAE.

In the presented model, we use a deep AE. Unlike some traditional AEs, deep AEs contain 2 typical deep belief networks, such as decoding and encoding, with 4 or 5 shallow layers each. DL is beneficial to AEs by a stacked AE, in which numerous HL construct depth and imitate vital thoughts. As an outcome of this improved depth, computing costs and quantity of instruction data needed will be reduced and accurateness will be enhanced. The result of one HL aids as an input to a future, which is a more innovative stage. The 1st-order features are frequently learned from unrefined data by 1st layer of a stacked AE. The 2nd-order features depend on movements in the occurrence of 1st-order behaviors that are normally absorbed by the 2nd layer. Successive layers construct our thoughtful highest-order features.

The input layer is the 1st layer that obtains input Xi and utilizes many HLs to encode and decode it. The encoder procedure compacts the aspects to make them lesser than input data, and the procedure of the decoder reinstates these aspects in a converse way to commence the last outcome at the deepest layer. The LSTM and convolution (Conv) layer are united with an AE to produce a strong DDoS attack classifier. LSTM is mainly capable of classifying procedures like time sequences and learning from knowledge. After the completion of encoding, dependent on the outcome of the HL, the resultant layer has been decoded and rebuilt based on Eq (2) to generate a result of a similar dimension as the layer of input.

The main intention of the AE part is to draw input $x \in [0,1]^d$ to hidden symbol $y \in [0,1]d'$, whereas the mapping is executed by the function as follows:

$$yi = s(Wx_i + b) \tag{1}$$

Through

$$z_i = s(W'yi + b') \tag{2}$$

This symbol of concealment has been mapped backward into a renovation of the similar form as input x, whereas, s signifies a nonlinear sigmoid function. The primary and second parts are the encoder and decoder, respectively. These parameters decrease the normal renovation error. This technique contains one Conv layer, one dense layer, one input layer, one max-pooling layer, and dual LSTM layers in output.

3.3. Hyperparameter tuning using FGA

Finally, the FGADL-DEVCA technique applies FGA-based hyperparameter tuning. FGA is a novel meta-heuristic that can be applied initially to resolve continuous global optimization complexity [23]. Recently, it could be attempted to employ this method for roaming salesman problems as well as vehicle routing problems, though it is not capable of achieving better solutions. This could be recommended and stimulates the performance of football players who try to determine the better places during a match. Alternatively, the FGA applies various approaches to create a balance between incorporation of intensification and diversification. The FGA method utilizes the combined intelligence of humans and various techniques to utilize animal swarm intelligence. Alternatively, as stated in this process and similar to a football team whose goal is to score an objective, this aim can be used for attaining a good potential solution to the problem. Thus, to employ this method in an optimizer problem, generating a comprehensive simulation among each module of an optimized issue in a football game is required, as given below.

- The football players, time, and pitch with the developed method were the possible complexity space, the quantity of period to execute the procedure, and the original population of difficulties.
- The early populations that the method needs to function are the similar team players who can be aggressive and desire to score as many goals as possible.
- It can be supposed that all opposing players in the game have similar local optimal points with search space. Hence, the players of this group are not considered to be members of the 1st-team and do not attempt to score objectives.

When a player's position is intended for an identical quality response of most members, the aim is that all players can acquire the soccer ball, the ball moves between players, and reaches the member with the better position. A highly significant fact in football matches is that a method can be used, and a coach may change members who are not as good as other members in this game. Otherwise, the member of the team with poor performance could be eliminated from the team, and because the coach makes best decisions, a better outcome could be achieved. This tactic remains to achieve the optimum goal or point until the closure of the game which can be the period of the entire process.

3.3.1. The general movement of players

In a football game, when the players are not under the instructions of their coach, the player is walking in the area without having a goal or they can move towards the ball. Certainly, in these two conditions, all players can have an objective to find a better position to score. In this game, one highly significant position, which other players request, is always the place of the players who have the ball. Hence, the additional goal of players is to be closer to the player with the ball (X_{ball}^t), receive the ball, and have a good position for their teams. Consequently, equation (1) represents the place of the members in repetition t. In this equation, $\beta \in [0.1]$ and $\varepsilon \in [-1,1]$ are both arbitrary variables that follow a uniform distribution. $\alpha > 0$ is a parameter fixed by the user, which obtains values dependent on problems to be procedure determined. α is the main value for a global or local search of the method due to reduced values, so the process searches nearby and the robustness of the method increases in intensification, whereas raising the approach prefers diversification or a global search. Slowly reducing this parameter, the method is modified from a global search at the beginning of the technique to a local search.

$$X_i^t = X_i^{t-1} + \alpha_i \varepsilon + \beta(X_{ball}^t - X_i^{t-1}) \tag{3}$$

Besides, in phase t, it demonstrates that the players have the ball. However, the passing of the ball between players is normally random, and a member or player of the team in a good position can likely acquire the ball. Thus, an equation for the variables that consider α can be given in Eq (4). From this equation, $\theta \in (0.1]$ and α_0 can be the constant quantity and initial parameter that were chosen arbitrarily.

$$\alpha_i = \alpha_0 \theta^t \tag{4}$$

3.3.2. Coaching

Football is a common game where the trainer is very significant since he or she can attain a worthy outcome by utilizing correct strategies as well as varying players. Therefore, a team trainer plays an important part in training as well as guiding players to be more active. Otherwise, the players finish their performance based on memory, such as coach's memory (CM), and at all times ensures performance and their placements as the best positions on the field. Therefore, it is extremely good to assign a few early populace dimensions in techniques as Coach Memory Size (CMS). This technique is capable of keeping essential answers. The main reason for utilizing this memory is that the technique employs two strategies similar to natural versions. The method is proposed to attain the chief goal of recording aims in football as well as get optimal probable answers in this method.

Attack strategy: The objective of a football game is to score goals. The normal way to do this is for midfielders and defenders to move near the opponent's goal and defeat them to have better chances of scoring. Nowadays, opposing players with developed techniques have similar solutions; therefore, the objective is to transport lesser solutions in models closer to results that play the character of a local optimizer. This kind of optimization is recognized so that modification of their purpose is lesser than a definite charge of Hyper Radius Limitation Value (HRLV); based on Eq (3), this value slowly reduces. It must be highly well-known that for every associate of the populace, hyper distance (HD) is the space for an optimal position, and few followers of the populace with a cost greater than HRLV the next strategy that is well-known as a hyper radius penalty (HRP) plan.

$$HRLV^{T} = HRLV_{min} + \gamma(HRLV^{t-1} - HRLV_{min}). \tag{5}$$

where $\gamma \in (0.1)$ is the decreased constant of HRLV.

Substitution Approach: This plan is an additional way to advance and enhance the group's score, so that players do not keep playing and are substituted by other players that assist the team for a high score. In this model, this kind of performance is also measured, and in iteration, the worst results are taken from the issue, and the method substitutes them with improved solutions to the issue. The times the change was completed is known as the fitness limitation value (FLV), which substitutes the results that provide values poorer than this value in every iteration. Thus, the quality of the solution can be predicted to increase at the time of performance, and this value is theoretically adjustable to the model's iterations, and its value develops (this value is higher in large problems and lower in small problems). It employs FLV values, and this plan is known as the efficient fitness penalty (FP) technique.

$$FLV^{t} = FLV_{min} + \lambda(FLV^{t-1} - FLV_{min}). \tag{6}$$

At this point, λ has the same role as Eq (6). In point, the training part is similar to the local search segment of the model. The novel positions for players that are out of bounds are found after applying plans by utilizing accidental movements from adjacent optimal positions to their prior position (Eq (7)).

$$X_{new} = X_{nearestbest} + \alpha_j \varepsilon \tag{7}$$

The fitness choice is a significant aspect controlling the solution of the FGA system. The hyperparameter choice contains the encoded performance for evaluating the effectiveness of candidate results. During this case, the FGA assumes accuracy as the main condition to design the fitness function (FF) that is expressed as:

$$Fitness = \max(P) \tag{8}$$

$$P = \frac{TP}{TP+FP} \tag{9}$$

whereas, FP and TP stand for the false and true positive values, respectively.

4. Experimental validation

In this section, the performance validation of the FGADL-DEVCA approach is examined in detail. In Table 1 and Figure 3, a comparison precision rate (PR) outcome of the FGADL-DEVCA system can be investigated in detail [11]. This acquired outcome shows that the FGADL-DEVCA method exhibited better performance with maximum PR values. It is shown that the RF and DA-WRF models demonstrate worse performance. Although the DA-WRF and PSODA-WRF models accomplish closer outcomes, the FGADL-DEVCA method attains superior performance with maximum PR values of 99.84%, 99.50%, 99.84%, 99.89%, and 99.68%, under CPUHog, MemoryOF, Scanning, IOHog, and DoS classes, respectively.

Table 1. PR analysis of FGADL-DEVCA approach with recent models under various classes.

Precision Rate (%)					
Classes	**FGADL-DEVCA**	**BDEVCA-ML**	**PSODA-WRF**	**DA-WRF**	**Random Forest**
CPUHog	99.84	99.69	98.73	97.20	95.99
MemoryOF	99.50	99.35	98.22	97.11	95.67
Scanning	99.84	99.72	98.44	97.30	96.18
IOHog	99.89	99.74	98.86	97.69	96.14
DOS	99.68	99.53	98.02	96.53	95.37

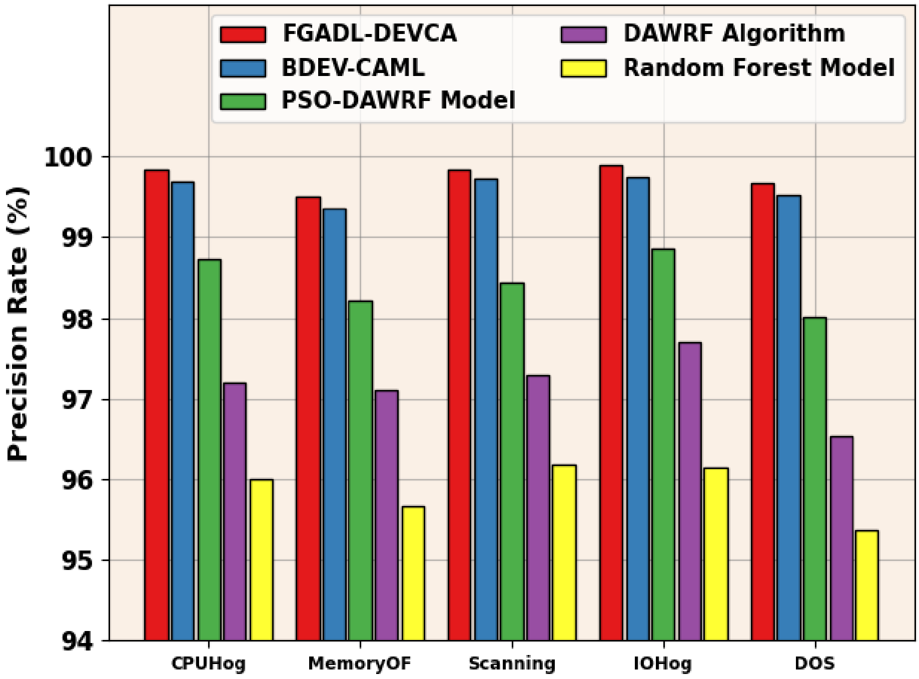

Figure 3. PR analysis of FGADL-DEVCA model for various classes.

A wide-ranging comparison recall rate (RR) analysis of the FGADL-DEVCA system is examined in Table 2 and Figure 4. These outcomes show that the FGADL-DEVCA technique has better performance with higher RR values. It is represented that the RF and DA-WRF systems demonstrate poorer performance. While the DA-WRF and PSODA-WRF methods achieve remarkable results, the FGADL-DEVCA algorithm gets superior performance with greater RR values of 99.78%, 99.51%, 99.78%, 99.87%, and 99.63% under CPUHog, MemoryOF, Scanning, IOHog, and DoS classes.

Table 2. RR analysis of the FGADL-DEVCA technique with recent models having various classes.

Recall Rate (%)					
Classes	**FGADL-DEVCA**	**BDEVCA-ML**	**PSODA-WRF**	**DA-WRF**	**Random Forest**
CPUHog	99.78	99.63	98.62	97.70	96.46
MemoryOF	99.51	99.37	97.99	96.35	95.30
Scanning	99.78	99.65	98.55	97.49	96.53
IOHog	99.87	99.74	98.17	97.01	95.64
DOS	99.63	99.49	97.91	96.82	95.46

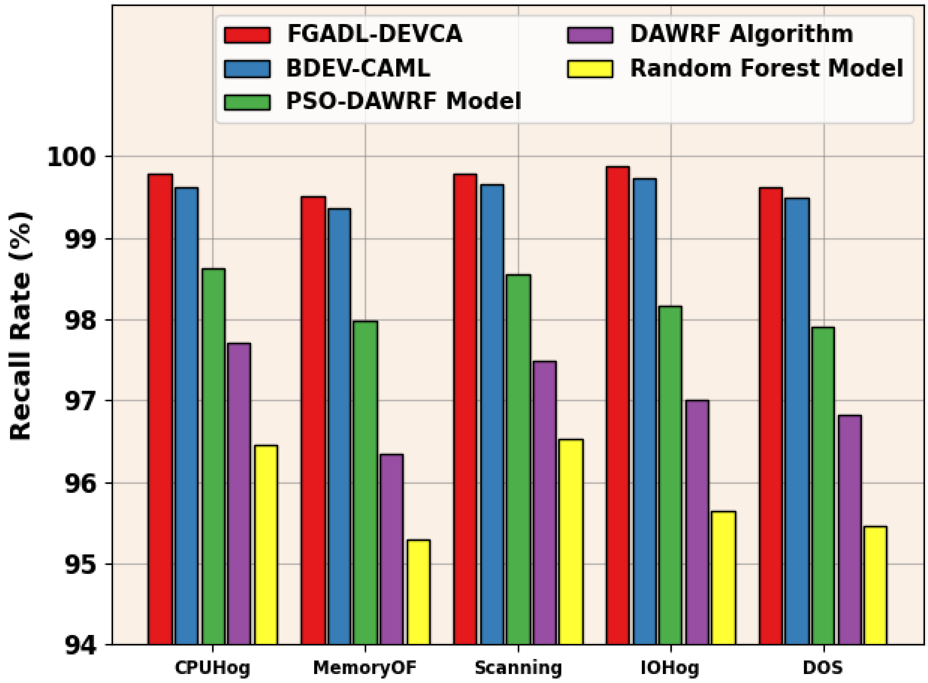

Figure 4. RR analysis of the FGADL-DEVCA model for various classes.

An extensive comparison accuracy rate (AR) outcome of the FGADL-DEVCA system can be determined in Table 3 and Figure 5. These achieved outcomes show that the FGADL-DEVCA algorithm exhibits increased performance with maximal AR values. It is displayed that the RF and DA-WRF systems show poorer performance. Though the DA-WRF and PSODA-WRF methods gain significant outcomes, the FGADL-DEVCA methodology obtains excellent performance with improved AR values of 99.89%, 99.71%, 99.91%, 99.78%, and 99.77% under CPUHog, MemoryOF, Scanning, IOHog, and DoS classes, respectively.

Table 3. AR analysis of the FGADL-DEVCA approach with recent models under various classes.

Accuracy Rate (%)					
Classes	**FGADL-DEVCA**	**BDEVCA-ML**	**PSODA-WRF**	**DA-WRF**	**Random Forest**
CPUHog	99.89	99.76	98.55	96.92	95.20
MemoryOF	99.71	99.54	98.15	97.15	96.13
Scanning	99.91	99.78	98.21	96.61	95.39
IOHog	99.78	99.65	98.36	96.65	95.16
DOS	99.77	99.62	98.17	97.06	95.95

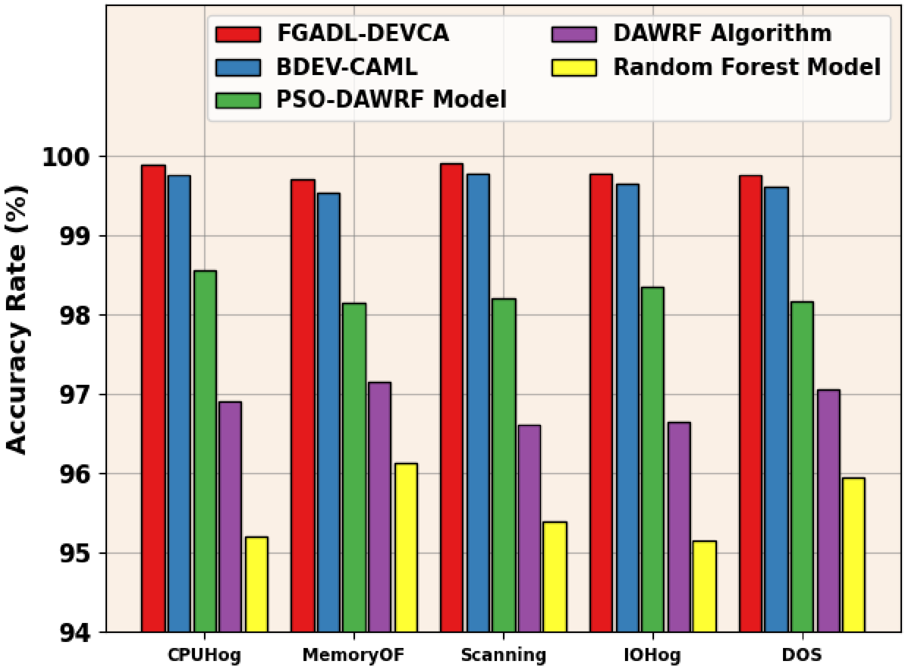

Figure 5. AR analysis of the FGADL-DEVCA system for various classes.

A comprehensive comparison F-score rate (FR) outcome of the FGADL-DEVCA system is measured in a detailed manner in Table 4 and Figure 6. These simulation values show that the FGADL-DEVCA method has greater performance with maximum FR values. It is displayed that the RF and DA-WRF techniques demonstrate low performance. While the DA-WRF and PSODA-WRF systems gain closer results, the FGADL-DEVCA algorithm gets better performance with the highest FR values of 99.60%, 99.65%, 99.71%, 99.74%, and 99.77% under CPUHog, MemoryOF, Scanning, IOHog, and DoS classes.

In Table 5 and Figure 7, a comparative fault detection accuracy (FAD) result of the FGADL-DEVCA system is provided. These simulation results specify that the FGADL-DEVCA technique gets superior performance under all fault probabilities (FP). With an FP of 0.05%, the FGADL-DEVCA methodology attains an increased FPA of 99.67% but the BDEVCA-ML, PSODA-WRF, NFD, ETX-TD, and DFD models gained decreased FPA of 99.23%, 98.02%, 96.81%, 96.39%, and 94.22%, respectively. Also, with FP of 0.20%, the FGADL-DEVCA method gets an increased FPA of 95.76% although the BDEVCA-ML, PSODA-WRF, NFD, ETX-TD, and DFD algorithms acquire diminished

FPA of 95.31%, 92.45%, 90.42%, 87.31%, and 83.26%, respectively. Besides, with FP of 0.35%, the FGADL-DEVCA system gets an increased FPA of 91.57%, but the BDEVCA-ML, PSODA-WRF, NFD, ETX-TD, and DFD algorithms obtain lessened FPAs of 91.11%, 89.09%, 84.61%, 80.57%, and 74.90%, respectively. Finally, with an FP of 0.50%, the FGADL-DEVCA system obtains a raised FPA of 87.62%; however, the BDEVCA-ML, PSODA-WRF, NFD, ETX-TD, and DFD approaches obtain reduced FPAs of 87.18%, 83.27%, 81.49%, 75.01%, and 65.94%, respectively.

Table 4. FR analysis of the FGADL-DEVCA approach with recent models under various classes.

F-Score Rate (%)					
Classes	**FGADL-DEVCA**	**BDEVCA-ML**	**PSODA-WRF**	**DA-WRF**	**Random Forest**
CPUHog	99.60	99.45	97.76	96.57	95.18
MemoryOF	99.65	99.49	97.92	96.61	95.62
Scanning	99.71	99.58	98.06	96.67	95.08
IOHog	99.74	99.60	97.99	97.04	96.01
DOS	99.77	99.60	97.88	96.75	95.82

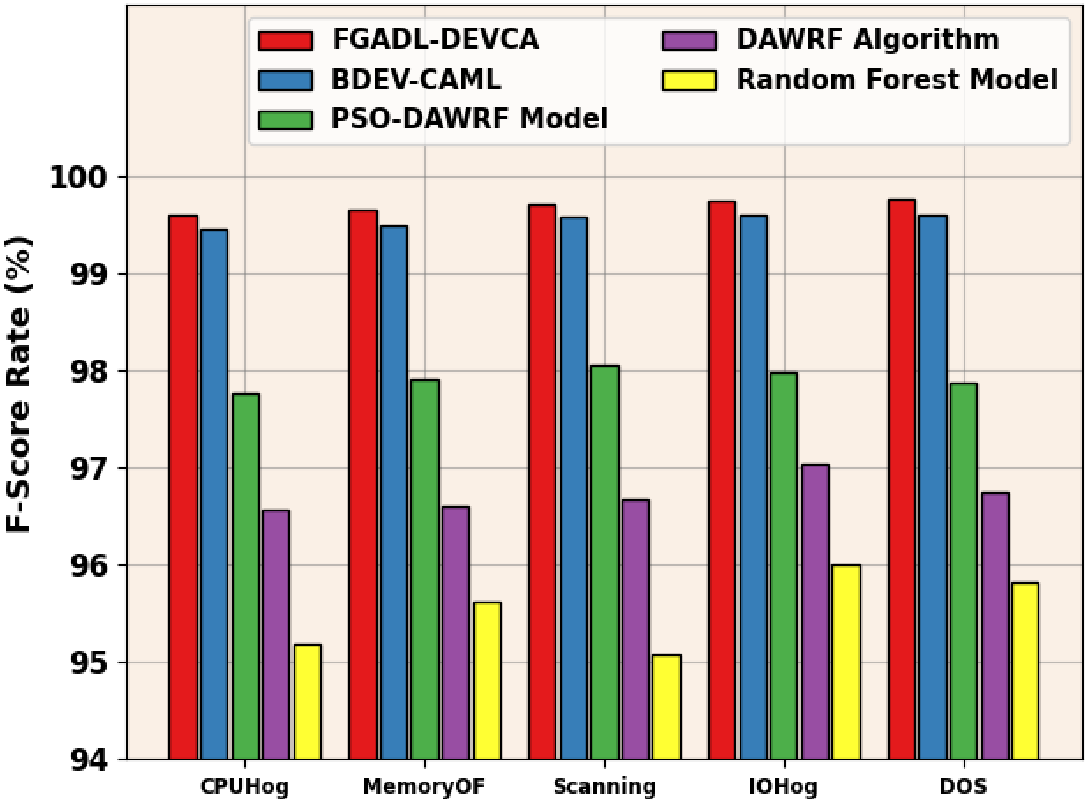

Figure 6. FR outcome of the FGADL-DEVCA methodology under various classes.

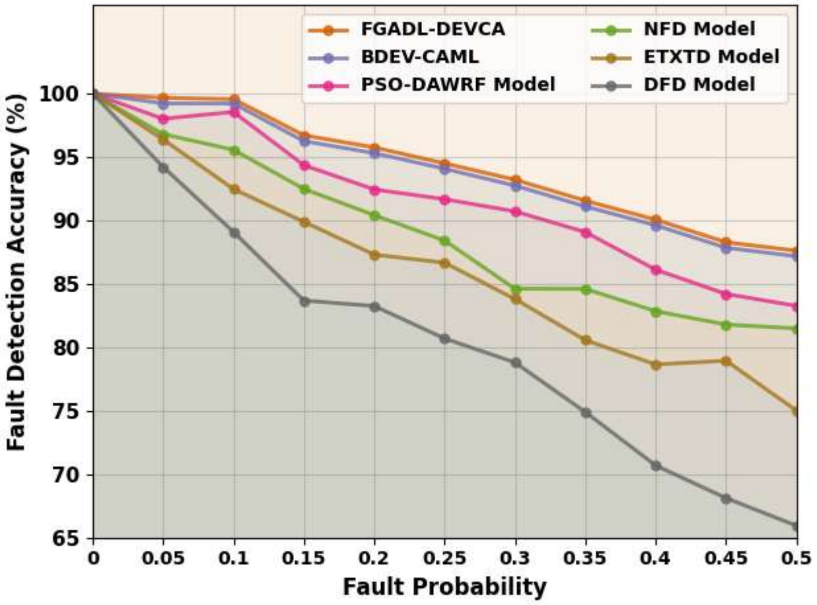

Figure 7. FAD outcome of FGADL-DEVCA technique under varying FP.

Table 5. FAD outcome of FGADL-DEVCA technique with existing approaches under varying FP.

Fault Detection Accuracy (%)						
Fault Probability	**FGADL-DEVCA**	**BDEVCA-ML**	**PSODA-WRF**	**NFD**	**ETX-TD**	**DFD**
0.00	100	100	100	100	100	100
0.05	99.67	99.23	98.02	96.81	96.39	94.22
0.10	99.57	99.22	98.56	95.57	92.48	89.10
0.15	96.72	96.26	94.36	92.49	89.90	83.69
0.20	95.76	95.31	92.45	90.42	87.31	83.26
0.25	94.50	94.08	91.68	88.42	86.67	80.70
0.30	93.22	92.75	90.72	84.62	83.81	78.81
0.35	91.57	91.11	89.09	84.61	80.57	74.90
0.40	90.06	89.62	86.12	82.85	78.65	70.69
0.45	88.29	87.85	84.21	81.80	78.95	68.12
0.50	87.62	87.18	83.27	81.49	75.01	65.94

The $accu_y$ curves for training (TR) and validation (VL) exhibited in Figure 8 for the FGADL-DEVCA technique offer valuable insights into its effectiveness for numerous epochs. Primarily, it can be a reliable improvement in both TR and TS $accu_y$ to rising epochs, demonstrating the proficiencies of the model in learning and recognizing patterns in both TR and TS data. The increasing trend in TS $accu_y$ underscores the adaptability of the model to the TR dataset and the ability to generate correct predictions on unseen data, underscoring capabilities of robust generalization.

Figure 9 offers a wide-ranging overview of the TR and TS loss values for the FGADL-DEVCA method through numerous epochs. The TR loss consistently decreases as the model refines weights to minimize classification errors under both datasets. The loss curves demonstrate the model's alignment with the TR data, underscoring its ability to capture patterns successfully. The constant improvement of parameters in the FGADL-DEVCA system is significant, targeted to diminish discrepancies between predictions and actual TR labels.

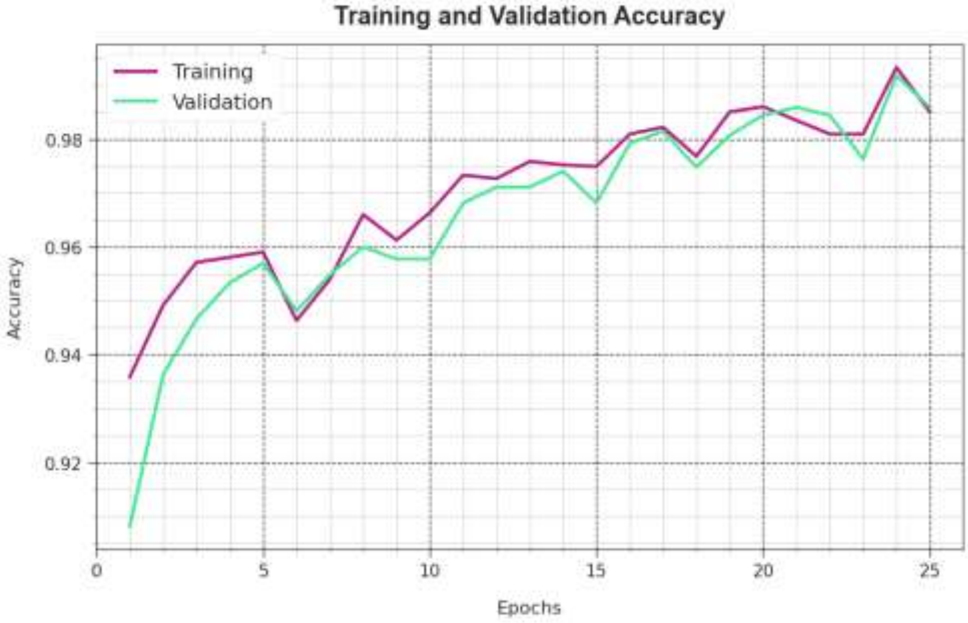

Figure 8. $Accu_y$ curve of the FGADL-DEVCA technique.

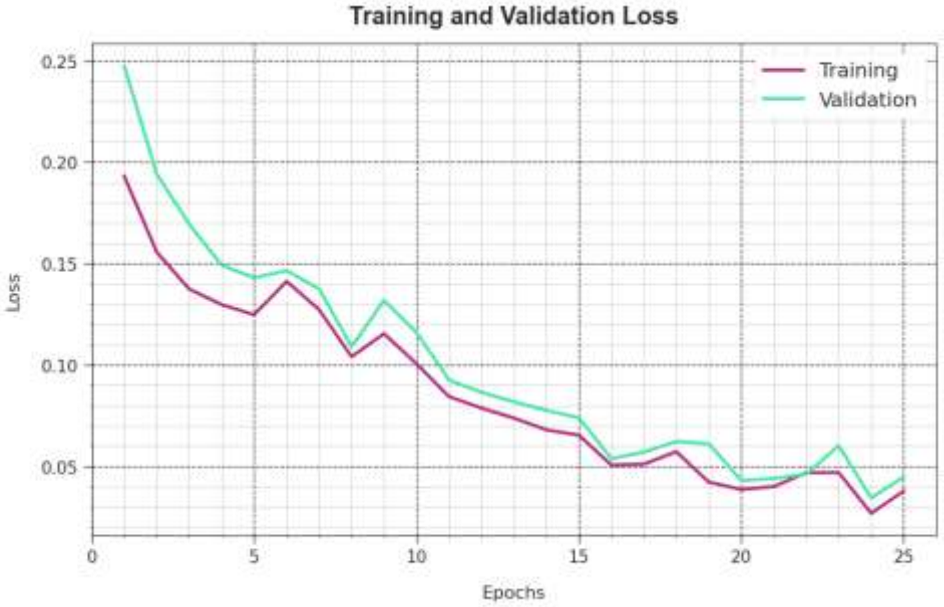

Figure 9. Loss curve of the FGADL-DEVCA technique.

These results confirmed that the FGADL-DEVCA technique gained better performance over other recent approaches.

5. Conclusions

In this study, an FGADL-DEVCA method for a BC-assisted IoT-cloud platform is introduced. The major drive of the FGADL-DEVCA approach is to incorporate BC technology to enable security in the IoT cloud environment, and the DL model can be applied for fault detection efficiently. In the FGADL-DEVCA technique, the IoT devices encompass considerable decentralized decision-making abilities for reaching an agreement based on the performance of the intrablock transactions. Besides, the FGADL-DEVCA technique exploits DAE for the recognition and classification of faults in the IoT-cloud platform. To enhance the fault detection solution of the DAE approach, the FGADL-DEVCA technique applies FGA-based hyperparameter tuning. The experimental results analysis of the FGADL-DEVCA technique is performed concerning distinct metrics. The experimental values demonstrated the betterment of the FGADL-DEVCA algorithm with other existing methods concerning various aspects. Future efforts for FGADL-DEVCA could focus on adaptations to various IoT-cloud scenarios and improving fault detection through ongoing algorithm refinement. However, a potential limitation is the sensitivity of FGA-based hyperparameter tuning to network variations, necessitating robustness considerations for real-world deployments.

Use of AI tools declaration

The author declares that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The author declares no conflicts of interest.

Acknowledgments

The author, Fahad F. Alruwaili, would like to thank the Deanship of Scientific Research at Shaqra University for supporting this research.

References

1. S. Ma, S. Wang, W. T. Tsai, Y. Zhang, Delay Optimization for Consensus Communication in Blockchain-Based End-Edge-Cloud Network, *In International Symposium on Advanced Parallel Processing Technologies* (pp 241–262), Singapore: Springer Nature Singapore, 2023. https://doi.org/10.1007/978-981-99-7872-4_14
2. S. Wadhwa, S. Rani, S. Verma, J. Shafi, M. Wozniak, Energy efficient consensus approach of blockchain for IoT networks with edge computing, *Sensors*, **22** (2022), 3733. https://doi.org/10.3390/s22103733
3. Y. Zhang, B. Li, B. Liu, Y. Hu, H. Zheng, A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain, *IEEE Internet Things*, **8** (2021), 13958–13974. https://doi.org/10.1109/JIOT.2021.3068410

4. Y. Tang, J. Yan, C. Chakraborty, Y. Sun, Hedera: A permissionless and scalable hybrid blockchain consensus algorithm in multi-access edge computing for IoT, *IEEE Internet Things*, 2023. https://doi.org/10.1109/JIOT.2023.3279108
5. K. Wang, S. P. Xu, C. M. Chen, S. H. Islam, M. M. Hassan, C. Savaglio, et al., A trusted consensus scheme for collaborative learning in the edge ai computing domain, *IEEE Network*, **35** (2021), 204–210. https://doi.org/10.1109/MNET.011.2000249
6. M. M. Alhejazi, R. M. A. Mohammad, Enhancing the blockchain voting process in IoT using a novel blockchain Weighted Majority Consensus Algorithm (WMCA), *Inf. Secur. J.*, **31** (2022), 125–143. https://doi.org/10.1080/19393555.2020.1869356
7. Z. Liao, S. Cheng, RVC: A reputation and voting based blockchain consensus mechanism for edge computing-enabled IoT systems, *J. Network Comput. Appl.*, **209** (2023), 103510. https://doi.org/10.1016/j.jnca.2022.103510
8. W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, Y. Zhang, Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment, *J. Syst. Archit.*, **115** (2021), 102024. https://doi.org/10.1016/j.sysarc.2021.102024
9. X. Fu, H. Wang, P. Shi, X. Zhang, Teegraph: A Blockchain consensus algorithm based on TEE and DAG for data sharing in IoT, *J. Syst. Archit.*, **122** (2022), 102344. https://doi.org/10.1016/j.sysarc.2021.102344
10. W. Li, Q. Zhang, S. Deng, B. Zhou, B. Wang, J. Cao, Q-learning improved lightweight consensus algorithm for blockchain-structured internet of things, *IEEE Internet Things*, 2023.
11. T. Vaiyapuri, K. Shankar, S. Rajendran, S. Kumar, S. Acharya, H. Kim, Blockchain Assisted Data Edge Verification with Consensus Algorithm for Machine Learning Assisted IoT, IEEE Access, 2023. https://doi.org/10.1109/ACCESS.2023.3280798
12. G. Xu, H. Bai, J. Xing, T. Luo, N. N. Xiong, X. Cheng, et al., SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles, *J. Paral. Distr. Comput.*, **164** (2022), 1–11. https://doi.org/10.1016/j.jpdc.2022.01.029
13. Y. Fan, H. Wu, H. Y. Paik, DR-BFT: A consensus algorithm for blockchain-based multi-layer data integrity framework in dynamic edge computing system, *Future Gener. Comp. Syst.*, **124** (2021), 33–48. https://doi.org/10.1016/j.future.2021.04.020
14. Y. Li, J. Shen, S. Ji, Y. H. Lai, Blockchain-Based Data Integrity Verification Scheme in AIoT Cloud-Edge Computing Environment, *IEEE Transactions on Engineering Management*, 2023.
15. Y. Du, Z. Wang, J. Li, L. Shi, D. N. K. Jayakody, Q. Chen, et al., Blockchain-aided edge computing market: Smart contract and consensus mechanisms, *IEEE T. Mobile Comput.*, 2022.
16. Z. Li, G. Li, M. Bilal, D. Liu, T. Huang, X. Xu, Blockchain-assisted Server Placement with Elitist Preserved Genetic Algorithm in Edge Computing, *IEEE Internet Things*, 2023.
17. M. Poongodi, S. Bourouis, A. N. Ahmed, M. Vijayaragavan, K. G. S. Venkatesan, W. Alhakami, et al., A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework, *Comput. Comm.*, **192** **(**2022), 48–56. https://doi.org/10.1016/j.comcom.2022.05.014
18. Y. Zhao, Y. Qu, Y. Xiang, Y. Zhang, L. Gao, A Lightweight Model-Based Evolutionary Consensus Protocol in Blockchain as a Service for IoT, *IEEE T. Serv. Computi.*, 2023. https://doi.org/10.1016/j.comcom.2022.05.014

19. Z. Chen, J. Zhang, Z. Huang, P. Wang, Z. Yu, W. Miao, Computation offloading in blockchain-enabled MCS systems: A scalable deep reinforcement learning approach, *Future Gener. Comp. Syst.*, **153** (2024), 301–311. https://doi.org/10.1016/j.future.2023.12.004
20. Z. Chen, Z. Yu, Intelligent offloading in blockchain-based mobile crowdsensing using deep reinforcement learning, *IEEE Commun. Mag.*, **61** (2023), 118–123. https://doi.org/10.1016/j.future.2023.12.004
21. M. Firdaus, H. T. Larasati, K. H. Rhee, A blockchain-assisted distributed edge intelligence for privacy-preserving vehicular networks, *Comput. Mater. Con.,* **76** (2023). https://doi.org/10.32604/cmc.2023.039487
22. A. K. Mousa, M. N. Abdullah, An improved deep learning model for DDoS detection based on hybrid stacked autoencoder and checkpoint network, *Future Internet*, **15** (2023), 278. https://doi.org/10.32604/cmc.2023.039487
23. Z. H. Ahmed, F. Maleki, M. Yousefikhoshbakht, H. Haron, Solving the vehicle routing problem with time windows using modified football game algorithm, *Egypt. Inform. J.,* **24** (2023), 100403. https://doi.org/10.32604/cmc.2023.039487

AIMS Press

© 2024 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)