Computers, Materials & Continua
DOI: 10.32604/cmc.2022.030018
Article

Tech Science Press

Mutated Leader Sine-Cosine Algorithm for Secure Smart IoT-Blockchain of Industry 4.0

Mustufa Haider Abidi*, Hisham Alkhalefah and Muneer Khan Mohammed

Industrial Engineering Department, College of Engineering, King Saud University, P.O. Box-800, Riyadh, 11421, Saudi Arabia
*Corresponding Author: Mustufa Haider Abidi. Email: mabidi@ksu.edu.sa
Received: 16 March 2022; Accepted: 31 May 2022

Abstract: In modern scenarios, Industry 4.0 entails invention with various advanced technology, and blockchain is one among them. Blockchains are incorporated to enhance privacy, data transparency as well as security for both large and small scale enterprises. Industry 4.0 is considered as a new synthesis fabrication technique that permits the manufacturers to attain their target effectively. However, because numerous devices and machines are involved, data security and privacy are always concerns. To achieve intelligence in Industry 4.0, blockchain technologies can overcome potential cybersecurity constraints. Nowadays, the blockchain and internet of things (IoT) are gaining more attention because of their favorable outcome in several applications. Though they generate massive data that need to be effectively optimized and in this research work, deep learning-based techniques are employed for this. This paper proposes a novel mutated leader sine cosine algorithm-based deep convolutional neural network (MLSC-DCNN) in order to attain a secure and optimized IoT blockchain for Industry 4.0. Here, an MLSC is hybridized using a mutated leader and sine cosine algorithm to enhance the weight function and minimize the loss factor of DCNN. Finally, the experimentation is carried out for various simulation measures. The comparative analysis is made for Best Tip Selection Method (BTSM), Smart Block- Software Defined Networking (SDN), and the proposed approach. The evaluation results show that the proposed approach attains better performances than BTSM and SDN.

Keywords: Industry 4.0; internet of things (IoT); blockchain; deep convolutional neural network; mutated leader

1 Introduction

The Internet of Things (IoT) connects actuation and sensing devices to collect information from distant surroundings and share it with various platforms for efficiency, better control, and accuracy. Currently, IoT devices are a significant part of digital control systems, environmental monitoring systems, smart homes, supply chain management, surveillance, and security [1]. The IoT devices can

execute tasks and commissions which mankind could not perform. The unmanned aerial vehicle is called a drone that is the microcosms of the IoT and performs large-scale activities from supplying a pack to tracing the crop qualities [2]. The authenticity and security of these devices are complicated because they have budgetary limitations like limited memory, low power requirements, and low area budget. The power limitation in the IoT devices bounds the encrypting function to sensor nodes, which leads to poor encryption communication. The information system includes global controlled blockchain datasets for availability, identity purposes, and integrity [3]. Blockchain technologies are used to track, coordinate, and store information from a huge number of devices and allow application creation that does not require a centralized cloud [4]. For the last two years, blockchain technology has been developing at an astonishing speed. Then the blockchain develops continually, adding extra blocks at each time interval. The full node holds the duplicate of the entire blockchain that includes the information of user balances and addresses. The blockchain contribution is the implementation of transactions via another person or entity that does not rely on third parties [5]. Blockchain 1.0 is usually connected with payment and cryptocurrency. Blockchain 2.0 is connected through automatic digital finance utilizing smart contracts. Blockchain 3.0 is concentrated on tackling the requirements of digital society like industry 4.0 and smart cities. The IoT and other associated technologies significantly fuel the fourth industry revolution (industry 4.0). Industry 4.0 results in a connected factory system [6]. It is the combination of several advanced technologies [7,8].

The German government first established the concept of industry 4.0 in 2011. Industry 4.0 consists of modern digital technology for operations and physical productions; it also focuses on machine learning, interconnectivity, and real-time control and monitoring [9]. Industry 4.0 allows the manufacturing traditions through modern techniques for creating intelligent environments. Manufacturing is a complicated system of complex functions that consists of components like end-end operational visibility, safety control, value chain integration, and performance optimization [10]. During the last decade, with the advent of Industry 4.0, contemporary technologies such as IoT, blockchain, virtual/augmented reality, and machine learning technologies have been widely investigated by researchers worldwide for various applications [11–13]. Khan et al. [14] presented an Recurrent Neural Network (RNN)-based hybrid model using Advanced Deep Learning (ADL) approaches. Deep learning is a contemporary advanced method under artificial intelligence for analyzing data and make accurate predictions based on that [15]. Hence, gated recurrent units (GRU) and Long Short-term memory (LSTM) models using Genetic algorithm (GA) optimization to improve the hybrid model's parameters could be allowed. Moreover, GA to identify the best training parameters before GRU is used to cascade LSTM. Numerous users evaluate the performance of this approach. This method aims to assist supply chain practitioners in making use of the standard approach, and it will also help the industry make policies based on ADL predictions. Hence, all these advancements in the field of computer science is paving way for progressions in manufacturing field, healthcare, smart-homes, transportation, etc. [16–21].

Jamil et al. [22] presented a blockchain-enabled greenhouse system optimization technique. The suggested system operates in three steps to offer an ideal greenhouse environment: optimization, controlling, and prediction. Initially, the Kalman filter method was used to anticipate greenhouse sensor data. The best parameters for the interior greenhouse environment were then determined in the following stage. Finally, the control module uses the optimal parameters to manage and operate the actuator's condition in order to get the required interior environment. Also, this technique created an emulation tool for accessing the performance of the suggested greenhouse system. The proposed system has been compared and studied to the baseline method in energy consumption and production rate. The collected findings showed that the recommended optimization strategy enhanced energy

usage by 41% compared to the baseline scheme and 19% compared to the prediction-based approach. A series of experiments on latency, resource use, and throughput utilizing Hyperledger calliper for experimental analysis.

Rahman et al. [23] proposed a layered hierarchical design for deploying a distributed still Software-Defined Network (SDN)-IoT framework with blockchain capabilities. It provides a safe network connection and effective cluster-head selection by isolating and detecting rouge switches. Furthermore, the flow-rules record enabled by Blockchain keeps account of the rules implemented in the switches and ensures consistency. Then, the suggested framework's performance in a simulated environment demonstrates that it is capable of achieving end-to-end latency, throughput, and optimal energy utilization compared to specified baselines, hence achieving security and efficiency in the smart network.

Rane et al. [24] proposed industrial pump optimization with an IoT approach, which has lately received a lot of interest in the context of Industry 4.0. To monitor, an industrial pump was IoTized and Sensorized its activities in real-time and took forecast steps for more agile asset management. The architecture was further improved to advocate the usage of blockchain and how it will help the organization. In developing the solution, Fault Tree Analysis (FTA) was used to do root-cause analysis, and the system's dependability was validated using on-field failure data. Based on the identified underlying causes, parameters were determined, sensors were added to the system to collect the same information, a solution was built utilizing the entire IoT package, and data were recorded in real-time.

Li et al. [25] presented an enhanced PBFT (Practical Byzantine Fault Tolerance) blockchain consensus method based on a punishment strategy and reward to create a lightweight blockchain. Furthermore, RS erasure the code-based blockchain storage optimization method to decrease store overhead while preserving blockchain recoverability. Experiment findings suggest that the solutions can minimize consensus time, blockchain storage costs, and communication resources required for consensus.

Leng et al. [26] provided a comprehensive literature survey about securing the intelligent manufacturing domain of Industry 4.0 with the help of blockchain technology. It was reported that cybersecurity issues are still a challenge for adopting smart manufacturing. Rathee et al. [27] presented a framework for securing the use of wireless IoT devices in industrial environment by utilizing blockchain. The proposed methodology was tested against security threats through simulation, and it was reported that the developed method performed efficiently. In an another research, the utilization of blockchain and IoT for enhancing traceability in a manufacturing firm was presented [28]. It was reported that through these technologies the visibility and data tracking of whole supply chain can be enhanced.

In IoT, the data provenance schemes are the only way to ensure reliability. These schemes provided information through the evaluation and origin of the data, like different phases of data modification and data creation. The provenance scheme stores the information in a replicable and tamper-proof way [29]. Data provenance determines the trust in the creation and origin of the data process. This assures users of trusting the data obtained from IoT devices. The proper operation for IoT is data provenance or self-trust. Most data provenance techniques utilize hardware security originals, while other methods use wireless channels [30,31]. This paper proposes a novel deep learning technique to achieve an effective blockchain-IoT framework. The vital contributions of the article are delineated below:

- To propose a novel mutated leader sine cosine algorithm based deep convolutional neural network (MLSC-DCNN) in order to attain a secure IoT blockchain of Industry 4.0.

- A hybrid MLSC algorithm is proposed, thus optimizing the parameters (i.e., weight and loss functions) of the DCNN technique.
- To compare the proposed MLSC-based DCNN technique with various other blockchain-based methods to evaluate the system's effectiveness.

The remaining part of the article is enumerated as follows: In the second section, some past literature works based on blockchain mechanisms are discussed. The proposed methodology describes the proposed MLSC-based DCNN for secure blockchain in Industry 4.0 in the third section. The fourth section presents the experimental evaluations and discussions, and finally, the last section provides the conclusions inferred from the research work.

2 Proposed Methodology

The incorporation of Industry 4.0 in the industrial sector makes it an active target for attackers to break in and access an intellectual property. If these attacks are not identified in the first place, it results in intellectual property theft, industrial espionage, sabotage and disruptions, etc. The attacks are increasing against intellectual property by the deployment of connected systems. Dark web monitorization, which is part of the threat intelligence, can be used as a warning system to detect planned assaults. So, the company can immediately respond to protect its physical infrastructure and digital corporate assets.

An IoT and blockchain-based provenance system in cybersecurity using Deep CNN-based Mutated Leader Sine Cosine (MLSC) Algorithm for Industry 4.0 are proposed in this research work. For our proposed method Hyperledger Fabric is employed as blockchain. Fig. 1 shows the overall architectural model of the IoT and blockchain provenance system. In this proposed model, the users are the owners of the connected devices. The users store their personnel files and also use smart contracts. The central processing unit is responsible for identifying malicious activities and implementing strong security in place. If any abnormalities are identified, the data is transferred to the operational technology unit. Initially, the IoT devices register their details with the blockchain network, and each device is given a unique identifier. In the next step, the tasks that need to be allocated for each device that is a member of the network are generated. The tasks in the network have a different number of parameters associated with them, such as the task ID, device ID, user information, etc., which the data owner mainly specifies. The device mainly submits the transaction proposal to the smart contract which is executed by the blockchain network. The completed transaction information is updated in the ledger, and a notification is also sent about whether the transaction is succeeded or failed. The task allocation from actuators or sensors is the last step.

2.1 Blockchain Framework

Blockchain is considered as a distributed data technology. In the computer network security field, the blockchain method is used for data recording by a hash function, and various authentication methods were utilized for securing the network. Generally, the server is used for user authentication, and the blockchain is considered a peer-to-peer network because it has no centralized system [14]. For user verification of this network, digital signature technology is used, and this technology comes under the encryption algorithm. Blockchain users are using asymmetric encryption methods to denote their identity. Users protected the private key, and the public key was distributed to others. The private key is employed in transmitting information by the user, and the corresponding public key verifies the authenticated data. Blockchain also offers the required features of smart contracts for automating the trade among two parties, devoid of using an intermediary. The smart contract is considered a soft

contract that is written from the programming language. Blockchain has various nodes in which each node comprises the replicate of a permanent chain. The permanent chain has multiple blocks, and each block comprises timestamps, hash values, and encrypted data. Endpoint security is only used for the protection of end-user nodes or endpoints and is represented as the access point of the blockchain. Securing endpoints and securing the supply chain are more essential for malicious parties. The entire assort of nodes in the network, like orders, clients, as well as admins, are required the certificates for interacting with the network.

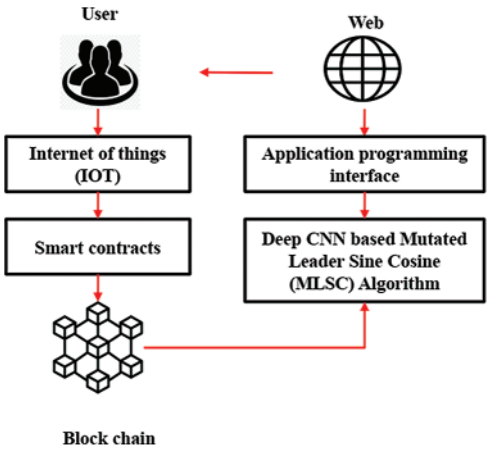

Figure 1: Overall structure of the proposed model

2.2 Integration of IoT with Blockchain

The blockchain is defined as a critical technology that will mainly concentrate on transforming information. Blockchain integration in industry 4.0 is helpful in saving time and task automation. The integration process performs some functions such as task generation, task verification, device registration, and task allocation. The first step of the integration process is to register a particular device present within the network. The service provider is used in registering the device, and every device accepts to create communication with other devices. The second process creates the tasks for devices to define the information about tasks, including participant information, device ID, task ID, and device data. This stage ejects the information from the nodes, whether the transaction was failed or succeeded. The third stage is denoted task allocation from the sensors. When the network allows requests, the sensing task information is ejected from the nodes, and this information will be assigned to the sensor. The final step involves the task verification process; according to the rules, the smart contract was employed for the task verification process. This set of rules was determined at the time of constructing the network.

2.3 Proposed MLSC Based DCNN for IoT Blockchain

This section depicts a brief description of a novel mutated leader sine cosine algorithm-based deep convolutional neural network (MLSC-DCNN) to attain a secure IoT blockchain of Industry 4.0. The techniques employed in the proposed methodology are discussed in the following subsections.

2.3.1 Deep Convolutional Neural Networks (DCNN)

CNN (Convolutional Neural Network) is a variety of Deep Artificial Neural Network which is used to classify and organize the images into groups by their similarity [32–34]. This CNN algorithm is used to recognize human poses, street signs, faces, tumors, characters, etc. Data classification is an important step in CNN [35,36]. The CNN is formed of one fully connected layer, two pooled layers, and three convolutional layers, as represented in Fig. 2.

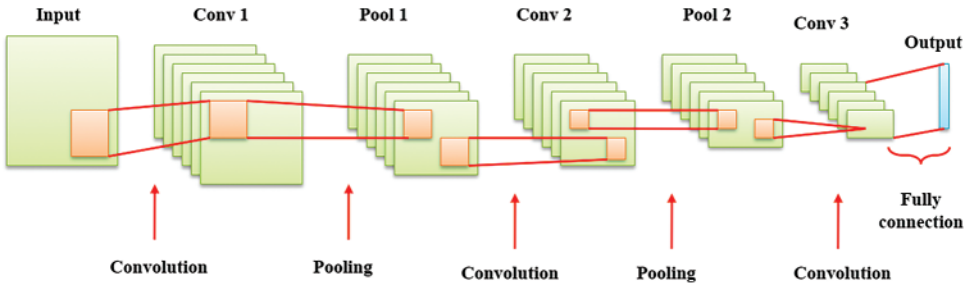

Figure 2: DCNN structure

Convolutional layer:

Convolutional layers (CL) are one of the most significant procedures in CNN. The output from the previous layer is fed as the input layer to each CL which is similar to the traditional neural network. Each CL feature graph corresponds to the same size kernel convolution, and each CL feature map is twisted with the feature map of the preceding layer. After this procedure, bias is added, followed by the equivalent element produced by the activation function. Where the first CL C1's convolutional kernel size is 5×5 and the base layer C2 and C3's convolutional kernel size is 3×3, which is relative to 5×5 and for even better outcomes. The final two convolutions employ 3×3 for better outcomes since two 3×3 boost the non-linear capabilities of the network, increasing the discrimination of the decision function. But, when the first layer is 3×3, the overall network model parameters will be too little, resulting in a performance drop. The layer is expressed as follows:

$$y_j^{layer} = a\left(\sum_{j \in F_z^{layer-1}} y_j^{layer-1} c_{jz}^{layer} + b_z^{layer}\right) \tag{1}$$

The term a denotes the activation function, c represents the convolutional kernel, b represents the bias, and F_z denotes the feature map.

Pooling layer:

In general, the dimension of the output feature maps created after the CL computation is not considerably decreased. If the variation in dimension does not occur, then a large amount of computation is required. This will be extremely challenging to obtain a fair outcome through the process of network learning. This pooling layer of CNN simplifies the output by executing non-linear down-sampling as well as reducing the parameters of the network wants to learn while maintaining the number of feature graphs.

Rectified linear unit (ReLU):

ReLU is the activation function commonly employed in deep learning models, which is its arguments' positive part. When the rectifier obtains any negative inputs, it is returned to zero. The mathematical representation of this is following:

$$f(y) = \max(0, y) \tag{2}$$

Fully connected layer:

In a neural network, the high-level reasoning is done through fully connected layers after max-pooling layers and several convolutions for the network. All neurons are connected to the previous layers' activators in fully connected layers. This creates a classifier called Multi-Layer Perceptron (MLP).

Output layer:

The softmax regression classifier is used in the classifier layer, which is the CNN's output layer. For the training, the data y is entered. The output category $O \in \{1, 2, \ldots, h\}$, with total h classes. In order to enhance the weight function and minimize the loss value, this paper proposes a mutated leader sine cosine algorithm (MLSC). Thus by employing the MLSC algorithm, the weight functions of DCNN are optimized. The following subsection elaborates on the numerical expression for both ML and SC techniques.

2.3.2 Mutated Leader (ML) Algorithm

ML algorithm is a population-based stochastic algorithm mainly utilized for solving various optimization issues by suggesting suitable quasi-optimal solutions [37]. In the ML algorithm, random solutions are generated initially by the population members to resolve the optimization issues. With the guidance of mutated leaders, all the obtained solutions are updated in the search domain. Subsequent to repeated iterations, the ML algorithm provides global optimal solutions to the optimization issues. The mathematical formulation of the ML algorithm is described below,

By employing a population matrix, the population members are recognized, which is defined using the below expression:

$$Y = \begin{bmatrix} Y_1 \\ \vdots \\ Y_x \\ \vdots \\ Y_n \end{bmatrix}_{n\times \mathrm{M}} = \begin{bmatrix} y_{1,1} & \cdots & y_{1,b} & \cdots & y_{1,M} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ y_{x,1} & \cdots & y_{x,b} & \cdots & y_{x,M} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ y_{n,1} & \cdots & y_{n,b} & \cdots & y_{n,M} \end{bmatrix}_{n\times \mathrm{M}} \tag{3}$$

The term Y depicts the population matrix, Y_x signifies x^{th} member in the population, total members in the population is represented as n, number of problem variables is denoted by M and b^{th} variable value conveyed by x^{th} member in the population is implied as $y_{x,b}$. In accordance with the suggested variable values, the objection function is determined using the following equation.

$$F_O = \begin{bmatrix} F_1 \\ \vdots \\ F_x \\ \vdots \\ F_n \end{bmatrix}_{n\times 1} = \begin{bmatrix} F_O(Y_1) \\ \vdots \\ F_O(Y_x) \\ \vdots \\ F_O(Y_n) \end{bmatrix}_{n\times 1} \tag{4}$$

Here, the objective function vector is indicated by the symbol F_O and the fitness value of x^{th} member in the population is depicted as f_x. Getting guidance from the mutated leader, the best, worst and normal members of the population are updated on the basis of achieved fitness values. This process of ML algorithm is defined by the following expression.

$$\mathrm{M}_L : m_{x,b} = \begin{cases} Y_{Bst}\,,\ \Re \le \rho_B \\ Y_{Wst}\,,\ \rho_B < \Re \le \rho_B + \rho_W \\ Y_{g,b}\,,\ otherwise \end{cases} \tag{5}$$

The above equation illustrates the mutated leader guiding x^{th} member at the b^{th} dimension in the search space. Moreover, the terms Y_{Bst}, Y_{Wst}, and $\mathrm{Y}_{g,b}$ indicates best population member, worst population member, and randomly chosen g^{th} population member at b^{th} dimension, respectively. Also, $\Re$ implies uniformly distributed random numbers with range [0, 1], ρ_B and ρ_W depict the probability selection of best and worst population members. According to the guidance of the mutated leader, all the population members are updated, which is formulated as,

$$Y_x^{New} : y_{x,b}^{New} = \begin{cases} y_{x,b} + \xi \times \left(m_{x,b} - \Gamma \times y_{x,b}\right), F_O^{\mathrm{M}_L} < f \\ y_{x,b} + \xi \times \left(y_{x,b} - \Gamma \times m_{x,b}\right),\ otherwise \end{cases} \tag{6}$$

From the above equation, $Y_x^{New} : y_{x,b}^{New}$ represent new position of x^{th} population member at b^{th} dimension, ξ and Γ signifies the random numbers in which it lies within [0, 1] and (1, 2), respectively. Thus, the ML algorithm provides an optimal solution to the optimization issues.

2.3.3 Sine Cosine (SC) Algorithm

The sine cosine(SC) algorithm is a population-based metaheuristic algorithm inspired by the concept of the trigonometric sine function and cosine function [38–40]. The SC algorithm drives the random candidate solutions toward or against the best search agent based on these functions. This SC algorithm accelerates convergence speed and eliminates local optima problems. The numerical formulation of the SC algorithm is delineated as follows:

Initially, the random candidate solution is generated, and the fitness function of each candidate is determined. Then the position of the solution for both exploitation and exploration phases is updated using the following expression.

$$Z_d^{i+1} = \begin{cases} Z_d^i + R_1 \times \sin\left(R_2\right) \times \left|R_3 \mathrm{P}_d^i - Z_d^i\right|\,,\ R_4 < 0.5 \\ Z_d^i + R_1 \times \cos\left(R_2\right) \times \left|R_3 \mathrm{P}_d^i - Z_d^i\right|\,,\ R_4 \ge 0.5 \end{cases} \tag{7}$$

The position of the current solution in i^{th} iteration at d^{th} dimension is depicted as Z_d^i and the best solution in i^{th} iteration at d^{th} dimension is signified as P_d^i. Also, R_2, R_3, and R_4, are the equally distributed random numbers which lie $[0, 2\pi]$, [0, 2], and [0, 1], respectively. To balance exploitation and exploration phases, the ranges of sine and cosine functions varies with respect to the random number R_1. The random number R_1 is defined using the below equation,

$$R_1 = C - i\frac{C}{t} \tag{8}$$

The terms C, i, and t, represent constant, current iteration, and total iteration, respectively. Thus, the SC algorithm effectively balances both exploitation and exploration phases, thereby achieving the global best solution.

2.3.4 MLSC Algorithm

The conventional Mutated leader (ML) algorithm has some benefits: computation shortness, structure simplicity, and ease of transforming creature concepts to program code. As a consequence, in the ML algorithm, the implementation of a random search strategy and generation of mutated leaders produces new individual positions, thereby achieving the global best search agents. On the other hand, the efficacy of the ML algorithm is significantly influenced by the random policy parameters. This causes several limitations when dealing with composition and multi-modal functions. Therefore, the SC algorithm is adopted to enhance the ML algorithm's exploitation capability and exploration capability. This enhanced concept is named as the MLSC algorithm, which efficiently handles the searching process, enhances convergence speed, and avoids local optima issues. The pseudo code of the algorithm is shown in below.

Algorithm Pseudo Code for MLSC algorithm

Initialize search members' set, and input optimization problem information
  Set number of iterations N and T.
   Create initial population matrix
   Initialize members positions randomly
   Do
     Evaluate each of the search members by the objective function
     Update the best solution obtained so far
     Update random number values (R_1, R_2, R_3, and R_4)
     Update search members' position as per Eq. (7)
   Return best solution
   Evaluate objective function
    For iteration $1{:}T$
    Update Y_{Bst} and Y_{Wst}
      For i $= 1{:}N$
       Create mutated leader using Eq. (5)
       Calculate Y_i^{new} using Eq. (6)
       end
       Save the best solution
  Show the best solution

The combined flow diagram of the ML and SC algorithm is delineated in Fig. 3.

2.4 MLSC Based DCNN for Secure Blockchain in Industry 4.0

Fig. 4 presents the flow diagram of the proposed MLSC-based DCNN for secure blockchain in Industry 4.0. Initially, the collected blockchain dataset is further categorized into two categories as training data and testing data. For training, firstly, the neural network parameters are selected, and subsequently, the blockchain data is allowed to pass through a deep CNN network. Then the deep CNN model is trained, and the fitness function is evaluated. If it satisfies the termination criterion, the optimal parameter is specified as output; else, the data is further optimized. The weight function of the deep CNN model restricts the performance to obtain an optimal solution. Therefore, the Mutated leader-based Sine Cosine (MLSC) algorithm is developed to optimize the weight function. The MLSC algorithm selects the high fitness individual as the optimal solution. Thus, the proposed MLSC-based DCNN method effectively forecasts the cyber security system.

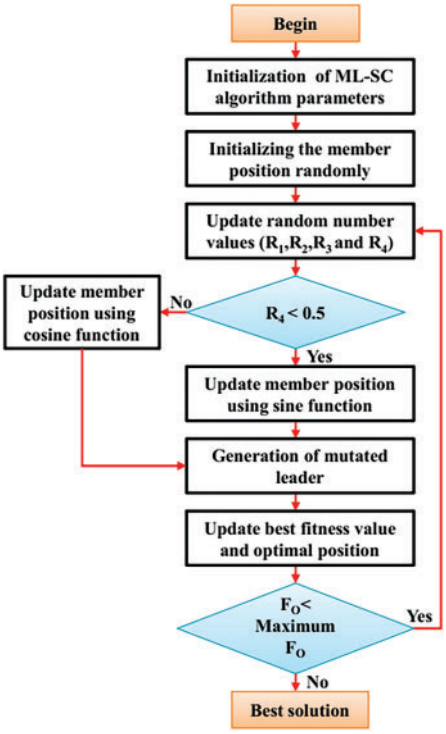

Figure 3: Combined flow diagram of MLSC algorithm

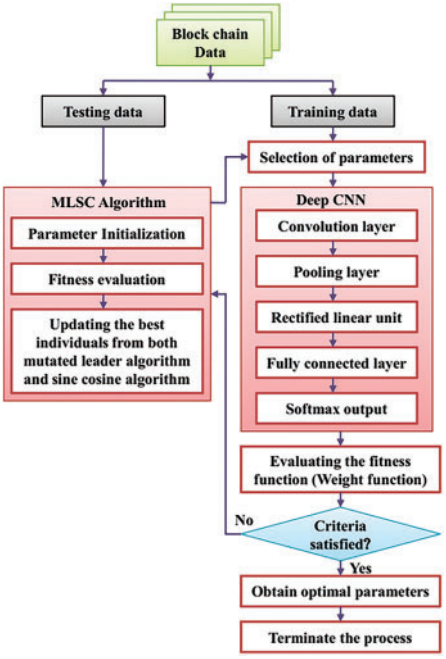

Figure 4: Proposed MLSC based DCNN for secure blockchain–IoT

3 Results and Discussion

The TON_IoT dataset [41] is obtained to determine the effectiveness of the proposed method. Various cybersecurity-based artificial intelligence applications like fraud detection, threat intelligence, digital forensics, malware detection, and privacy preservation are examined and verified by using this dataset. The TON_IoT datasets are new generations of Industry 4.0/Internet of Things (IoT) and Industrial IoT (IIoT) datasets for testing the fidelity and efficiency of various cybersecurity applications that use Artificial Intelligence (AI), i.e., Machine/Deep Learning techniques. It contains data from a variety of sources, including IoT and IIoT sensor telemetry datasets, Windows 7 and 10 operating system datasets, and Ubuntu 14 and 18 TLS and network traffic datasets. For the industry 4.0 network, which incorporates IoT and IIoT networks, a new testbed network was established to collect data. To manage the interconnection between the three levels of IoT, Cloud, and Edge/Fog systems, the testbed was installed utilizing numerous virtual machines and hosts running Windows, Linux, and Kali. In this research work, the parameters like accuracy, probability of malicious identification, latency, space-saving comparison, and transaction list are shown below.

Performance Evaluation

The proposed method is compared with Best Tip Selection Method (BTSM) and Smart Block-Software Defined Networking (SDN). BTSM considers the following: (a) each vital transaction indicated by the IoT application's priority level; (b) time since the request was made to join tangle; (c) the transaction's own weight. Smart Block-SDN is a distributed flow-rule verification technique and an innovative and efficient cluster-head selection mechanism that ensures network consistency and security. The cluster-head selection method, in particular, implements an effective procedure for picking cluster heads with optimum energy usage, which is necessary in a resource-constrained setting.

Fig. 5 shows the comparative analysis of the accuracy of various methods. The graph is plotted between a different number of IoT devices and the accuracy rate. It compares the accuracy of the projected scheme to the basic scheme in terms of identifying the probability of assaults in terms of authenticating the user as legitimate or malevolent. The proposed method obtains lower authentication accuracy than existing methods, while the existing methods attain higher accuracy. It is expressed in ms, since it is time to authenticate the user as legitimate or malicious. With faster authentication process, there will be no lag in the operations, and hence it is very important factor.

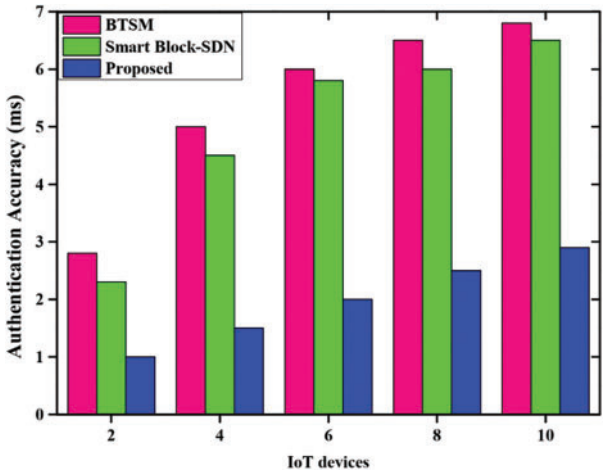

Figure 5: Comparative analysis of accuracy

Fig. 6 depicts the comparative graphical analysis of the probability of malicious identification of the proposed method. The X-axis specifies the CPA (computational power of attacker), and the Y-axis specifies the probability of malicious identification. The proposed method attains a lower probability of malicious identification than existing methods such as BTSM and Smart Block-SDN. When the CPA is maximum, the probability of malicious identification will be negligible.

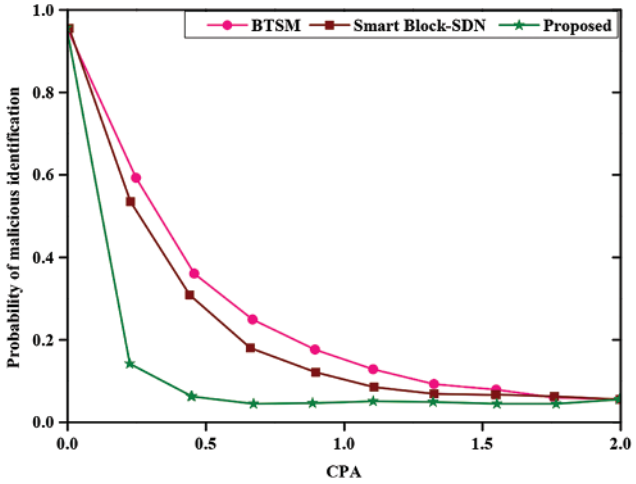

Figure 6: Comparative analysis of the probability of malicious identification

Fig. 7 portrays the graphical representation of the probability of malicious identification with CPA (computational power of attacker). The probability of malicious identification was determined with respect to CPA (computational power of attacker) with honest transaction arrival rate (HTAR), HTAR = 1, HTAR = 2, HTAR = 3, HTAR = 4, respectively. The probability is higher for HTAR = 4. From the graph, it is clear that if HTAR is high, then the probability will be high for the respective CPA. This analysis demonstrates that given the same computation power, we have a high probability of detecting fraudulent behavior when the honest transaction arrival rate is high.

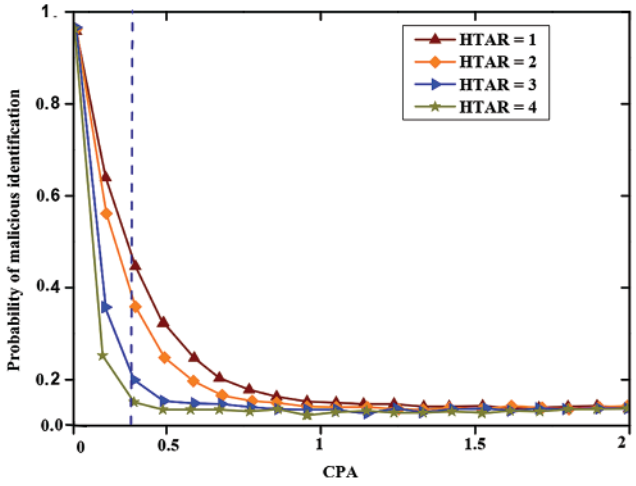

Figure 7: Graphical representation of the probability of malicious identification with CPA

The latency analysis of three different groups is shown in Fig. 8. Groups of 200, 400, and 800 users were chosen for this evaluation. The amount of time a block (tip) must wait for a transaction to be executed is known as latency. In power-constrained IoT devices, computational power, memory, and battery capacity are critical. Low latency and secure communication are therefore critical. When the number of users varies, the latency of the system changes though it won't disturb the system performance. The evaluation is split up into average, minimum, and maximum values for three groups of users. Among them, the group of 800 users has a large gap than the other two, which shows that an increase in users tends to a higher latency rate. Hence, it is important to optimize the latency rate with number of users.

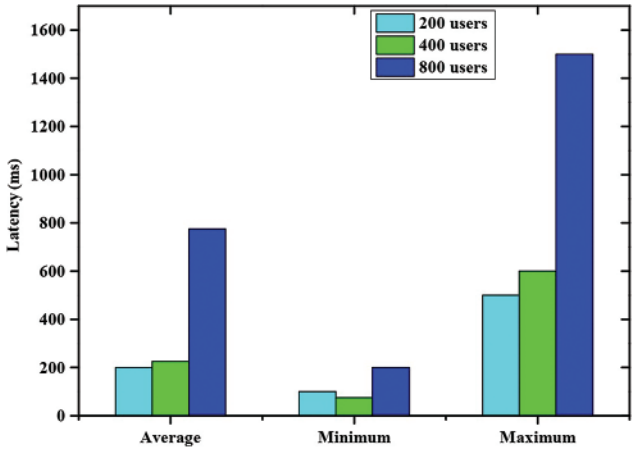

Figure 8: Latency analysis

Fig. 9 represents the space-saving comparison of the proposed method. The graph is plotted between a different number of blocks and the amount of data in megabytes (MB). The proposed method is compared with BTSM and Smart Block-SDN, respectively. The amount of data increases from each number of blocks. However, the proposed method has a minimum amount of data compared to the existing methods thereby; the proposed method reduces the space cost-efficiently. Saving in digital space is proportional to cost savings.

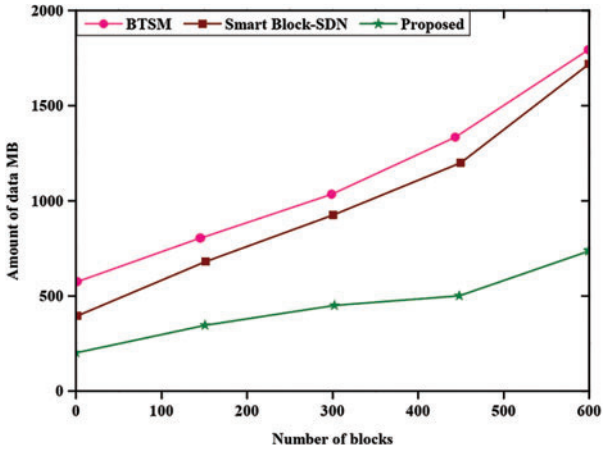

Figure 9: Space-saving comparison

Fig. 10 shows the transaction list evaluation of the proposed method. The list of transactions gradually increases with respect to the increase in the number of transactions. The proposed method obtains a minimal transaction list compared to the existing methods like BTSM and SmartBlock-SDN. Keeping the minimum transaction list will reduce the space storage as well as reduce the complexity in data processing.

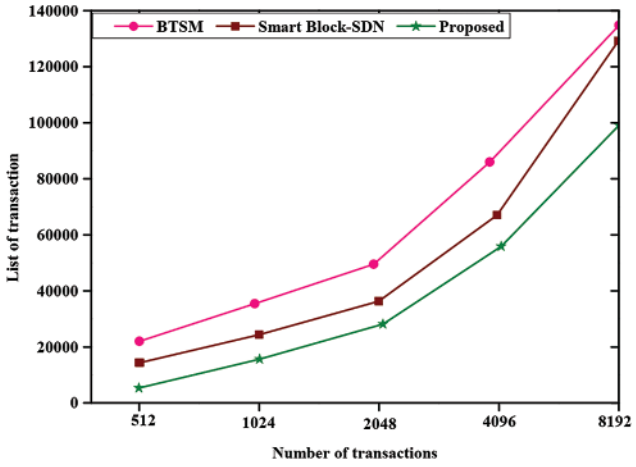

Figure 10: Evaluation of transaction list

4 Conclusions

This paper proposed a novel mutated leader sine cosine algorithm-based deep convolutional neural network (MLSC-DCNN) in order to attain a secure blockchain IoT of Industry 4.0. Here, the TON_IoT dataset is obtained to determine the effectiveness of the proposed method. The accuracy, probability of malicious identification, latency, space-saving comparison, and transaction list are compared and evaluated to determine the effectiveness of the proposed model. With a minimum amount of data, the proposed method reduces the space cost-efficiently. The authentication accuracy time of the proposed method is low compared to the existing methods. Hence, the proposed method can achieve the goal of providing a safe and secure network for Industry 4.0, in an efficient manner. This will improve the trust of people in Industry 4.0 without worrying much about cybersecurity issue. Furthermore, the time employed in validating the individual block prior to blockchain process will be computed in future work. Moreover, the proposed method's authentication accuracy will be increased further by optimizing the algorithm parameters.

Acknowledgement: The authors extend their appreciation to King Saud University for funding this work through Researchers Supporting Project Number (RSP2022R499), King Saud University, Riyadh, Saudi Arabia.

Funding Statement: The authors extend their appreciation to King Saud University for funding this work through Researchers Supporting Project Number (RSP2022R499), King Saud University, Riyadh, Saudi Arabia.

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

References

[1] S. Ali, G. Wang, M. Z. A. Bhuiyan and H. Jiang, "Secure data provenance in cloud-centric internet of things via blockchain smart contracts," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Guangzhou, China, pp. 991–998, 2018.

[2] X. Liang, J. Zhao, S. Shetty and D. Li, "Towards data assurance and resilience in IoT using blockchain." in *MILCOM 2017 - 2017 IEEE Military Communications Conf. (MILCOM)*, Baltimore, MD, USA, pp. 261–266, 2017.

[3] U. Guin, P. Cui and A. Skjellum, "Ensuring proof-of-authenticity of IoT edge devices using blockchain technology." in *2018 IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, pp. 1042–1049, 2018.

[4] M. H. Abidi, H. Alkhalefah, U. Umer and M. K. Mohammed, "Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process," *International Journal of Intelligent Systems*, vol. 36, no. 1, pp. 260–290, 2021.

[5] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, no. 1, pp. 32979–33001, 2018.

[6] T. Alladi, V. Chamola, R. M. Parizi and K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, no. 1, pp. 176935–176951, 2019.

[7] M. H. Abidi, H. Alkhalefah, M. K. Mohammed, U. Umer and J. E. A. Qudeiri, "Optimal scheduling of flexible manufacturing system using improved lion-based bybrid machine learning approach," *IEEE Access*, vol. 8, no. 1, pp. 96088–96114, 2020.

[8] M. H. Abidi, H. Alkhalefah and U. Umer, "Fuzzy harmony search based optimal control strategy for wireless cyber physical system with industry 4.0," *Journal of Intelligent Manufacturing*, 2021. https://doi.org/10.1007/s10845-021-01757-4.

[9] M. H. Abidi, M. K. Mohammed and H. Alkhalefah, "Predictive maintenance planning for industry 4.0 using machine learning for sustainable manufacturing," *Sustainability*, vol. 14, no. 6, pp. 3387, 2022.

[10] Y. Zuo, "Making smart manufacturing smarter–A survey on blockchain technology in industry 4.0," *Enterprise Information Systems*, vol. 15, no. 10, pp. 1323–1353, 2021.

[11] M. H. Abidi, A. Al-Ahmari, A. Ahmad, W. Ameen and H. Alkhalefah, "Assessment of virtual reality-based manufacturing assembly training system," *The International Journal of Advanced Manufacturing Technology*, vol. 105, no. 9, pp. 3743–3759, 2019.

[12] M. H. Abidi, U. Umer, M. K. Mohammed, M. K. Aboudaif and H. Alkhalefah, "Automated maintenance data classification using recurrent neural network: Enhancement by spotted hyena-based whale optimization," *Mathematics*, vol. 8, no. 11, pp. 2008–2040, 2020.

[13] R. Ch, T. R. Gadekallu, M. H. Abidi and A. Al-Ahmari, "Computational system to classify cyber crime offenses using machine learning," *Sustainability*, vol. 12, no. 10, pp. 4087, 2020.

[14] P. W. Khan, Y. -C. Byun and N. Park, "IoT-Blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning," *Sensors*, vol. 20, no. 10, pp. 2990, 2020.

[15] S. Bhattacharya, P. -K. -R. Maddikunta, I. Meenakshisundaram, T. -R. Gadekallu, S. Sharma *et al.,* "Deep neural networks based approach for battery life prediction," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 2599–2615, 2021.

[16] M. Alamgeer, S. -S. Alotaibi, S. Al-Otaibi, N. Alturki, A. -M. Hilal *et al.,* "Privacy preserving image encryption with deep learning based IoT healthcare applications," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 1159–1175, 2022.

[17] A. O. Almagrabi, "An efficient security solution for industrial internet of things applications," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 3961–3983, 2022.

[18] H. Tang, C. Hu, T. Liu and J. Ouyang, "A blockchain-based framework for secure storage and sharing of resumes," *Computers, Materials & Continua*, vol. 72, no. 3, pp. 5395–5413, 2022.

[19] A. Vangala, A. K. Das, Y. Park and S. S. Jamal, "Blockchain-based robust data security scheme in IoT-enabled smart home," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 3549–3570, 2022.
[20] M. Zia, "B-DRIVE: A blockchain based distributed IoT network for smart urban transportation," *Blockchain: Research and Applications*, vol. 2, no. 4, pp. 100033, 2021.
[21] R. L. Kumar, F. Khan, S. Kadry and S. Rho, "A survey on blockchain for industrial internet of things," *Alexandria Engineering Journal*, vol. 61, no. 8, pp. 6001–6022, 2022.
[22] F. Jamil, M. Ibrahim, I. Ullah, S. Kim, H. K. Kahng *et al.,* "Optimal smart contract for autonomous greenhouse environment based on IoT blockchain network in agriculture," *Computers and Electronics in Agriculture*, vol. 192, no. 1, pp. 106573, 2022.
[23] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza *et al.,* "Smartblock-SDN: An optimized blockchain-SDN framework for resource management in IoT," *IEEE Access*, vol. 9, no. 1, pp. 28361–28376, 2021.
[24] S. B. Rane and Y. A. M. Narvel, "Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future industry 4.0," *Benchmarking: An International Journal*, vol. 28, no. 5, pp. 1883–1908, 2021.
[25] C. Li, J. Zhang, X. Yang and L. Youlong, "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices," *Information Processing & Management*, vol. 58, no. 4, pp. 102602, 2021.
[26] J. Leng, S. Ye, M. Zhou, J. L. Zhao, Q. Liu *et al.,* "Blockchain-secured smart manufacturing in industry 4.0: A survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 237–252, 2021.
[27] G. Rathee, M. Balasaraswathi, K. P. Chandran, S. D. Gupta and C. S. Boopathi, "A secure IoT sensors communication in industry 4.0 using blockchain technology," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 533–545, 2021.
[28] M. S. Faridi, S. Ali, G. Duan and G. Wang, "Blockchain and IoT based textile manufacturing traceability system in industry 4.0." in *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 13th Int. Conf., SpaCCS 2020, Nanjing, China, December 18–20, 2020, Proc.*, Nanjing, China, Springer-Verlag, pp. 331–344, 2020.
[29] M. Sigwart, M. Borkowski, M. Peise, S. Schulte and S. Tai, "Blockchain-based data provenance for the internet of things." in *Proc. of the 9th Int. Conf. on the Internet of Things*, Bilbao, Spain, Association for Computing Machinery, pp. 1–8, 2019.
[30] M. N. Aman, K. C. Chua and B. Sikdar, "Secure data provenance for the internet of things." in *Proc. of the 3rd ACM Int. Workshop on IoT Privacy, Trust, and Security*, Abu Dhabi, United Arab Emirates, Association for Computing Machinery, pp. 11–14, 2017.
[31] M. N. Halgamuge, "Optimization framework for best approver selection method (BASM) and best tip selection method (BTSM) for IOTA tangle network: Blockchain-enabled next generation industrial IoT," *Computer Networks*, vol. 199, no. 1, pp. 108418, 2021.
[32] R. I. Bendjillali, M. Beladgham, K. Merit and A. Taleb-Ahmed, "Improved facial expression recognition based on DWT feature for deep CNN," *Electronics*, vol. 8, no. 3, pp. 324–339, 2019.
[33] N. Baghel, U. Verma and K. K. Nagwanshi, "WBCs-Net: Type identification of white blood cells using convolutional neural network," *Multimedia Tools and Applications*, 2021. https://doi.org/10.1007/s11042-021-11449-z.
[34] M. Heenaye-Mamode Khan, N. Boodoo-Jahangeer, W. Dullull, S. Nathire, X. Gao *et al.,* "Multi-class classification of breast cancer abnormalities using deep convolutional neural network (CNN)," *PLoS One*, vol. 16, no. 8, pp. e0256500, 2021.
[35] J. Gupta, S. Pathak and G. Kumar, "Bare skin image classification using convolution neural network," *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 1, pp. 138–145, 2022.
[36] S. Basheer, K. K. Nagwanshi, S. Bhatia, S. Dubey and G. R. Sinha, "FESD: An approach for biometric human footprint matching using fuzzy ensemble learning," *IEEE Access*, vol. 9, no. 1, pp. 26641–26663, 2021.

[37] F. -A. Zeidabadi, S. -A. Doumari, M. Dehghani, Z. Montazeri, P. Trojovský *et al.,* "MLA: A new mutated leader algorithm for solving optimization problems," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 5631–5649, 2022.

[38] Y. Fan, P. Wang, A. A. Heidari, M. Wang, X. Zhao *et al.,* "Rationalized fruit fly optimization with sine cosine algorithm: A comprehensive analysis," *Expert Systems with Applications*, vol. 157, no. 1, pp. 113486, 2020.

[39] A. B. Gabis, Y. Meraihi, S. Mirjalili and A. Ramdane-Cherif, "A comprehensive survey of sine cosine algorithm: Variants and applications," *Artificial Intelligence Review*, vol. 54, no. 7, pp. 5469–5540, 2021.

[40] S. Mirjalili, "SCA: A sine cosine algorithm for solving optimization problems," *Knowledge-Based Systems*, vol. 96, pp. 120–133, 2016.

[41] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, no. 1, pp. 165130–165150, 2020.