Egyptian Informatics Journal 24 (2023) 100406

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Federated learning optimization: A computational blockchain process with offloading analysis to enhance security

Selvarajan Shitharth [a,h], Hariprasath Manoharan [b], Achyut Shankar [c,g,*], Rakan A. Alsowail [d], Saravanan Pandiaraj [d], Seyyed Ahmad Edalatpanah [e], Wattana Viriyasitavat [f]

[a] Department of Computer Science, Kebri Dehar University, Kebri Dehar, Ethiopia
[b] Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee-600123, Chennai, Tamil Nadu, India
[c] WMG, University of Warwick, Coventry, UK
[d] Computer Skills, Self-Development Skills Department, Deanship of Common First Year, King Saud University, 11362 Riyadh, Saudi Arabia
[e] Department of Applied Mathematics, Ayandegan Institute of Higher Education, Tonekabon, Iran
[f] Chulalongkorn Business School, Faculty of Commerce and Accountancy, Chulalongkorn University, Thailand
[g] School of Computer Science Engineering, Lovely Professional University, Phagwara - 144411, Punjab, India
[h] School of Built Environment, Engineering and Computing, Leeds Beckett University, LS1 3HE Leeds, UK

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Blockchain
Data blocks
Federated learning
Security

ABSTRACT

The Internet of Things (IoT) technology in various applications used in data processing systems requires high security because more data must be saved in cloud monitoring systems. Even though numerous procedures are in place to increase the security and dependability of data in IoT applications, the majority of outside users can decode any transferred data at any time. Therefore, it is essential to include data blocks that, under any circumstance, other external users cannot understand. The major significance of proposed method is to incorporate an offloading technique for data processing that is carried out by using block chain technique where complete security is assured for each data. Since a problem methodology is designed with respect to clusters a load balancing technique is incorporated with data weights where parametric evaluations are made in real time to determine the consistency of each data that is monitored with IoT. The examined outcomes with five scenarios process that projected model on offloading analysis with block chain proves to be more secured thereby increasing the accuracy of data processing for each IoT applications to 89%.

1. Introduction

It is estimated that the number of Internet of Things (IoT) devices will reach approximately estimated to reach around 75 billion devices by 2025 [1]. With IoT delivering a large amounts of collected data and diverse observations about environments and well-being and quality of life for people [2], this has created an internet of vulnerabilities (IoV) [3,4]. The Internet of Things (IoT) covers a wide spectrum of applications' domains, these domains includes smart homes, Health care services, manufacturing, agriculture, intelligent transportation, supply chain, smart city, critical mission applications as well as utilities. Gartner reported that, the digital twin (DT) is one of the top 10 technologies that dominates in 2020. More than 50 % of IoT Enterprises have a digital twin in their strategic plan [5] (see Table 1).

Most wireless application advancements occur within various platform segments where numerous users rely on particular patterns that must be adhered to using pre-defined models in real-time. Predefined models must constantly be introduced into the system with all the relevant security measures that support the complete system format and knowledge about various data processing techniques. IoT typically operates in the manner indicated above, but most models are not defined with the proper pre-specified features. Therefore, the suggested method uses a federated learning strategy to process the data, where all information pertaining to data security issues is immediately analyzed and decrypted. Additionally, there are numerous application methods in IoT, and only authorized users are permitted access to the data [4].

In contrast, other users are prohibited from accessing any data in the system. However, because numerous distinct processing systems are involved when IoT models are established explicitly for people, a separate authentication key is not present in the cloud [4,6,7]. Thus, a

* Corresponding author.
E-mail address: ashankar2711@gmail.com (A. Shankar).

https://doi.org/10.1016/j.eij.2023.100406
Received 19 May 2023; Received in revised form 16 September 2023; Accepted 26 September 2023
Available online 20 October 2023

Table 1
Existing models vs Proposed.

References	Integrated methods	Objectives				
		A	B	C	D	E
[5]	Digital twin model					
[9]	Sharding based blockchain	✓		✓		
[10]	Blockchain for digital twins	✓	✓			
[11]	Blockchain for turbo machinery	✓			✓	✓
[12]	Phases of digital twins using blockchain		✓	✓		
[13]	Directed acyclic graph for industrial operations		✓		✓	
[14]	Decentralization of blockchain using IoT		✓	✓		✓
[15]	Stable cyber security model			✓	✓	
[16]	Novel mathematical approach with cyber security			✓		✓
[17]	Mechanistic model for cyber threats			✓	✓	✓
[18]	Creation of digital shadows with multiple agents	✓		✓		✓
Proposed	**Federated learning model with blockchain procedure**	✓	✓	✓	✓	✓

A: Number of transaction blocks and nodes; B: Block consistency ratio; C: Data load balance; D: Block energy; E: Learning accuracy.

typical application platform is developed by employing central processing units in the proposed technique, and data exchange is only carried out in response to requests from various users. As soon as a shared application platform is established, data can only be processed in the form of blocks. There are five fundamental architectural attributes of blockchain: decentralized, immutable, anonymous, cryptographically encrypted, and trust-based [8], Therefore, a blockchain approach is merged with federated learning technology to enhance data security in IoT.

Additionally, if data blocks are used, the consistency ratio of the data transmission technology will be significantly higher, reducing the latency period for the data. The IoT block diagram with the federated learning technique is shown in Fig. 1. The proposed model in Fig. 1 shows how the technique starts by utilizing the main setup with a nearby data center for data transmission. Duplication of packets is avoided at this point since various copies of the data will be saved in the database using distinct storage units once it has been transferred. A unique authentication key is used to unite all segmented levels after integrating several data sets, which starts the blockchain process. So, after looking at several key strategies, the complete set of data can be stored in the cloud, where all output units can be seen through gateway routes.

1.1. Research gap and motivation

Even though there are different block chain technologies that are integrated with various system model for describing the effect of data processing states most of the analyzed methods fails to build the gap by examining the number of transaction blocks. Moreover most of the methods are introduced with major gap on security that is provided to each cluster where individual weights are allocated to increase the consistency ratio. Hence the solution to following queries must be provide to overcome the gap that is present in existing approach.

- Is the offloading analysis provides same features for all blocks at maximized transactions that is present on each cluster head?
- Can integration of federated learning affects the system accuracy after removing unnecessary blocks at each state?
- Whether the data blocks that is monitored with IoT be transmitted with low energy even if maximum load in present in the offloading systems?

The model that is provided in [5] for block transaction process provides a deep insight on basic transmission systems where data in each block is forwarded to destination with more amount of security. Since most of the process is changed to digital representations a new model of data transmission in each block is carried out with digital twin representations that are directly connected with IoT [5]. The above mentioned model is defined as mechanistic mathematical model where it is used for defining the importance of block transactions only with on load analysis therefore the major drawback in such type of process is that due to creation of identical blocks the loss rate will be much higher in each block and in addition the energy for each block will also be maximized.

1.2. Major contributions

The major objective is to design a model with federated learning and blockchain technology for IoT. The contribution of the paper is three folds

- Minimize the number of computational blocks and offloading tasks using federated learning procedures.

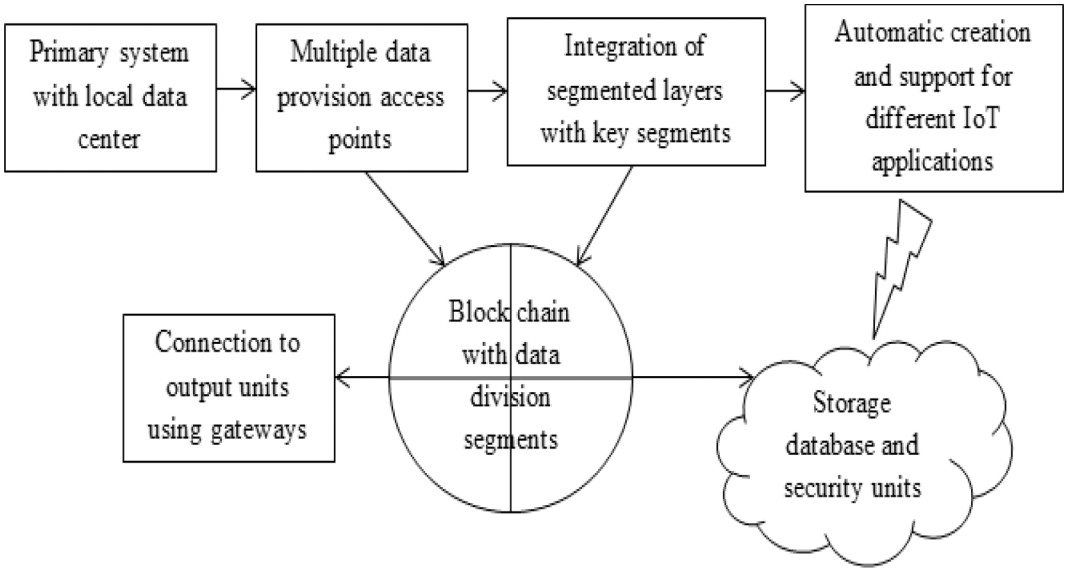

Fig. 1. Representation of the proposed system.

- Maximize the accuracy of computational blocks with a unique key management strategy.
- Represent a common identification model for all IoT applications using consistency ratio and aggregate values.

Federated learning can be applied in block chain technology to prevent unnecessary leakage in data transactions to other external users. This type of combination process provides two types of advantages for data transmission techniques such as trust of data and live feed of training data to learn the updated parametric designs. During the process of federated learning many block data is used for training multiple devices at same time period therefore it is possible to feed local data inside every block thereby avoiding failure even at offloading analysis. Additionally due to inherent knowledge of each block at collaborative learning stage every client can able to transmit the blocks by utilizing low amount of energy at high secured state.

1.3. Paper organization

The rest of the paper is organized as follows; Section 2 provides background and related work. The analytical system model of representation for designing a number of block transactions in the system is presented in section 3. Section 4 introduces federated learning and blockchain model for IoT. Section 5 analyzes the outcomes of the integrated process with performance measures. Section 6 concludes the paper with future research directions.

2. Background and related work

This section examines all pertinent available techniques to assess the state of security for various Internet of Things (IoT) applications. All flaws in the existing case studies are reviewed in light of the need to update the system parameters, and using the flaws found; the suggested system model is represented with the necessary variables. All IoT applications are used in real-time, including the current learning methodologies monitored and modified to address any weaknesses revealed by using many scenarios to define the learning techniques. In [19], a hierarchal layer-based architecture is employed for performance measurements, and the entire operation is run on micro-service systems. The client–server model is designed with a hierarchical layer operation architecture, which supports all network parameters. However, if a network model is employed, the system model will need to be merged with learning parameters, which are not processed in these kinds of measurement scenarios. An intelligent IoT device is added to the system to integrate learning parameters and maintain the necessary energy trade-off conditions in the system [20]. When processing the designed energy model, heterogeneous data measurement values are used to make the essential trade-off even when the characteristics are spread. But the trade-off condition looks at more information about possible failures, which means that the best place for each component in the system has to be found.

It has been noted during assessment cases that healthcare applications leverage blockchain technology to guarantee the execution of the intelligent identification process [21]. Thus, a squirrel search algorithm is integrated into the smart monitoring process, where all the necessary building components are linked. All parametric values are tracked due to this linkage, and values are saved under strict security guidelines. Despite the security, users are not given private keys, allowing all unauthorized users to access the system. As a result, a medi-block is used to process the transfer of private keys, allowing for continuous data sharing [22]. As a result, when users are located at other nodes, the data exchange procedure diminishes the level of security. Constraints must be created to convey data in various formats, making developing an effective system model complex. Additionally, an offloading mechanism divides data transfer computation measures, making it much easier to distribute resources equally to all network devices [23]. But because IoT applications will be given high data rates, it is much harder to ensure everyone gets the same resources in sixth-generation networks.

Non-terminal node transmission architecture is created for the Internet of Things applications with a unique data set for medical monitoring systems [24]. The healthcare system architecture incorporates blockchain processes, where each block of patient data is encrypted using public keys. However, better and more secure encryption will be offered if private keys are employed to keep each information set distinctively. Due to the researchers' [25] usage of private essential management techniques in all electronic health records, communication networks are now more reliable. Even with more excellent reliability, ideal solutions are offered. If perfect answers are already present in blockchain networks, it is crucial to prioritize finding other solutions, even though their accuracy will often be substantially lower [26]. By merging several objective situations, a storage optimization technique is presented with a time-changing sensation when different solutions are reached in the system. However, because there is no performance study of case studies with many objectives, the system as a whole is less susceptible to scalability features. A safe framework that examines the performance evaluation metrics of IoT systems has been introduced [27] to guarantee proper scalability measures. This performance study offers transparency in data transport for all blocks with minimal resource constraints. Even if there is little data, the transmission time is prolonged due to poor resource supply. Even if there aren't enough resources for each channel measure, the Internet of Things data processing units still keeps safe transaction blocks.

Additionally, analyses are conducted using various bibliometric methods, with the fundamental theories and frameworks for all IoT applications receiving top priority [28]. According to this observation, most techniques are not implemented using blockchain technology's high-security features. However, other security measures show that higher robustness, which minimizes accuracy, is available if an IoT system is represented. In contrast, as complete entities are present and under observation at three distinct stages, it is crucial to combine the entire data source into a single framework [29–35]. Three phases result in a bilinear communication, which maximizes the overall system's accuracy. The approach needs a unique authentication process to generate time-based solutions using the correct memory resources. IoT applications require a particular approach with an analytical model, so a blockchain technique with federated learning is introduced and discussed in the following sections.

As a result, mathematical models that specify the number of transactions in the network with an additional block transfer approach are used to depict the proposed system. However, decentralized techniques can be resolved using a block approach with key management procedures, provided federated learning is included for defined networks. As a result, the number of computational nodes in the system is kept to a minimum in the suggested method, which employs a special key management mechanism. Additionally, the system model was created with the lowest amount of offloading duties possible, resulting in all transmitted blocks having low energy attributes. The accumulation strategy of the projected method also improves network accuracy by making blocks and periods work better.

2.1. 1.5 System model

Using a mathematical framework, the design of blockchain technology in IoT applications is evaluated to look at suitable functioning principles and constraints. 5G- networks are used to construct a set of computational jobs as part of the suggested way to offer high security for IoT applications. Additionally, as described by Equation (1), the computational jobs are transferred by utilizing an offloading transaction procedure with a minimal number of computational nodes [36,37].

$$OT_i = \sum_{i=1}^{n} c_{ij} + trans_i \tag{1}$$

where

c_{ij} indicates blockchain cluster head

$trans_i$ represents the number of transactions

Equation (1) shows that to ensure the effective functioning of computational processes at various time intervals, the summation of the cluster head and transactions must be kept to a minimum. Equation (2) shows how the number of transaction blocks will slow down if the number of cluster heads is not reduced [38].

$$d_t(i) = min \sum_{i=1}^{n} \frac{off_i * d_s(i)}{t_r(i)} \tag{2}$$

where

off_i denotes number of offloading tasks

d_s indicates data size of transaction blocks

t_r represents rate of transmission blocks

Equation (2) calculates the overall delay that is experienced in offloading circumstances for IoT applications when transaction blocks with different data sizes are present. A consistency ratio must be defined even if the system is designed with various data segments and it is created using Equation (3) as follows [39],

$$cons_i = min \sum_{i=1}^{n} \frac{UB_i - t_n(i)}{t_n(\mathrm{i}) - 1} \tag{3}$$

where

UB_i indicates random block transmissions

$t_n(i)$ denotes total number of operational factors in each block

Equation (3) shows that the defined ratio must be less than the threshold value of 0.1 if consistency is required in IoT applications. Equation (4) is used to define a load balancing strategy, which is as follows. If the ratio values are greater than the stated threshold values, consistency in data transmission blocks cannot be accomplished [40].

$$threshold_l = \min \sum_{i=1}^{n} \begin{bmatrix} wt_1 & \cdots & wt_i \\ \vdots & \ddots & \vdots \\ wt_i & \cdots & wt_n \end{bmatrix} \times \begin{bmatrix} t_{b1} & \cdots & t_{bi} \\ \vdots & \ddots & \vdots \\ t_{bi} & \cdots & t_{bn} \end{bmatrix} \tag{4}$$

where

$wt_1..wt_i..wt_n$ indicates weight of each blocks

$tb_1..tb_i..tb_n$, represents allocated blocks that are transmitted

Equation (4) states that to achieve the proper level of load balancing, the resource burden allocated to the various blocks must be minimized. Once the loads from the various blocks are balanced, key processing procedures employing digital signatures are enabled. Equation (5) is used to formulate this, as shown below [41,42].

$$key_i = \sum_{i=1}^{n} (tag_b * sign_i) + p_i \tag{5}$$

where

tag_b describes the number of tag blocks

$sign_i$ indicates the representation of digital signatures

p_i denotes the total number of private keys

The energy used at the beginning stage will be completely different from the energy used at the transmission and intermediate phases since digital signatures vary for each transaction block. The energy efficiency of transaction blocks in IoT applications is then calculated using Equation (6).

$$Energy_i = min \sum_{i=1}^{n} \beta_i + \tau_i + I_e \tag{6}$$

where

β_i, τ_i, I_e represents energies at initial, transmission and intermediate nodes

Equation (6), which shows how the minimization objective function changes based on the measured distance (7), is used to figure out the values for the change in energy representation.

$$Energy_{modified}(i) = min \sum_{i=1}^{n} dist_i * b_i * r_{in} \tag{7}$$

where

$dist_i$, b_i describes distance of measurement and transaction bits

r_{in} denotes residual period of transaction

Different variables that are crucial to the integration process are represented by the system model that is defined with analytical equations. So, the objective function to improve the performance of proposed blockchain IoT systems is built into the federated learning algorithm.

3. Optimization algorithm

When all decentralized edge computing detection systems are processed utilizing local data set values in the form of distributed functions, the process of a combined learning algorithm offers a better technique to increase training process efficiency [43–45]. Additionally, federated learning may be deployed in all IoT applications, solving all risky problems and greatly enhancing data security. Blockchain technology is incorporated into the suggested solution to further strengthen the security of IoT applications during various network update processes. Since all data sizes are somewhat similar, implementing federated learning fully reduces the latency of the defined system. Furthermore, it becomes much more difficult to update the data once it has been applied, and even sharing opportunities are limited. As a result, in all IoT applications, the data will be present on the node itself, where key encryption algorithms are less frequently used. Federated learning can address complicated problems involving big data analytics, and authorized individuals are granted access to the data. In federated learning, Equation (8) expresses the mathematical expression of selecting several data points at a specific time and the step by step implementation is deliberated in Fig. 2. In addition the representation base code for blockchain is provided in Fig. 3.

$$s_d(i) = \sum_{i=1}^{n} \gamma_i * \aleph_{in} \tag{8}$$

where

γ_i indicates number of selected data

$\aleph_{in}$ denotes proportion of data segments

Since the data in IoT applications are provided in proportions, it is essential to implement an accumulation strategy by using training parameters which is formulated using Equation (9) as follows [46,47],

$$agg_i = \sum_{i=1}^{n} \varphi(\vartheta_x, \vartheta_y) \tag{9}$$

where

ϑ_x, ϑ_y represents the attention parametric values in two different layers

If the total values are significantly greater, then the accuracy of the federated learning model must be determined using the loss function. Accordingly, Equation (10) is used to describe the accuracy of formulation as follows [48–51],

$$accuracy_i = max \sum_{i=1}^{n} (fed_i - sum_i) * loss_i \tag{10}$$

where

fed_i, sum_i indicates loss representations of federated and data summation values

$loss_i$ represents total loss in the system

The accuracy function, which must be maximized with low loss function values, is represented by equation (10). In the weight representation model, equation (11) can be used to make the loss function as

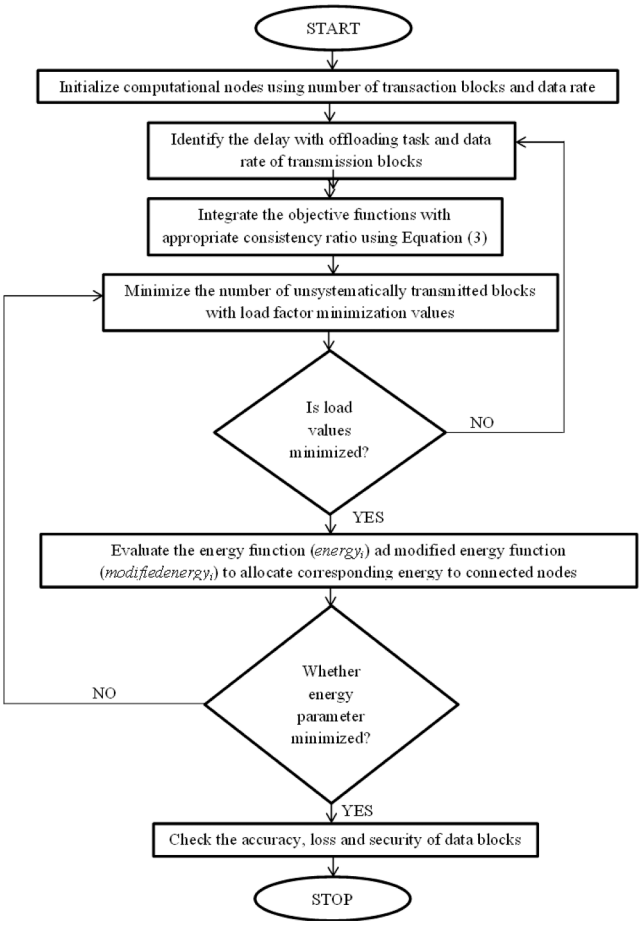

Fig. 2. Federated learning for IoT applications.

```
classdef Block < handle
    properties
    index
    timestamp
    data
    nonce
    hash
    previous_hash
  end
    methods
    function obj = Block(varargin)
      % index, prev_hash, timestamp, data, nonce, hash
      if nargin == 1
        obj.index = varargin{1}.index;
        obj.timestamp = varargin{1}.timestamp;
        obj.data = varargin{1}.data;
        obj.nonce = uint32(varargin{1}.nonce);
        assert(isa(obj.nonce, 'uint32'));
        obj.hash = varargin{1}.hash;
        obj.previous_hash = varargin{1}.previous_hash;
      elseif nargin == 6
        obj.index = varargin{1};
        obj.timestamp = varargin{3};
        obj.data = varargin{4};
        obj.hash = varargin{6};
        obj.nonce = varargin{5};
        assert(isa(obj.nonce, 'uint32'));
        obj.previous_hash = varargin{2};
      else
        error('Block creation requires either struct input or six input arguments.');
      end
    end
      end
end
```

Fig. 3. Representation code for blockchain.

small as possible [53–61].

$$loss_i = min \sum_{i=1}^{n} \frac{weight_{in}}{dp_{in}} \tag{11}$$

where

$weight_{in}$, dp_{in} represents input weights and data respectively.

3.1. 2.1 Implementation of FL and blockchain in IoT applications

Input: Initialize the offloading transaction blocks with computational time periods, number of cluster heads, transactions and proportion of data segments in IoT applications using representation values of selected data functions $OT_i(OT_i \leq i \leq n)$, $\gamma_i(\gamma \leq i \leq n)$ and offload period matrix off_i;

Output: Maximize the security with block transactions, data rate representations, minimize the data size of transaction blocks and loss periods;

Step 1: At first, the objective function is constructed with different transaction blocks and one transaction factor value using f_i;

Step 2: Establish the consistency ratio relationship between unsystematically transmitted blocks and working functionalities of IoT devices that must be followed by different load periods $load_i$ with $1 \leq i \leq n$, and its weight matrix representation values $w_1..w_n$ at different marginal functions;

Step 3: While $(accuracy_i < N)$ do.

Select the transmitted blocks and allocated loads, measure the number of tag files with digital signatures using different IoT data set in a systematic way for computing the exact consistency ratio by using Equation (3);

Verify the value of $Energy_i$ and $modifiedEnerigy_i$ using node value set;

If the energy allocations are higher $Energy_i$ is not at $(Energy_i < N)$ do

Divide the layers with aggregate values of different nodes such as initial, transmission and intermediate nodes using number of measurement bits b_i which ensures maximized accuracy conditions using Equation (10) $accuracy_i$ with $1 \leq i \leq N$ into N number of affected points;

// Loss minimization phase

Update the loss factors and weighting units using input weight matrix with minimized loss function using training loss as shown in Equation (11);

//Energy minimization phase

Select the amount of residual period functions with distance measurement representation values of different training samples with separate IoT application analysis in a single output;

Update the energy representation values of relative bit positions and identified position followed by measurement of data security index, and compute the relative weight of all parameters $weight_{in}$ as defined in Equation (11);

Identified loss at each point is updated by using the learning factors and data that is designed for input signals;

$$iter_i(new) = iter_i(old) + 1$$

End;

Step 4: If $(loss_i < iter_i)$ then

$loss_i \leftarrow 0$; //Interchange the existing solution in the current loop with the new solution;

End if;

Step 5: If $(accuracy_i[0,1] < loss_i)$ then

Re-initialize the federated learning factors that are taken with new processing technique;

Obtain the overall best solution;

End if;

Step 6: If $(accuracy_i > N)$ //Existing solution is replaced with the new solution

$$iter_{new} = iter_i$$

$iter_{old} = iter_i$; //Attain the most feasible solutions for determining the overall best solution;

Increment the count $iter_i$ by 1;

Return the best overall solution;

End;

The flow chart in Fig. 2 provides the integration steps of federated learning with block chain that is designed by using RS corda in order to process the implementation for observing parametric outcomes. Therefore the loop functions are determined between start and stop where total number of computational blocks that are represented with maximum values are provided. After creation of various computational blocks the transaction blocks are separated for transferring the data to destination thereby the process of offloading analysis takes place with low load. During the above mentioned process for offloading analysis total delay and data rates are measured for each transaction blocks thereby maintaining a constant rate till the end of transmissions. In addition at this step the objective functions which are termed with multi-objective functionalities are included and energy is modified for each data thereafter at minimized energy rate individual data is transmitted to destination.

4. Results and discussions

To check the security states of the entire system, real-time experimental verifications using a variety of processors are performed in this part. However, the system does not use the microcontroller-based operational processor since the results will be of low security. Following the integration of blockchain methods, more transactions at each block are detected, and their aggregate effects are discussed using the models for the current data set. Additionally, the IoT-based system offers a clear overview of numerous software tools that are employed in the examination process because it's important to examine the systematic behavior of different system characteristics. The IoT node MATLAB toolbox is also used in the suggested method to monitor experimental output unit characteristics that are present in hardware systems. The primary benefit of using such a toolbox over an open source or programming model is that all device connections may be established directly, resulting in a significantly shorter simulation time. Additionally, federated learning processes are integrated as a subsystem at local data bases, combining IoT and learning processes into a single framework. Additionally, very few resources are provided in the system for the output analysis phase because blockchain technology uses more energy when it is waking up. As a result, the resources are only allotted during the listening window during which data from an IoT output unit is relayed to various network systems. Offloading is the above procedure that provides a trade-off between load and allocated energy. Additionally, very few resources are provided in the system for the output analysis phase because blockchain technology uses more energy when it is waking up. As a result, the resources are only allotted during the listening window during which data from an IoT output unit is relayed to various network systems [52]. The following scenarios are about the system model to study the experimental examples.

Scenario 1: Transaction blocks and computational nodes

Scenario 2: Consistency ratio

Scenario 3: Load balancing

Scenario 4: Minimization of modified energy

Scenario 5: Accuracy detection

All five situations are simulated using loop-based formation, which integrates a particular mathematical model with a federated learning process. For various IoT applications, operational tasks and loading levels are also offered. In the proposed method for generating blocks a separate protocol is followed by using R3 corda where a distributed ledger technology is followed for providing consistent ratio among different blocks. R3 corda also provides high flexibility for IoT operations where a cloud computing platform can be connected with various blocks by using an authentication key. Hence only safety blocks are created and data is transmitted in necessary blocks that enable multiple users to remain connected in the network. In R3 corda protocol a strong identification is made and connections in thus type of distributed cases are made by following a progressive flow that allows removal of duplicate blocks thereby the major objective of offloading analysis can be satisfied. In federated learning the amount of training and testing ratio varies according to input data functions and in accordance with each block that is present with active labels. At initial state the training ratio for proposed method is much higher for about 90 % and only 10 % of data is tested. But once the offloading analysis of each blocks are established then 50 % of the data is trained and tested for achieving effecting outcomes. The following are brief descriptions of various scenarios.

Scenario 1

Various cluster heads present at each transaction block are used in this scenario to calculate the number of transaction blocks and computing nodes. For this, the offloading technique is introduced, in which all blocks are solely handled using the fewest possible computational nodes. Due to this minimal allocation, all offloading duties are completed in the shortest time possible, decreasing transmission delay. Each transaction block will be analysed throughout this procedure to verify adequate operational conditions. During this time, the size of data segments will also be noticed, along with different data rates. As a result, the offloading activities that repeat with data size are divided by the transmission rate systems. Additionally, decreasing the number of separated computing nodes is essential, making blockchain operations a better replication technique than alternative security indices. The number of computing nodes in the system, as intended is shown in Fig. 4 and Table 2.

From Fig. 4 it is observed that number of offloading tasks are separated in step size of 20 as 10,30,50,70 and 90 where for each task the following data size 6,15,29,45 and 63 are represented. The reproduction rate of above mentioned values are provided thus the data size is chosen as 2.33,4.56,7.8,9.1 and 11.4 bits and they are separated at output units. After the separation process a comparison is made with existing method [4–7] and it indicates that computational transaction nodes are minimized in proposed method. This minimization process can be proved with 70 different tasks with 45 different data segments and at 9.1 bits per second each data is transmitted where the total computational transaction in this case is 16 for proposed method and 84 for existing approach in the absence of federated learning procedure. Even for all offloading task existing method minimizes the transaction of computational nodes in an effective manner thus making all IoT application to be represented with minimum blocks.

Scenario 2

In this case, the number of unsymmetrical blocks is counted to determine the consistency ratio of the transmission, and the appropriate transmission rates are determined under offloading circumstances. Since the receiver must receive all data in a short time, it is crucial in IoT applications to often evaluate the transmission rate. The ratio must be maintained for a period to distribute all transaction factors. All data processing units will be removed from the network if the ratio exceeds a predetermined threshold, creating duplicated situations. If continuous periods are represented in the system, the consistency ratio for each transmitted data must be higher than 60 % to avoid such redundant conditions. As a result, a transformation factor of 1 must be used to separate the difference between the number of unsymmetrical transmitted blocks and total transaction factors. Fig. 5 and Table 3 shows how the consistency ratio compares with different types of data.

From Fig. 5 it is pragmatic that total number of unsymmetrical blocks are changed in step size of 3 as 3,6,9,12 and 15 respectively. For each unsymmetrical block the number of transaction factors is kept at higher rate as 50,100,150,200 and 250 where the difference between unsymmetrical blocks and transaction factors with separation provides consistency ratio. In addition the measured consistency ratios are compared with existing technique [4–7] where it must be higher than 60

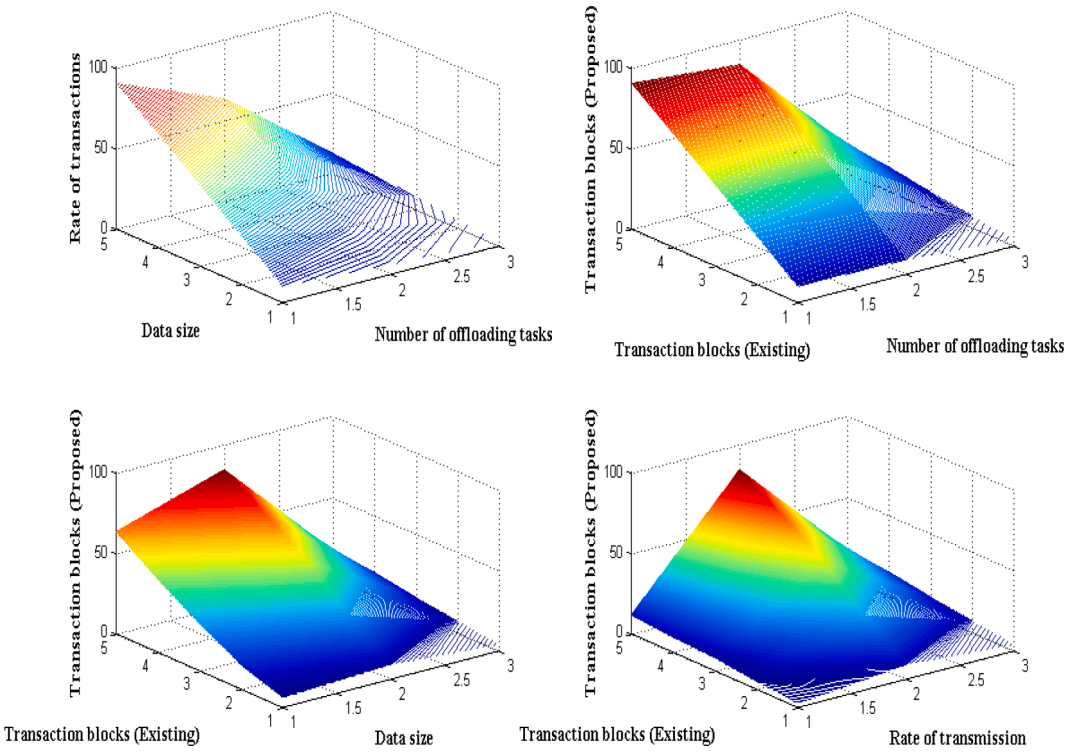

Fig. 4. Number of transaction blocks.

Table 2
Number of transaction blocks.

Number of off-loading task	Data size	Rate of transmission	Transaction blocks [5]	Transaction blocks (Proposed)
10	6	2.33	9	4
30	15	4.56	28	7
50	29	7.8	50	10
70	45	9.1	67	14
90	63	11.4	84	16

percentage. During this comparison case the proposed method achieves 60 percent of consistent rate as compared to existing method. This can be demonstrated using 150 different transaction factor with 9 unsymmetrical blocks where the consistency ratio in this case is 60 percent for existing model and 71 percent for proposed method. But if number of unsymmetrical blocks and transactions are lesser that is at initial phase existing method has not intersected with consistency ratio of 60 percentage.

Scenario 3

The system's data must all be balanced with equal load factors, resulting in an equal distribution of data across resources. Therefore, in this case, the load-balancing strategy is tested using various weight factors ranging from 1 to n. If more weights are assigned, the full load cannot be balanced. Hence the proper weight factor must be present for transmitted blocks. Even in the Internet of Things applications, if the sent data has a distinct weight, it is still possible to share it in a transaction block, but the proper matching level is not offered due to size restrictions. As a result, key processing strategies are created using digital signal representations, and key tag files are linked throughout the process so that, up until the final state, the data is processed using the proper loads. For load distribution, properly implementing the weight matrix with a system for each user's private key decryption is required. The load balanced adequately in IoT applications is shown in Fig. 6 and Table 4.

From Fig. 6 it is realistic that random number of blocks is transmitted as compared to allocated blocks. For real time experimentation number of allocated blocks are considered as 10,15,20,25 and 30 with transmitted blocks as 8,13,16,22 and 27. Thus by examining the above values more than 60 percent of data is successfully transmitted with different loading conditions. In the comparison case [4–7] it is much clear that the proposed method provides successful transmission with low weighting factors but with same allocated and transmission blocks existing method transmits the data using high weights. This can be verified with 20 different number of allocated blocks with 16 transmitted blocks where total data load that is provided in proposed method is 2.06 whereas high load of 6.34 is distributed for existing method. Thus even at low loading conditions it is much easier to transmit necessary data with private keys (see Tables 5 and 6).

Scenario 4

Reduced energy consumption at each data block is one of the main goals of blockchain data transactions. To examine this scenario, energy expenditure at initial, transmitted, and intermediate node representations is analyzed. This scenario generates a real-time energy setup module, which modifies initial energy using distance data. The distance measurement values are therefore observed with the total number of transaction bits and reproduced in the system for a better energy examination case. Although it is even possible to allocate the same amount of energy to process a specific data set when separated, the values for the energy representation must typically be kept to a minimum. Therefore, this technique minimizes the quantity of remaining energy, as seen in Fig. 7. Since the distance measurement values are different, the current method does not use the dataset used in the comparison case for the proposed method.

From Fig. 7 it is perceived that distance measurement values are changed in step size of 50 and clogged at 450 m. For each values of distance measurement number of bits are represented as 2,4,6,8 and 10 respectively where the values are reproduced with common residual energy of 0.45. By using the aforementioned measurement values modified energy of existing and projected methods are compared and in this case proposed method with federated learning uses much lower energy for transmitting high number of data transaction blocks. This can

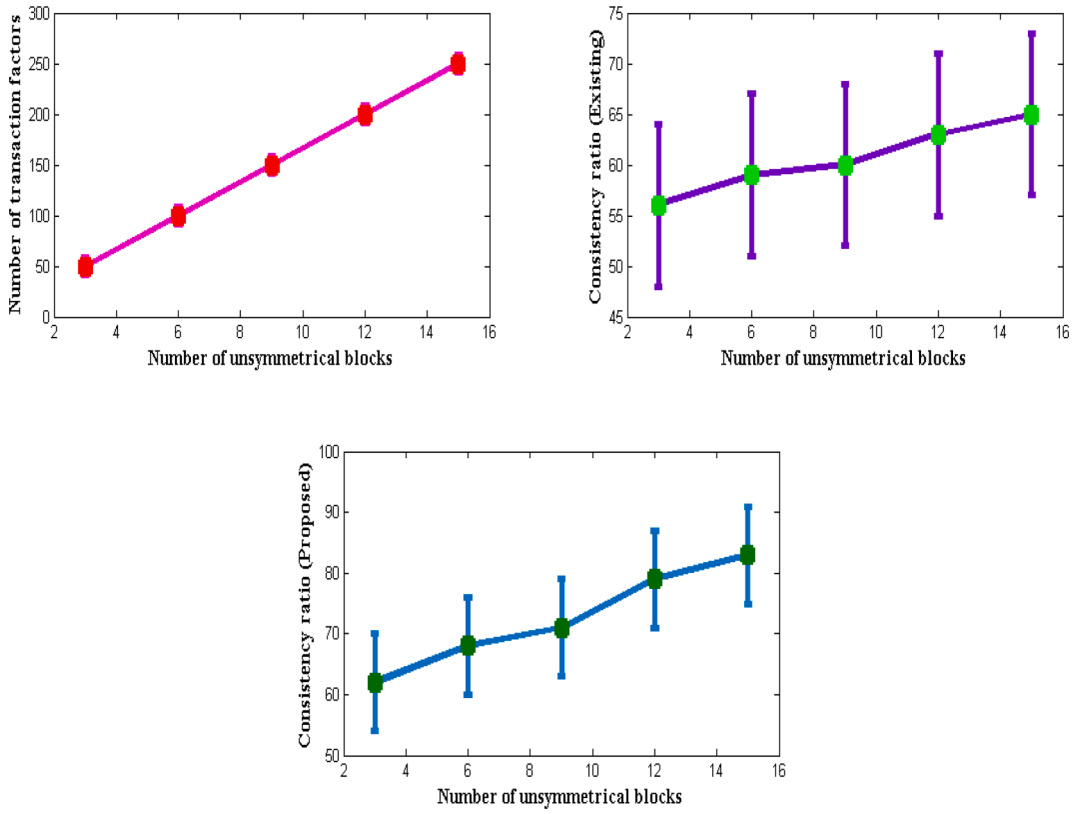

Fig. 5. Consistency ratio of blocks.

Table 3
Block consistency.

Number of unsymmetrical blocks	Number of transaction factors	Consistency ratio [5]	Consistency ratio (Proposed)
3	50	56	62
6	100	59	68
9	150	60	71
12	200	63	79
15	250	65	83

be verified with 250 m of distance with 6 different bit values where the modified energy in this case is 3.67 and for existing approach [4–7] it is equal to 6.79. Even for other cases the proposed method modifies higher energy state to lower state and within the allocated energy itself the data will be successfully transmitted to target blocks at same defined time periods.

Scenario 5

Using federated and data summation values, this scenario examines the correctness of integrating federated learning. Aggregate values are stored in two different layers during this evaluation process, completely minimizing system total loss. The accuracy of the learning model is greatly increased as a result of this minimization. Different weighting factors are generated as part of the process of analyzing system total loss along with the quantity of introduced data in IoT applications. As a result, the complete loss is provided by the separation values and is immediately recreated by federation and data summation values. Therefore, where attention parameters are employed to gauge the accumulation approach, such values must be maximized. Several selected data points are included in the accumulation strategy's system configuration settings. As a result, all data points are separated into real-time values, as shown in Fig. 8. Since there needs to be a secondary back-off state, the additional data sets used in the integration process are not

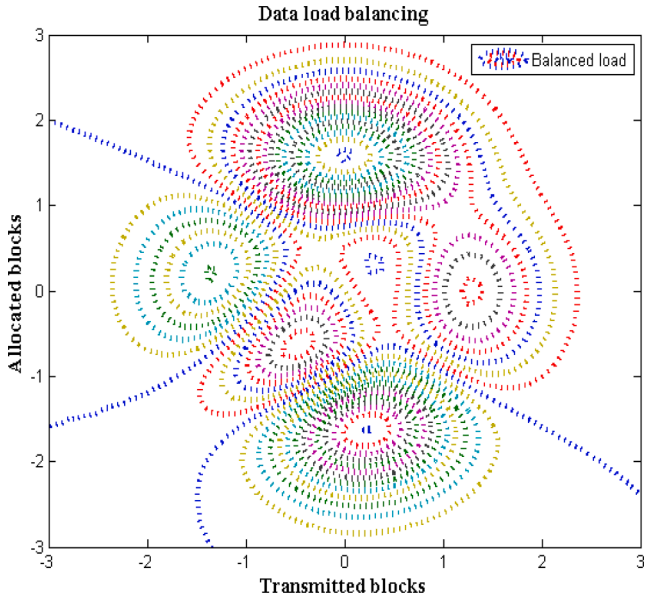

Fig. 6. Data load balancing with transmitted and allocated blocks.

Table 4
Total load for blocks.

Transmitted blocks	Allocated blocks	Load [5]	Load (Proposed)
8	10	3.14	1.23
13	15	5.17	1.76
16	20	6.34	2.04
22	25	7.12	2.16
27	30	8.09	2.27

Table 5
Energy with bit representations.

Distance	Number of bits	Modified energy [5]	Modified energy (Proposed)
50	2	4.56	2.29
150	4	5.18	3.14
250	6	6.79	3.67
350	8	8.9	4.12
450	10	9.2	4.45

Table 6
Comparison of accuracy.

Percentage of loss	Percentage of federated data	Accuracy [5]	Accuracy (Proposed)
20	10	52	84
22	15	57	87
24	20	63	89
26	25	69	92
28	30	74	97

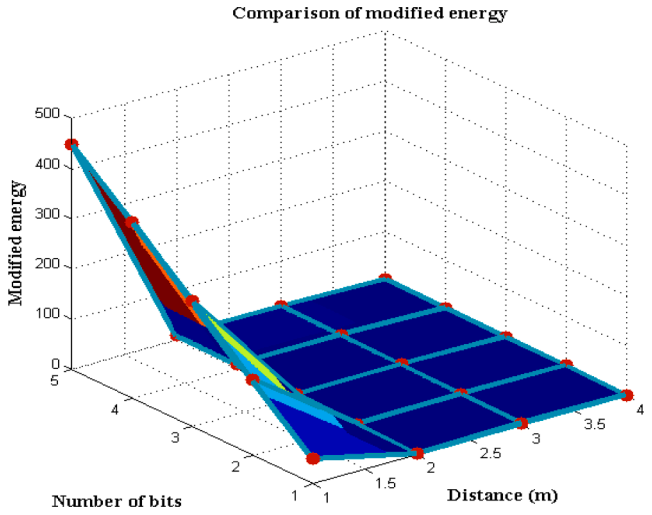

Fig. 7. Modified energy representations.

broken up.

From Fig. 6 it is obscure that percentage of loss at initial stages are much higher than 20 percent but once the process is made with stable configurations then total loss in the system falls beyond 10 percent. However the test case is examined for high loss values such as 20,22,24,26 and 28 with federated learning values as 10,15,20,25 and 30 respectively. During this process the difference in corresponding values provides accuracy percentage and it is compared with existing approach [4–7]. In the comparison state it is pragmatic that percentage of accuracy is highly improved for proposed method using federated learning as 97 percentage of security is provided for different blocks of data. This improvement in accuracy values can be verified with loss percentage of 24 and federated data of 20 where total accuracy is 89 percent for projected technique and 63 percent for existing approach.

4.1. Comparative analysis

The efficiency of the suggested method is compared using several typical phenomena in the section, which bases its use of the federated learning model for IoT applications on distinct specification variables. A method called federated learning is also used, and its effectiveness is judged by the following:

Case study 1: Accurate convergence

Case study 2: Strength of federated learning

Case study 3: Space complexity

Case study 1

Since the convergence factor can vary significantly in some circumstances, examining convergence is conducted using best iteration values. But in the suggested approach, Fig. 9 and Table 7 illustrate and discuss the convergence of the federated learning model about precise measurements. Since many IoT applications send data using high-frequency ranges, there are numerous faults in the additional components. These errors must be eliminated using a smoothing rate, and if such rates are decreased, correct convergence of solutions can be attained in much less time. Additionally, a lot of factors that are directly linked to changes in physical phenomena might alter and lead to the elimination of significant factors that are linked to the development of various systemic blocks. The accuracy of convergence in the system can be considerably enhanced by minimizing the two aforementioned scenarios.

Fig. 9 shows that as smoothing parameters are enhanced, accuracy for federated learning increases significantly. Iteration values are adjusted from 10 to 100 to demonstrate the accuracy factor. Still, to provide an accurate overview, only the best epoch is displayed, and the remaining values are left as indicated in the arrangement. The suggested method reaches convergence during the variations at 50 epochs, and after 50 epochs, the rate stays constant, indicating that block formation does not change significantly. However, the number of duplicate blocks increases without federated learning [5], which lowers accuracy factors.

Case study 2

Determining the strength of the suggested strategy in various IoT applications is crucial because federated learning takes place in various environments. The necessity for other devices to rely on the same device until full strength is present arises when the strength of one particular device is higher. In other words, a system that is extremely resilient to one change in the system cannot also be very present. If federated learning is more robust, parametric values may change from minimum to maximum and vice versa, which needs to be stopped right away. Data for a specific duration will be more inactive, resulting in a loss of data transfer if a learning procedure's avoidance time is considerably longer.

Robustness values associated with changes in iteration values are shown in Fig. 10 and Table 8. Iteration numbers are increased from 10 to 100 to test the data's robustness, but just like in the prior instance, only the best iteration values are selected. The current technique [5] is very resilient to changes in learning circumstances during these periodic changes, as many blocks alter their complete properties due to the lack of key encryption mechanisms. However, because federated learning offers the necessary critical elements, the arrangement's robustness is much reduced, allowing data to flow properly during various IoT applications.

Case study 3

Since more number of transaction blocks are present it is essential to determine the total space that is occupied for each block before creating a data path for transmission. It is well known that before establishment of data paths it is possible that every block can able to occupy more space therefore necessary steps must be taken for removing unnecessary blocks. Further after creating a data path more amount of traffic will be created and in this step various characteristics of every block must also be analysed. Hence it is much essential to allocate space for entire system until all blocks are executed successfully and if any storage space remains unoccupied then it can also be used for decision making. Whenever a block is called with input functions then an individual data variable is created which takes more amount of space and blocks the forthcoming data to remain at queue mode. However in the proposed method the space that is provided to each data functions are much lesser due to involvement of clusters in defined regions. Due to differentiation of data clusters offloading tasks are executed even for unsymmetrical transaction blocks that are present with high weightage factors.

Fig. 11 illustrates the space complexity outcomes and its comparison with existing approach where with low amount of space more data

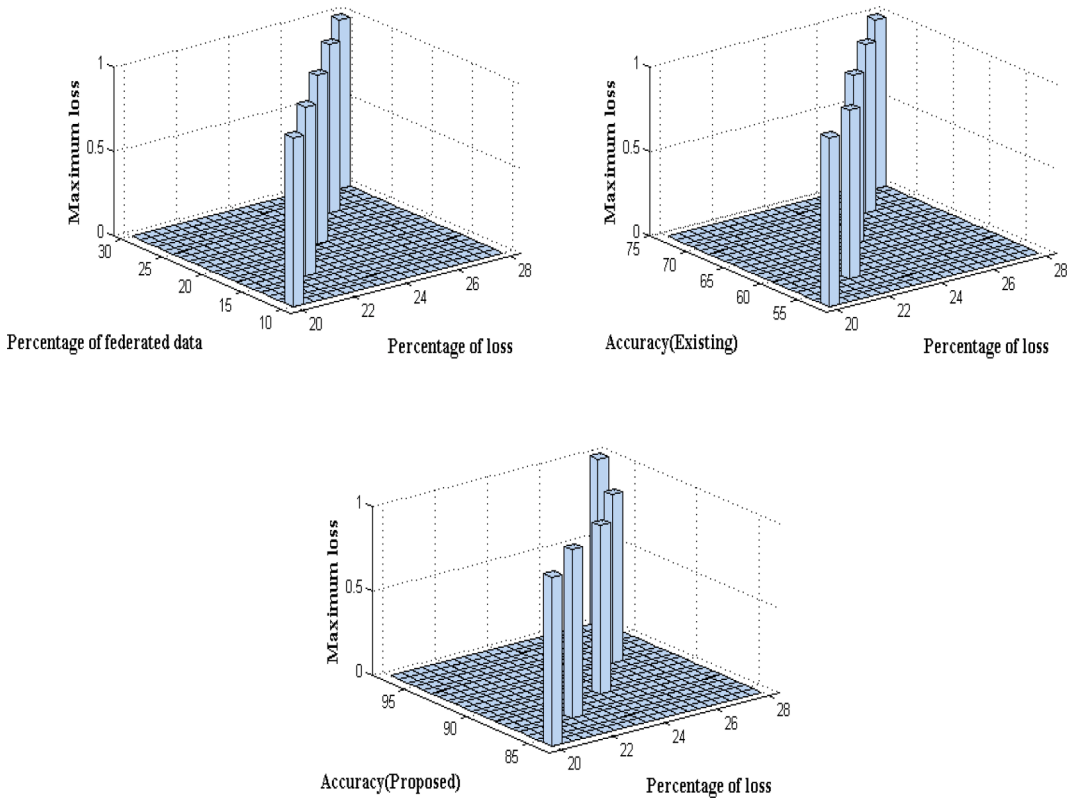

Fig. 8. Accuracy with loss factor.

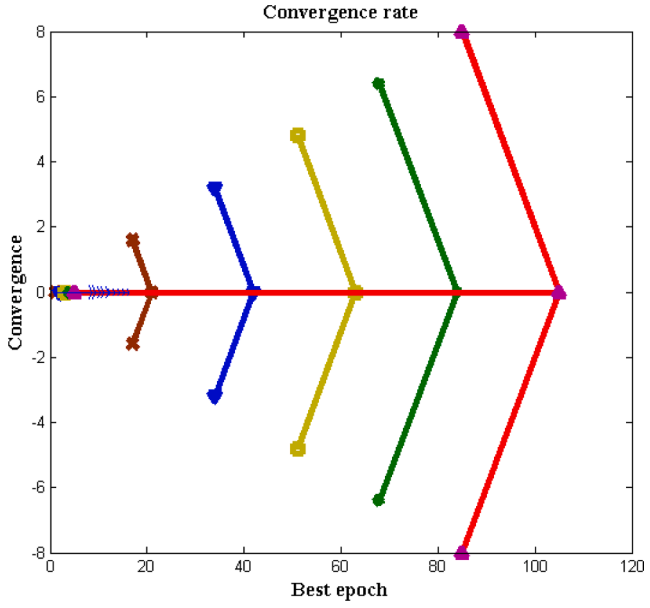

Fig. 9. Convergence rate.

Table 7
Convergence with best epoch.

Best epoch	Convergence [5]	Convergence (Proposed)
20	2.43	1.29
40	2.31	1.25
60	2.24	1.24
80	2.02	1.24
100	1.99	1.24

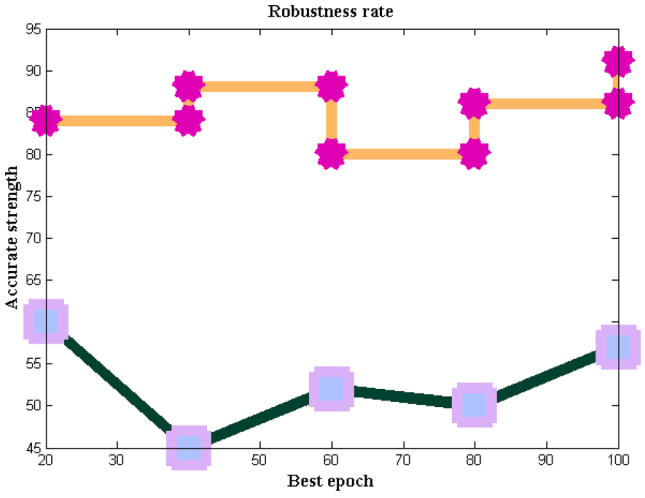

Fig. 10. Comparison of accurate strength.

Table 8
Robustness with best epoch.

Best epoch	Robustness [5]	Robustness (Proposed)
20	60	84
40	45	88
60	52	80
80	50	86
100	57	91

blocks are transmitted for proposed method after monitoring state of necessary applications that is processed in cloud networks. To verify the space complexity total number of iterations are varied from 10 to 100

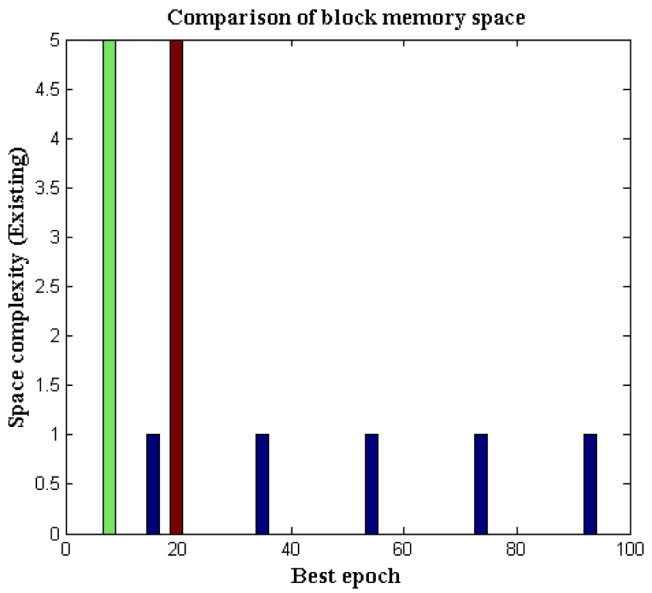

Fig. 11. Comparison of block memory space.

and only the best epoch values for 20 step periods are considered as 20,40,60,80 and 100 respectively. During the above mentioned iteration periods space complexity of proposed method is reduced to 3 % of total transaction blocks whereas the complexity of existing approach even after learning about input functions is increased to 12 %. The major reason for such reductions in space complexity is that collaborative learning functions are included with input data variables that make the offloading task to function in an effective way as compared to existing approach.

5. Conclusions

To provide high-security characteristics for wireless communication devices, the significance of blockchain technology for various IoT applications is investigated as a real-world case study. Wireless data transfer devices come with an inherent security mechanism, but data theft must be prevented by using extra features. When all of the data is transferred in encrypted blocks, network security features are typically supplied in a form that computing systems cannot comprehend. Due to such block transfer technology, the majority of real-time cloud apps that have a larger user base aim to investigate the impact of blockchains. An analytical framework is not, however, positioned as a common application point; rather, the suggested method creates a new system model and implements it in a loop-based style. The proposed method, in contrast to previous blockchain integration strategies, allocates a small number of blocks during the initial transaction, preserving the proper consistency ratio over the data transmission phase.

Additionally, it is crucial that every block understand the full features of the many IoT applications because, during the parametric value monitoring stage, many computational nodes will be adjusted and require precise responses. As a result, the suggested solution includes a federated learning algorithm for computing applications that provides aggregate values during times of low latency. By comparing the values of the existing data set under five different scenarios such as analyzing the number of computational nodes, consistency ratio of node transfer, load balancing, applied energy, and accuracy of integration—the integrated system model with federated learning is tested and simulated.

The major difference between proposed method and existing method in comparison case study is that more number of offloading transactions are present thereby making the designed system to be more secured. Further in each case study the indicated parametric values are represented with minimization and maximization framework where the observation analysis indicates that only unsystematic blocks are transmitted in existing method whereas the process of transmission happens in a systematic procedure in case of projected model. Additional case studies also proves that as compared to existing approaches high consistency in blockchain transmission ratio is made with modified primary energy sources. Hence for approximately 65 percent of the comparisons, the projected method is significantly more effective. The proposed system could be improved in the future to reduce the loss factor and improve detection accuracy by using a deep convolutional neural network. In addition the future work can also be extended by considering various perspectives of effective block functionalities that are defined only with offloading analysis as much energy reductions can be achieved. Also instead of standard functionalities a collaborative functionalities can be added as extension work to increase the testing data values than current operational features.

CRediT authorship contribution statement

S. Shitharth: Conceptualization, Methodology, Software, Writing – original draft. **Hariprasath Manoharan:** Data curation, Writing – original draft. **Achyut Shankar:** Visualization, Investigation. **Rakan A. Alsowail:** Supervision. **Saravanan Pandiaraj:** Software, Validation. **Seyyed Ahmad Edalatpanah:** Writing – review & editing. **Wattana Viriyasitavat:** Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors of this study extend their appreciation to the Researchers Supporting Project number (RSPD2023R544), King Saud University, Riyadh, Saudi Arabia.

References

[1] S. Shitharth, Hariprasath Manoharan, Rakan A. Alsowail, Achyut Shankar, Saravanan Pandiaraj, Carsten Maple, Gwanggil Jeon, 'Development of Edge Computing and Classification using The Internet of Things with Incremental Learning for Object Detection, Internet of Things, 2023,100852, ISSN 2542-6605, doi: 10.1016/j.iot.2023.100852.
[2] Shen Y, Gou F, Wu J. Node Screening Method Based on Federated Learning with IoT in Opportunistic Social Networks. Mathematics 2022;10. https://doi.org/10.3390/math10101669.
[3] El Saddik A, Laamarti F, Alja'Afreh M. The Potential of Digital Twins. IEEE Instrum Meas Mag 2021;24(3):36–41.
[4] Rawat, R., Oki, O.A., Sankaran, K.S., Olasupo, O., Ebong, G.N., Ajagbe, S.A. (2023). A New Solution for Cyber Security in Big Data Using Machine Learning Approach. In: Shakya, S., Papakostas, G., Kamel, K.A. (eds) Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, vol 166. Springer, Singapore. doi: 10.1007/978-981-99-0835-6_35.
[5] Moser A, Appl C, Brüning S, Hass VC. Mechanistic Mathematical Models as a Basis for Digital Twins. Adv Biochem Eng Biotechnol 2021;176:133–80.
[6] Vijarania, M., Gupta, S., Agrawal, A., Adigun, M. O., Ajagbe, S. A., & Awotunde, J. B. (2023). Energy Efficient Load-Balancing Mechanism in Integrated IoT-Fog-Cloud Environment. Electronics, 12(11), 2543. MDPI AG. Retrieved from https://doi.org/10.3390/electronics12112543.
[7] iAwotunde, J.B. Oguns, Y.J., Amuda, K. A., Nigar, N., Adeleke T. A., Olagunju, K. M., Ajagbe, S. A. (2023). Cyber-Physical Systems Security: Analysis, Opportunities, Challenges, and Future Prospects. In: Maleh, Y., Alazab, M., Romdhani, I. (eds) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security, vol 102. Springer, Cham. Pp 21-46, doi: 10.1007/978-3-031-25506-9_2.
[8] Alhalabi W, Al-Rasheed A, Manoharan H, Alabdulkareem E, Alduailij M, Alduailij M, et al. Distinctive Measurement Scheme for Security and Privacy in Internet of Things Applications Using Machine Learning Algorithms. Electronics 2023;12:747. https://doi.org/10.3390/electronics12030747.
[9] Hafid A, Hafid AS, Samih M. New mathematical model to analyze security of sharding-based blockchain protocols. IEEE Access 2019;7:185447–57.
[10] Hasan HR, Salah K, Jayaraman R, Omar M, Yaqoob I, Pesic S, et al. A Blockchain-Based Approach for the Creation of Digital Twins. IEEE Access 2020;8:34113–26.

[11] Xie R, Chen M, Liu W, Jian H, Shi Y. Digital twin technologies for turbomachinery in a life cycle perspective: A review. Sustain 2021;13:1–21.
[12] Bevilacqua, M.; Bottani, E.; Ciarapica, F.E.; Costantino, F.; Donato, L. Di; Ferraro, A.; Mazzuto, G.; Monterìù, A.; Nardini, G.; Ortenzi, M.; et al. Digital twin reference model development to prevent operators' risk in process plants. Sustain. 2020, 12, 1–17.
[13] Elmamy SB, Mrabet H, Gharbi H, Jemai A, Trentesaux D. A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0. Sustain 2020;12:1–19.
[14] Jesus EF, Chicarino VRL, De Albuquerque CVN, Rocha AADA. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Secur Commun Networks 2018, 2018..
[15] Rao YS, Rauta AK, Saini H, Panda TC. Mathematical model for cyber attack in a computer network. Int J Bus Data Commun Netw 2017;13:58–65.
[16] Saini DK. Cyber Defense: Mathematical Modeling and Simulation. Int J Appl Phys Math 2012;2:312–5.
[17] Massel LV, Massel AG. Development of Digital Twins and Digital Shadows of Energy Objects and Systems Using Scientific Tools for Energy Research. E3S Web Conf 2020:209.
[18] Hu K, Wu J, Li Y, Lu M, Weng L, Xia M. FedGCN: Federated Learning-Based Graph Convolutional Networks for Non-Euclidean Spatial Data. Mathematics 2022;10: 1–24.
[19] Whaiduzzaman M, Mahi MJN, Barros A, Khalil MI, Fidge C, Buyya R. BFIM: Performance Measurement of a Blockchain Based Hierarchical Tree Layered Fog-IoT Microservice Architecture. IEEE Access 2021;9:106655–74. https://doi.org/10.1109/ACCESS.2021.3100072.
[20] Soret B, Nguyen LD, Seeger J, Broring A, Ben Issaid C, Samarakoon S, et al. Learning, Computing, and Trustworthiness in Intelligent IoT Environments: Performance-Energy Tradeoffs, IEEE Trans. Green. Commun Netw 2022;6:629–44. https://doi.org/10.1109/TGCN.2021.3138792.
[21] Adil O. Khadidos , S. Shitharth ,Alaa O. Khadidos , K. Sangeetha, and Khaled H. Alyoubi, "Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism," Journal of Sensors, vol. 2022, Article ID 8457116, 17 pages, 2022. doi: 10.1155/2022/8457116.
[22] Uddin M, Selvarajan S, Obaidat M, Arfeen SU, Khadidos AO, Khadidos AO, et al. From Hype to Reality: Unveiling the Promises, Challenges and Opportunities of Blockchain in Supply Chain Systems. Sustainability 2023;15(16):12193. https://doi.org/10.3390/su151612193.
[23] Manoharan, H., Manoharan, A., Selvarajan, S., & Venkatachalam, K. "Implementation of Internet of Things With Blockchain Using Machine Learning Algorithm: Enhancement of Security With Blockchain." Handbook of Research on Blockchain Technology and the Digitalization of the Supply Chain, edited by Tharwa Najar, et al., IGI Global, 2023, pp. 399-430. doi: 10.4018/978-1-6684-7455-6.ch019.
[24] Selvarajan S, Mouratidis H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Sci Rep 2023;13(1):7107. https://doi.org/10.1038/s41598-023-34354-x.
[25] Aluvalu R, Kumaran V. N. S, Thirumalaisamy M, Basheer S, Ali aldhahri E, Selvarajan S. 2023. Efficient data transmission on wireless communication through a privacy-enhanced blockchain process. PeerJ Computer Science, doi: 10.7717/peerj-cs.1308.
[26] Selvarajan S, Srivastava G, Khadidos AO, Khadidos AO, Baza M, Alsheri A, et al. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. J Cloud Comp 2023:12–38.
[27] Ahmed AH, Omar NM, Ibrahim HM. Performance evaluation of a secured framework for iot based on blockchain. J Commun 2022;17:1–10. https://doi.org/10.12720/jcm.17.1.1-10.
[28] Duan R, Guo L. Application of Blockchain for Internet of Things: A Bibliometric Analysis. Math Probl Eng 2021;2021. https://doi.org/10.1155/2021/5547530.
[29] S. Shitharth, G.B. Mohammed, J. Ramasamy, R. Srivel, (2023). Intelligent Intrusion Detection Algorithm Based on Multi-Attack for Edge-Assisted Internet of Things. In: G. Srivastava et al. (eds.), Security and Risk Analysis for Intelligent Edge Computing, Advances in Information Security 103, doi: 10.1007/978-3-031-28150-1_6.
[30] Amanat M, Rizwan C, Maple YB, Zikria AS, Almadhor SWK. Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. Front Public Heal 2022;10. https://doi.org/10.3389/fpubh.2022.938707.
[31] Miralles-Quirós JL, Miralles-Quirós MM. Mathematics. Cryptocurrencies and Blockchain Technology 2022. https://doi.org/10.3390/math10122038.
[32] Guo H, Yu X. A survey on blockchain technology and its security. Blockchain Res Appl 2022;3:100067. https://doi.org/10.1016/j.bcra.2022.100067.
[33] Zheng J, Dike C, Pancari S, Wang Y, Giakos GC, Elmannai W, et al. An In-Depth Review on Blockchain Simulators for IoT Environments. Futur Internet 2022;14: 1–22. https://doi.org/10.3390/fi14060182.
[34] Alferaidi K, Yadav Y, Alharbi W, Viriyasitavat S, Kautish G. Dhiman, Federated Learning Algorithms to Optimize the Client and Cost Selections. Math Probl Eng 2022;2022.
[35] Shitharth S, Manoharan H, Alsowail RA, Shankar A, Pandiaraj S, Maple C, et al. Development of Edge Computing and Classification using The Internet of Things with Incremental Learning for Object Detection. Internet of Things 2023;23: 100852. https://doi.org/10.1016/j.iot.2023.100852.
[36] Khadidos AO, Khadidos AO, Selvarajan S, Mirza OM. TasLA: An innovative Tasmanian and Lichtenberg optimized attention deep convolution based data fusion model for IoMT smart healthcare. Alex Eng J 2023;79:337–53. https://doi.org/10.1016/j.aej.2023.08.010.
[37] Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access 2022;10:57143–79.
[38] Colombo P, Ferrari E. Access control technologies for Big Data management systems: literature review and future trends. Cybersecurity 2019;2.
[39] Song G, Wang Y, Li Y. Dynamic Mathematical Model of Information Spreading on News Platform. Wirel Commun Mob Comput 2021;2021.
[40] Chen A, Lu G, Xing H, Xie Y, Yuan S. Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments. Int J Distrib Sens Networks 2020;16.
[41] Aftab, M.U.; Munir, Y.; Oluwasanmi, A.; Qin, Z.; Aziz, M.H.; Zakria; Son, N.T.; Tran, V.D. A Hybrid Access Control Model with Dynamic COI for Secure Localization of Satellite and IoT-Based Vehicles. IEEE Access 2020, 8, 24196–24208.
[42] Papakonstantinou N, Van Bossuyt DL, Linnosmaa J, O'Halloran B, Hale B. A Zero Trust Hybrid Security and Safety Risk Analysis Method. J Comput Inf Sci Eng 2021; 21.
[43] R.karthickeyan, B. Sundaravadivazhagan, Robin Cyric, Praveen Kumar and S. Shitharth, "Preserving Resource Handiness and Exigency-Based Migration Algorithm (PRH-EM) for Energy Efficient Federated Cloud Management Systems," Mobile Information Systems, vol. 2023, Article ID 7754765, 11 pages, 2023. doi: 10.1155/2023/7754765.
[44] Saisree, S., Shitharth, S. (2022). A Comprehensive Study on Eucalyptus, Open Stack and Cloud Stack. In: Kumar, A., Fister Jr., I., Gupta, P.K., Debayle, J., Zhang, Z.J., Usman, M. (eds) Artificial Intelligence and Data Science. ICAIDS 2021. Communications in Computer and Information Science, vol 1673. Springer, Cham. doi: 10.1007/978-3-031-21385-4_33.
[45] Elangovan, G.R.; Kumanan, T. Energy Efficient and Delay Aware Optimization Reverse Routing Strategy for Forecasting Link Quality in Wireless. Wirel. Pers. Commun. 2022.
[46] Kesarwani A, Khilar PM. Development of trust based access control models using fuzzy logic in cloud computing. J King Saud Univ – Comput Inf Sci 2022;34: 1958–67.
[47] Fu W, Liu S, Srivastava G. Optimization of big data scheduling in social networks. Entropy 2019;21:1–16.
[48] Al-Ani K, Arfeen Laghari SU, Manoharan H, Selvarajan S, Uddin M. Improved transportation model with internet of things using artificial intelligence algorithm. Comput Mater Continua 2023;76(2):2261–79.
[49] Decusatis, C.; Liengtiraphan, P.; Sager, A.; Pinelli, M. Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. Proc. - 2016 IEEE Int. Conf. Smart Cloud, SmartCloud 2016 2016, 5–10.
[50] A.K. Al-ani, S. Ul, A. Laghari, H. Manoharan, S. Selvarajan, M. Uddin, Improved Transportation Model with Internet of Things Using Artificial Intelligence Algorithm, (2023). doi: 10.32604/cmc.2023.038534.
[51] Chang D, Sun W, Yang Y, Wang T. A Dynamic Access Control Method for SDN. J Comput Commun 2019;07:105–15.
[52] Ojo OS, Oyediran MO, Bamgbade BJ, Adeniyi AE, Ebong GN, Ajagbe SA. Development of an Improved Convolutional Neural Network for an Automated Face Based University Attendance System. ParadigmPlus 2023;4(1):18–28. https://doi.org/10.55969/paradigmplus.v4n1a2.
[53] M.A. Hameed, M. Hassaballah, M.E. Hosney, A. Alqahtani, An AI-Enabled Internet of Things Based Autism Care System for Improving Cognitive Ability of Children with Autism Spectrum Disorders, 2022 (2022).
[54] Abdel M, Omar H, Aleem AA. A secure data hiding approach based on least – significant – bit and nature – inspired optimization techniques. J Ambient Intell Hum Comput 2023;14:4639–57. https://doi.org/10.1007/s12652-022-04366-y.
[55] M. Hassaballah, M.A. Hameed, M.H. Alkinani, Introduction to digital image steganography, (2020) 1–15. doi: 10.1016/B978-0-12-819438-6.00009-8.
[56] M. Hassaballah, M.A. Hameed, S. Aly, A.S. Abdelrady, method based on ADPVD and HOG, Elsevier Inc., 2020. doi: 10.1016/B978-0-12-819438-6.00010-4.
[57] M. Hassaballah, M.A. Hameed, A.I. Awad, S. Member, K. Muhammad, A Novel Image Steganography Method for Industrial Internet of Things Security, 3203 (2021) 1–9. doi: 10.1109/TII.2021.3053595.
[58] M.A. Hameed, M. Hassaballah, S. Aly, A.I. Awad, An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques, IEEE Access. PP (2019) 1. doi: 10.1109/ACCESS.2019.2960254.
[59] M. Abdel, H. Saleh, M. Hassaballah, An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD), (2017). doi: 10.1007/s11042-017-5056-4.
[60] L. Emerging, S. Conference, An Artificial Intelligence Based Technique for COVID-19 Diagnosis from Chest X-Ray ., (2020) 191–195.
[61] M.A. Kenk, M. Hassaballah, Visibility Enhancer : Adaptable for Distorted Traffic Scenes by Dusty Weather, (2020) 213–218.