

Research Article

Deep Learning-Based Privacy-Preserving Data Transmission Scheme for Clustered IIoT Environment

Kuruva Lakshmanna ¹, **R. Kavitha**,² **B. T. Geetha**,³ **Ashok Kumar Nanda**,⁴
Arun Radhakrishnan ⁵ and **Rachna Kohar**⁶

¹Department of Information Technology, Vellore Institute of Technology, Vellore, India

²Department of CSE, Vel Tech Rangarajan Dr. Sagunihala R & D Institute of Science and Technology, Chennai, India

³Department of ECE, Saveetha School of Engineering, SIMATS, Saveetha University, Chennai, India

⁴CSE Department, B. V. Raju Institute of Technology, Narsapur, Medak, Telangana, India

⁵Faculty of Electrical and Computer Engineering, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia

⁶School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India

Correspondence should be addressed to Arun Radhakrishnan; arun.radhakrishnan@ju.edu.et

Received 7 April 2022; Revised 9 May 2022; Accepted 21 May 2022; Published 8 June 2022

Academic Editor: Kapil Sharma

Copyright © 2022 Kuruva Lakshmanna et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Industrial Internet of Things (IIoT) has received significant attention from several leading industries like agriculture, mining, transport, energy, and healthcare. IIoT acts as a vital part of Industry 4.0 that mainly employs machine learning (ML) to investigate the interconnection and massive quantity of the IIoT data. As the data are generally saved at the cloud server, security and privacy of the collected data from numerous distributed and heterogeneous devices remain a challenging issue. This article develops a novel multi-agent system (MAS) with deep learning-based privacy preserving data transmission (BDL-PPDT) scheme for clustered IIoT environment. The goal of the BDL-PPDT technique is to accomplish secure data transmission in clustered IIoT environment. The BDL-PPDT technique involves a two-stage process. Initially, an enhanced moth swarm algorithm-based clustering (EMSA-C) technique is derived to choose a proper set of clusters in the IIoT system and construct clusters. Besides, multi-agent system is used to enable secure inter-cluster communication. Moreover, multi-head attention with bidirectional long short-term memory (MHA-BLSTM) model is applied for intrusion detection process. Furthermore, the hyperparameter tuning process of the MHA-BLSTM model can be carried out by the stochastic gradient descent with momentum (SGDM) model to improve the detection rate. For examining the promising performance of the BDL-PPDT technique, an extensive comparison study takes place and the results are assessed under varying measures. A significant amount of capital is required. It goes without saying that one of the most obvious industrial IoT concerns is the high cost of adoption. Secure data storage and management connectivity failures are common among IoT devices due to the massive amount of data they create. The simulation results demonstrate the enhanced outcomes of the BDL-PPDT technique over the recent methods. Despite the fact that the offered BDL-PPDT technique has an accuracy of just 98.15 percent, it produces the best feasible outcome. Because of the data analysis conducted as detailed above, it was determined that the BDL-PPDT technique outperformed the other current techniques on a range of different criteria and was thus recommended.

1. Introduction

Industrial Internet of Things (IIoT) employs actuators and sensors with communication and computation capabilities to transform the way the information is exchanged, analyzed, transformed, and collected into decisions [1]. This

pervasive capability results in advanced Industry 4.0 (called Industrial Internet) application for enhanced efficiency and productivity in large industries like healthcare, energy, agriculture, mining, and transportation. The innovative Industry 4.0 features, namely, ML-based quality control and predictive maintenance and run-time reasoning, need to be

simplified by distributed data acquisition [2]. In IIoT-based systems like open banking and smart healthcare, ML and data methods trained with the local boundary should be interacted with the branches or users to make organization-wider knowledge [3]. Often, vendors desired to limit their internal insight on product improvements and development with the organizational boundary for increasing business values against their contender. Furthermore, industries like open banking and smart healthcare are vastly convoluted with human-specific sensitive information [4]. ML model is trained on sensitive information that could expose confidential or private data to the attackers [5]. Therefore, trustworthiness and privacy are the key elements of ML in IIoT system. The Internet of Things is one of the primary drivers of the Industry 4.0 movement, since it enables greater automation, data collection, and analytics, as well as workflow and process optimization. The intelligence enabled by the Internet of Things enables devices to work cooperatively to produce outputs on an assembly line. MAS as a popular technique to offer trusts with distributed and decentralized settings might be employed in lots of potential applications, namely, supply chain management, IIoT, and healthcare [6]. The Internet of Things is a major driver of the Industry 4.0 movement since it enables increased automation, data collection, and analytics, as well as workflow and process optimization. The Internet of Things' intelligence enables devices to operate together on an assembly line to produce outputs. A multi-agent system (MAS or "self-organized system") is a computerized system that is built of numerous intelligent agents that communicate with one another. Multi-agent systems are capable of resolving problems that a solo agent or a monolithic system would find difficult or impossible to solve. Methodical, functional, or procedural techniques, algorithmic search, or reinforcement learning can all be considered forms of intelligence. Among them, it is the mainstream application field, where blockchain is regarded as enabling technology for various applications. IIoT setup is a well-developed and also comprehensive deployment that can increase multiple challenges involving ensuring confidentiality, improving data accountability, availability, integrity, and availability (CIA). Blockchain can address this requirement and acts as a significant role by providing secure and verifiable solutions to store and share data [7]. IIoT application has requirements of similar kinds to guarantee trust and data integrity between several shareholders related to dissimilar parts of the logistic chain (e.g., storage, acquiring raw material, processing to customer, transportation, and industrial deployment). Also, in this application, requirements such as monitoring and maintaining history of each procedure are vital. The conventional security method has a number of constraints and does not fit for intelligent grid systems; for example, secured end-to-end encryption method could produce higher false alarm rate and interrupt analytical approach [8]. There is a considerable range of potential smart grid risks, like passive and active attacks. Another way of the attack is the smart grids, namely, sniffing the information from the CPS through open source data, and in active attack, the hackers can change the information

through data poisoning attack or inference attack [9]. In data poisoning attacks, attackers attempt to change the standard information.

This article develops a novel MAS with deep learning-based privacy-preserving data transmission (BDL-PPDT) scheme for clustered IIoT environment. This research proposes a unique multi-agent system (MAS) method for clustered IIoT environments using deep learning-based privacy preserving data transmission (BDL-PPDT). The BDL-PPDT technique's objective is to achieve secure data transfer in a clustered IIoT environment. The BDL-PPDT technique involves the design of an enhanced moth swarm algorithm-based clustering (EMSA-C) technique for cluster head (CH) selection. In addition, blockchain technology (BCT) is applied for accomplishing secure inter-cluster communication. Furthermore, a new multi-head attention with bidirectional long short-term memory (MHA-BLSTM) model is used to find intrusions. To increase the detection rate, the stochastic gradient descent with momentum (SGDM) model can be used to tune the MHA-BLSTM model's hyperparameters. Finally, the stochastic gradient descent with momentum (SGDM)-based hyperparameter tuning process takes place. To inspect the significant performance of the BDL-PPDT technique, a wide-ranging comparative analysis is made and the results are inspected in terms of different measures.

2. Related Works

Sodhro et al. [10] proposed sustainable, secure, efficient, and reliable blockchain-driven methods. The presented method handles key arbitrarily by presenting the chain of blocks with a smaller amount of cores, less power drain, computation bit, and transmission. Next is an analytic hierarchy process (AHP) based smart decision-making method for the blockchain-driven that is more secured, reliable, sustainable, interoperable, and concurrent IIoT. Rahman et al. [11] presented a blockchain-based architecture to provision a verifiable query and privacy-preserving facilities to end-user in IIoT system. The architecture employs blockchain to save broad information as off-chain data and to save IoT information as on-chain data and provision search service to the user by performing a query in off-chain and on-chain data as well as generate an effective result.

Zhang et al. [12] developed a medical data privacy protection architecture-based blockchain (MPBC). In this method, they secure confidentiality by including different privacy noises to federated learning. Additionally, the increasing amount of healthcare data can make blockchain storage challenges. Thus, a storage mode is presented for reducing the storage burden of blockchain. The new information is locally stored and the hash values are estimated by IPFS and are saved in blockchain. Deebak and Al-Turjman [13] introduced a privacy-preserving smart contract with blockchain and artificial intelligence (PPSC-BCAI) architecture which facilitates system activities, human interaction, security risks, fraudulent claims, and service alerts. In order to examine the data sharing and transaction, an XGBoost is employed.

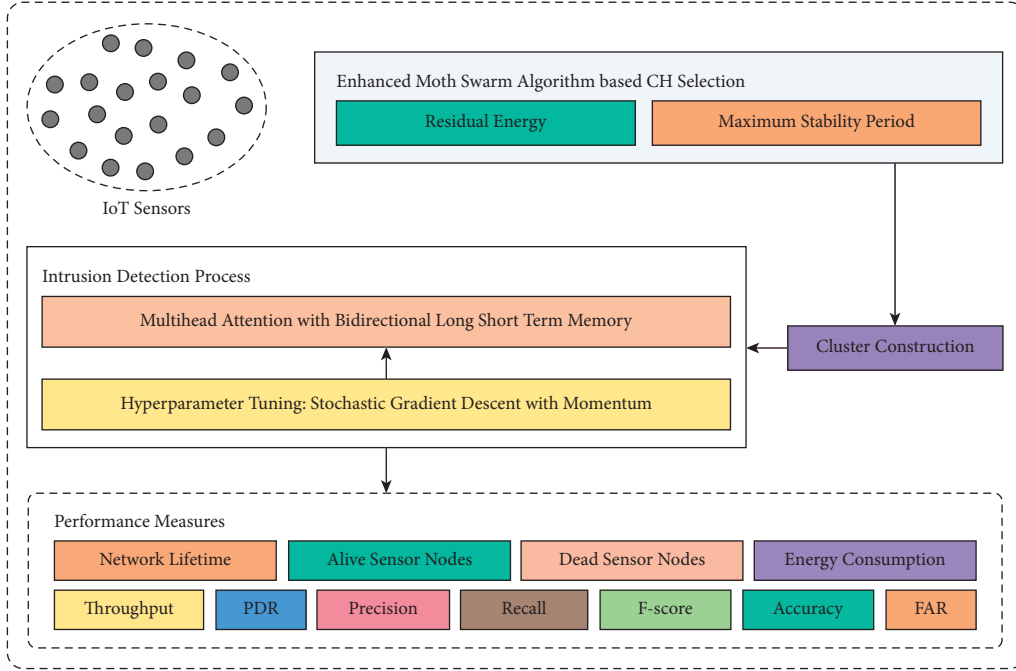


FIGURE 1: Working process of BDL-PPDT approach.

Weng et al. [14] proposed a secure, fair, and distributed DL architecture called DeepChain to resolve this problem. DeepChain provides a value-driven incentive method based on blockchain for forcing the participant to perform properly. In the meantime, DeepChain ensures data privacy for all the participants and provides auditability for the entire training procedure. Arachchige et al. [15] presented an architecture called PriModChain which forces trustworthiness and privacy on IIoT information by amalgamating federated ML, differential privacy, smart contracts, and Ethereum blockchain. The possibility of PriModChain based on resilience, privacy, security, reliability, and safety is estimated by the simulation technologically advanced in Python with socket programming on a multipurpose computer.

Kumar and Tripathi [16] designed a deep blockchain-based trustworthy privacy-preserving secured framework (DBTP2SF) for IIoT. This architecture contains two-phase privacy-preservation model, anomaly detection module, and trust management module. In the two-phase privacy model, a BC-enabled improved proof of work method is concurrently employed with AE, to convert cyber physical information to a novel form which avoids poisoning and inference attacks.

3. The Proposed Model

In this study, an effective BDL-PPDT technique has been developed to accomplish secure data transmission in clustered IIoT environment. The BDL-PPDT technique has presented a new EMSA-C technique to choose a proper set of clusters in the IIoT system and construct clusters. Next, the MHA-BLSTM with SGDM model is utilized for intrusion detection and the hyperparameter tuning process is made by the SGDM model resulting in improved detection performance. Figure 1 illustrates the overall process of BDL-PPDT manner.

3.1. Process Involved in EMSA-C Technique. The nocturnal behaviors of moth are the motivation for the MSA [17]. In the model, the exploration and exploitation tradeoff considers a divider of candidate solutions generating the population:

- (i) Onlooker (to exploit the optimal region discovered by the prospector).
- (ii) Pathfinder (to explore novel region of the searching space).
- (iii) Prospector (to exploit the novel regions attained by the pathfinder).

With other meta-heuristics models, this one begins with population initialization:

$$x_{ij} = r \text{ and } (u_j - l_j) + l_j, \forall i \in \{1, 2, n\}, j \in \{1, 2, d\}, \quad (1)$$

whereas u and l represent maximum and minimum bounds of the searching space, x_i denotes the candidate solution, n indicates the population size, d signifies the dimensionality of problems, and $rand$ means an arbitrary number drawn from a uniform distribution. For generating pathfinder crossover, it is essential to estimate the variation coefficient and dispersal degree at iteration t :

$$\sigma_j^t = \frac{\sqrt{\left(\frac{1}{n_p}\right) \sum_{i=1}^{n_p} (x_{ij}^t - P_j^t)^2}}{P_j^t}, \quad (2)$$

$$\mu^t = \frac{1}{d} \sum_{j=1}^d \sigma_j^t, \quad (3)$$

whereas n_p represents the amount of pathfinders

$$P_j^t = \frac{1}{n_p} \sum_{i=1}^{n_p} x_{ij}^t. \quad (4)$$

In the MSA, the crossover point represents minimum dispersal value, as follows:

$$j \in c_p \text{ if } \sigma_j^t \leq \mu^t. \quad (5)$$

Form this, $n_c \in c_p$ crossover point is employed for creating a novel sub-trial pathfinder vector $\vec{v}_p = [v_{p1}, v_{p2}, \dots, v_{pn_c}]$ from the novel pathfinder $\vec{\chi}_p = [\chi_{p1}, \chi_{p2}, \dots, \chi_{pn_c}]$:

$$\vec{v}_p^t = \vec{\chi}_p^t + L_{p1}^t \cdot (\vec{\chi}_{r^2}^t - \vec{\chi}_{r^3}^t) + L_{p2}^t \cdot (\vec{\chi}_{r^4}^t - \vec{\chi}_{r^5}^t), \quad (6)$$

$$\forall r^1 \neq r^2 \neq r^3 \neq r^4 \neq r^5 \neq p \in \{1, 2, \dots, n_p\}. \quad (7)$$

For each of the independent variables [18], the variables L_{p1} and L_{p2} are calculated using the Lévy stable distribution. There should only be one set of indexes r selected from the pathfinder solution, in which L_{p1} and L_{p2} represent independent variable calculated from the Lévy α -stable distribution [18]. The set of indexes r should be only chosen from the pathfinder solution, and position is upgraded by the mutated variable extracted from the sub-trail vector as follows:

$$V_{pj}^t = \begin{cases} v_{pj}^r, & \text{if } j \in c_p, \\ x_{pj}^t, & \text{if } j \notin c_p. \end{cases} \quad (8)$$

Lastly, MSA employs a selection approach among the original and trial pathfinders as follows:

$$\vec{x}_p^{t+1} = \begin{cases} \vec{x}_p^t, & \text{if } f(\vec{V}_p^t) \geq f(\vec{x}_p^t), \\ \vec{V}_p^t, & \text{otherwise.} \end{cases} \quad (9)$$

The possibility of choosing the next pathfinder is determined by

$$p_p = \frac{\text{fit}_p}{\sum_{p=1}^{n_p} \text{fit}_p}. \quad (10)$$

That employs the luminescence intensity estimated as follows:

$$\text{fit}_p = \begin{cases} \frac{1}{1 + f_p}, & \text{if } f_p \geq 0, \\ 1 + |f_p|, & \text{otherwise.} \end{cases} \quad (11)$$

From the pathfinder, n_f individual is chosen as prospector; this value is modified dynamically as follows:

$$n_f = \text{round}\left(\left(n - n_p\right) \times \left(1 - \frac{t}{T}\right)\right), \quad (12)$$

where T represents the maximal iteration number. The MSA enables the moth to move in a spiral manner over a pathfinder using equation (12):

$$x_i^{t+1} = |x_i^t - x_p^t| \cdot e^\theta \cdot \cos 2\pi\theta + x_p^t \quad (13)$$

$$\forall p \in \{1, 2, \dots, n_p\}; i \in \{n_p + 1, n_p + 2, \dots, n_f\}$$

Let $\theta \in [r, 1]$ be an arbitrary value employed for giving the spiral formation to the prospector path, while $r = -1 - (t/T)$.

The onlooker is the moth with the minimum luminescent intensity moving toward the shiniest source of light; in MSA, the onlooker is employed for intensifying the exploitation process. Further, the onlooker is separated into Gaussian walk and associative learning using immediate memory. Initially, the onlooker in the real iteration is attained as follows:

$$x_i^{t+1} = x_i^t + \varepsilon_1 + [\varepsilon_2 \cdot \frac{g^t}{\text{best}} - \varepsilon_3 \cdot x_i^t], \quad \forall i \in \{1, 2, \dots, n_o\}, \quad (14)$$

whereas ε_2 and ε_3 represent uniformly distributed random value, best_g denotes the optimal candidate solution, $n_o = \text{round}(n_u/2)$ indicates the amount of onlookers performing a Gaussian movement, n_u shows the amount of onlookers, and ε_1 means an arbitrary value estimated by

$$\varepsilon_1 \sim \text{random}(\text{size}(d)) \oplus N(\text{best}^t)(x_i^t - \text{best}_g^t). \quad (15)$$

The behavior of the moth considered short-term memory and associative learning is upgraded as follows:

$$x_i^{t+1} = x_i^t + 0.001 \cdot G + \left(1 - \frac{g}{G}\right) \cdot \varepsilon_2 \cdot (\text{best}_p - x_i^t) + \left(\frac{2g}{G}\right) \cdot \varepsilon_3 \cdot (\text{best}_p^t - x_i^t), \quad \forall i \in \{1, 2, \dots, n_m\} \quad (16)$$

with $n_m = n_u - n_o$ being the amount of onlookers performing short-term memory and associative learning; $1 - (g/G)$ indicates a cognitive factor, $2g/G$ represent a social factor, best_p indicates the optimal light source from the pathfinder, and $G \sim N(x_i^t - \chi_i^{\min}, \chi_i^{\max} - \chi_i^t)$.

To improve the performance of the MSA, the EMSA is derived by the use of OBL concept. The efficient implementation of OBL contributes approximation of the opposite and current populations in the same generation for identifying optimum candidate solutions of a given problem. Object-based learning (OBL) is a student-centered learning approach that uses objects to facilitate deep learning. Objects may take many forms, small or large, but the method typically involves students handling or working at close quarters with and interrogating physical artefacts. The OBL models have been efficiently used in different meta-heuristics employed for improving convergence speed. The models of the opposite amount should be described in OBL.

Consider $N \in N[x, y]$ to denote real numbers. The opposite numbers N^o are given by

$$N^o = x + y - N. \quad (17)$$

In d-dimension searching region, the depiction may be extended as follows:

$$N_i^o = x_i + y_i - N_i, \quad (18)$$

whereas (N_1, N_2, \dots, N_d) indicates d-dimension searching region and $N_i[x_i, y_i]$, $i = 1, 2, \dots, d$. From the OBO, the approach of OBL is employed in this initiation procedure of MSA method and for all iterations in the application of jump rate.

Consider an IoT network of n sensor deployed arbitrarily. In order to be CH selective, the projected SSA executes squirrel population that was utilized by generating suitable clusters and maintaining the lower power employment of systems. Consider $X = (X_1, X_2, \dots, X_n)$ stands for the population vector of IoT with n sensors, where $X_i(j) \in \{0, 1\}$. The CH and normal nodes were signified as one and zero. The fundamental population of NP solution has inspired arbitrarily by representing 0 s as well as 1 s and representing as follows:

$$X_i(j) = \begin{cases} 1, & \text{if } (r \text{ and } \leq p_{opt}), \\ 0, & \text{otherwise,} \end{cases} \quad (19)$$

where p_{opt} stands for the recommended percentage of CHs and r and refers to uniform arbitrary values in zero and one. An arbitrarily located sensor node has been decided as K clusters: C_1, C_2, \dots, C_K . The CH selective has responsible to decrease the cost of FF. Therefore, FF to CH selective was showcased as follows:

$$f_{obj_CH} = \sum_{i=1}^2 w_i \times f, \quad (20)$$

with $\sum_{i=1}^2 w_i = 1$. The maximum stability period is given by decreasing the Standard Deviation (SD) of the RE of node which is a significant issue. Therefore, SD (σ_{RE}) is applicable to measure the control of uniformly distributed load in sensor node and illustrated as follows:

$$f_1 = \sigma_{RE} = \sqrt{\frac{1}{n} \sum_{j=1}^n \{\mu_{RE} - E(\text{node}_j)\}^2}, \quad (21)$$

where $\mu_{RE} = (1/n) \sum_{i=1}^n E(\text{node}_i)$, $E(\text{node}_i)$ stands for the RE of i^{th} node, and n depicts the node count. A final objective was dependent upon clustering quality in that function of cluster isolation and cohesion has been implemented. Once the proportion of cohesion for separating was minimal, afterward optimum clustering was executed. It is accomplished by utilizing FF ratio of overall Euclidean distance of CH to CM and restricted Euclidean distance of 2 varying CHs.

$$f_2 = Q_c = \frac{\sum_{k=1}^K \sum_{\forall \text{node}_j \in C_k} d(\text{node}_j, CH_k)}{\min_{\forall C_c, C_k, C_c \neq C_k} \{d(CH_c, CH_k)\}} \quad (22)$$

3.2. Secure Inter-Cluster Communication via Blockchain. Generally, blockchain is assumed as a collection of blocks; also, a single block comprises of hash value of the existing

block, information about the transaction (Ethereum, bitcoin), timestamp, and previous block. Furthermore, blockchain is determined as common and distributed digital ledger utilized to save the transaction data under different points. Therefore, when an attacker tries to derive information, it is not possible as every block has cryptographic value of the earlier block [19]. Now, each transaction is attained under the application of cryptographic hash values, viz. confirmed by all the miners. It consists of blocks of each transaction and captures same value of the comprehensive ledger. Figure 2 illustrates the framework of blockchain. The blockchain offers the facility to share detailed ledgers in protective, confidential, and shared manner. Decentralized storage is the other source in blockchain, and the massive number of information data is linked and stored from existing blocks to earlier blocks through smart contract code. LitecoinDB, Swarm, SiacoinDB, MoneroDB, BigchainDB, Interplanetary File System (IPFS), and various factors were employed for decentralized dataset.

3.3. Intrusion Detection Process. During the intrusion detection process, the MHA-BLSTM with SGDM model is utilized. LSTM is a variant of RNN that could resolve gradient disappearance problems by presenting memory cell state, input gate i , output gate o , and forget gate f . LSTM could enhance the memory model of NN for receiving training and input data that is appropriate to model time series data, such as text, owing to the design characteristics. BiLSTM is an integration of backward and forward LSTM. The greatest benefit of the model is that the sequence context data are taken fully into account. An LSTM unit contains controlling gate, along with IG i_t , a forget gate f_t , outcome gate o_t , and a memory cell state c_t , that affects the unit capacity to update and store data. The IG outcome value lies between 0-1 according to the input h_{t-1} and w_t . Once the outcome is 1, it implies that the cell state data are retained completely, and once the outcome is 0, it is abandoned completely. Then, the IG determines which value needs updating, and the tanh layer creates a novel candidate value vector \tilde{c}_t that is added to the cell state. Next, both are integrated for updating the cell state c_t ; lastly, the outcome layer decides the outcome value based on the cell state. Among other, $W_f, U_f, b_f, W_i, U_i, b_i, W_c, U_c, b_c$, and W_o, U_o, b_o represent the internal training parameter in the LSTM, $\sigma(\cdot)$ indicates sigmoid activation function, and \odot implies dot multiplication.

$$f_t = \sigma(W_f w_t + U_f h_{t-1} + b_f), \quad (23)$$

$$i_t = \sigma(W_i w_t + U_i h_{t-1} + b_i), \quad (24)$$

$$\tilde{c}_t = \tanh(W_c w_c + U_c h_{t-1} + b_c), \quad (25)$$

$$c_t = i_t \odot \tilde{c}_t + f_t \odot c_{t-1}, \quad (26)$$

$$o_t = \sigma(W_o w_t + U_o h_{t-1} + b_o), \quad (27)$$

$$h_t = o_t \tanh \odot (c_t). \quad (28)$$

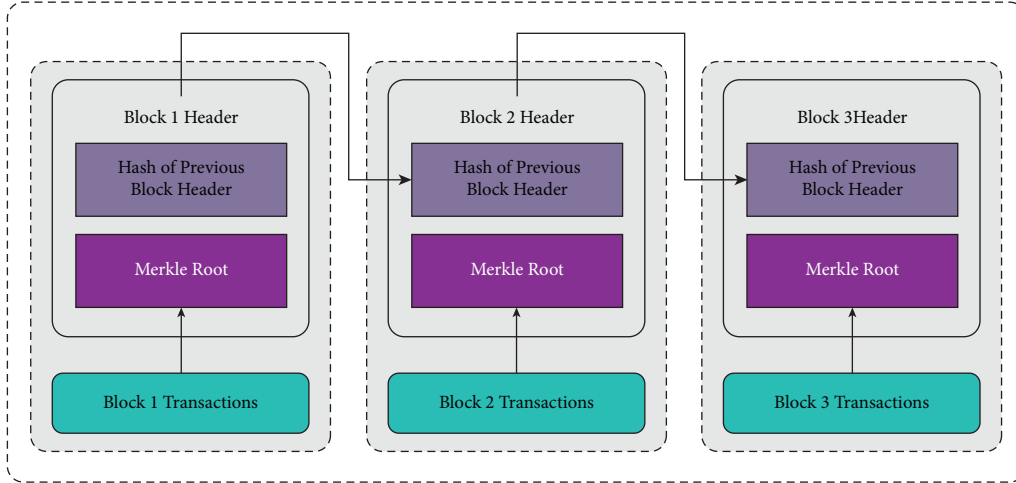


FIGURE 2: Structure of blockchain.

The abovementioned method is the computation method of LSTM. As previously mentioned, BiLSTM comprises backward and forward LSTM. \overrightarrow{LSTM} in BiLSTM reads the input from w_1 to e_n for generating \overrightarrow{h}_t , and other \overleftarrow{LSTM} reads the input from e_n to w_1 for generating \overleftarrow{h}_{t-1} :

$$\overrightarrow{h}_t = \overrightarrow{LSTM}(w_t, \overrightarrow{h}_{t-1}, c_{t-1}), t \in [1, m+n], \quad (29)$$

$$\overleftarrow{h}_t = \overleftarrow{LSTM}(w_t, \overleftarrow{h}_{t-1}, c_{t-1}), t \in [m+n, 1]. \quad (30)$$

The reverse and forward context representations generated using \overrightarrow{h}_t and \overleftarrow{h}_t are linked to the long vector,

$$h_t = \overrightarrow{h}_t \oplus \overleftarrow{h}_t. \quad (31)$$

Lastly, the output $[h_1, \dots, h_i, \dots, h_m, l_1, \dots, l_j, \dots, l_n]$ of the entire sentence is attained, whereas h_i and l_j are exploited to signify the output of emoticons and words, correspondingly. Furthermore, set each intermediate layer in BiLSTM for returning the comprehensive output sequence, thus ensuring that the output of all the hidden layers retains the longer-distance data as possible.

Attention mechanism is used to improve the effects of RNN-based model, and also it consists of dot-product attention and additive attention [20]. The calculation of attention is separated into 3 stages. Initially, utilize F attention function to score key and query to get s_i ; next, utilize softmax function to standardize the scoring results s_i , for obtaining the weight a_i . Lastly, estimate attention that is the weighted average of each value and weight a_i . Multi-head attention mechanism has enhanced the classical attention method; thus, all the heads could extract the features of key and query in distinct subsets. More precisely, this feature comes from Q and K that is the projection of key and query in the subspaces. Note that in the multi-head attention model, the attention functions can be the scaled dot-product function that is similar to the classical attention mechanism, excepting the regulating scaling factors [21–27]. In this work, h should be debugged continuously for determining the

appropriate values. Lastly, the result, i.e., returned in every head, is linearly converted and concatenated to attain multi-head attention. Eventually, transmit the vector from the preceding layer to the densely connected layer. They utilize ReLU function as the activation function for completing the nonlinear transformation. Finally, execute the softmax function on the output of the preceding layer and attain intrusion detection output.

For optimally adjusting the hyperparameter of the MHA-BLSTM model, the SGDM is applied. SGDM is a first-order momentum depending on SGD. The 1st-order momentum represents the exponential moving of the gradient direction at all the moments, nearly equivalent to sum of the gradient vector at the current T_j moment. And, the T_j is denoted by

$$T_j = \frac{1}{1 - \beta_i}. \quad (32)$$

In another word, the descendant direction at t time is described using the descending direction accumulated before as well as gradient direction of the existing point. The empirical value of β_1 is 0.9, which implies the direction of decline is particularly the before accumulated direction of decline.

4. Results and Discussion

In this section, a detailed experimental validation of the BDL-PPDT technique takes place under varying numbers of IoT sensor nodes and rounds. The results are examined in varying aspects. An extensive throughput analysis of the BDL-PPDT technique with other methods is given in Table 1 and Figure 3. The results reported that the BDL-PPDT technique has demonstrated enhanced throughput under every IoT sensor node. For instance, with 100 IoT sensor nodes, the BDL-PPDT technique has offered improved throughput of 99.71 Mbps whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have accomplished decreased NSAN of 69.98 Mbps, 84.17 Mbps, 88.89 Mbps, 88.68 Mbps, and 98.16 Mbps, respectively. Moreover, with 500 IoT sensor nodes, the BDL-PPDT technique has accomplished raised throughput of 89.72 Mbps, whereas the

TABLE 1: Result analysis of BDL-PPDT technique with existing approaches.

IoT sensor nodes	Packet delivery ratio (%)					
	DEEC	PHC	HNS	CHSES	RDAC-BC	BDL-PPDT
100	94.74	94.57	96.80	95.48	98.11	99.72
200	91.93	94.61	96.26	96.44	98.87	99.23
300	92.21	94.32	95.84	96.22	97.10	98.97
400	91.86	91.89	92.53	95.88	96.50	98.84
500	91.45	92.76	94.39	93.53	97.69	98.16

IoT sensor nodes	Throughput (Mbps)					
	DEEC	PHC	HNS	CHSES	RDAC-BC	BDL-PPDT
100	69.98	84.17	88.89	88.68	98.16	99.71
200	63.40	76.46	83.26	84.32	94.27	98.42
300	61.05	68.33	75.50	76.67	92.03	93.80
400	54.68	60.53	68.89	71.76	88.97	91.57
500	51.48	55.31	62.24	70.42	85.05	89.72

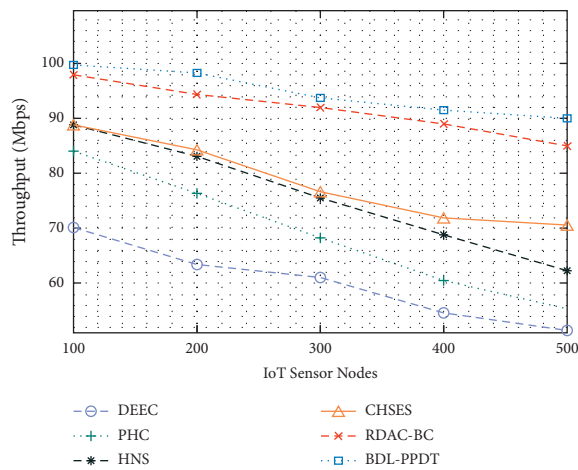


FIGURE 3: Throughput analysis of BDL-PPDT technique with existing approaches.

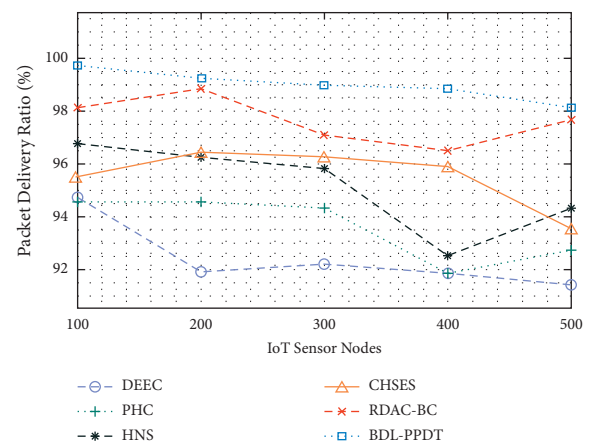


FIGURE 4: PDR analysis of BDL-PPDT technique with existing approaches.

DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have led to lessening NSAN of 51.48 Mbps, 55.31 Mbps, 62.24 Mbps, 70.42 Mbps, and 85.05 Mbps, respectively.

Figure 4 offers the detailed PDR analysis of the BDL-PPDT technique under several IoT sensor nodes. From the results, it can be observed that the BDL-PPDT technique has reported enhanced PDR under every IoT sensor node. For instance, with 100 IoT sensor nodes, the BDL-PPDT technique has gained an increased PDR of 99.72%, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have reached to decrease PDR of 94.74%, 94.57%, 96.80%, 95.48%, and 98.11%, respectively. Besides 500 IoT sensor nodes, the BDL-PPDT technique has exhibited a maximum PDR of 98.16%, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have depicted minimum PDR of 91.45%, 92.76%, 94.39%, 93.53%, and 97.69%, respectively.

A brief comparative NLT analysis of the BDL-PPDT technique is illustrated in Table 2 and Figure 5. From the results, it is evident that the BDL-PPDT technique has provided supreme NLT under every IoT sensor node. For instance, with 100 IoT sensor nodes, the BDL-PPDT technique has given superior NLT of 1793 rounds, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have

offered inferior NLT of 1386, 1492, 1529, 1588, and 1612 rounds, respectively. Eventually, with 500 IoT sensor nodes, the BDL-PPDT technique has exhibited higher NLT of 3633 rounds, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have attained lower NLT of 3103, 3326, 3289, 3463, and 3547 rounds, respectively.

The ECM analysis of the BDL-PPDT technique with other methods under distinct IoT sensor nodes is represented in Figure 6. The results inferred that the BDL-PPDT technique has managed to offer minimal ECM under all IoT sensor nodes. For instance, with 100 IoT sensor nodes, the BDL-PPDT technique has achieved minimal ECM of 0.0470 mJ, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have obtained maximum ECM of 0.2058 mJ, 0.1690 mJ, 0.1425 mJ, 0.1165 mJ, and 0.0756 mJ, respectively. Furthermore, with 500 IoT sensor nodes, the BDL-PPDT technique has offered a least ECM of 0.3654 mJ, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have reached to an increased ECM of 0.8872 mJ, 0.8277 mJ, 0.7007 mJ, 0.7351 mJ, and 0.4084 mJ, respectively.

A brief comparative number of alive sensor node (NASN) analysis of the BDL-PPDT technique takes place in Table 3 and Figure 7. From the results, it can be noticed that

TABLE 2: Comparative analysis of BDL-PPDT technique with varying IoT sensor nodes.

IoT sensor nodes	Energy consumption (mJ)					
	DEEC	PHC	HNS	CHSES	RDAC-BC	BDL-PPDT
100	0.2058	0.1690	0.1425	0.1165	0.0756	0.0470
200	0.4164	0.3315	0.2576	0.2761	0.1496	0.1176
300	0.5478	0.5684	0.4784	0.4635	0.2343	0.2017
400	0.7226	0.6687	0.6027	0.6048	0.3570	0.2872
500	0.8872	0.8277	0.7007	0.7351	0.4084	0.3654

IoT sensor nodes	Network lifetime (rounds)					
	DEEC	PHC	HNS	CHSES	RDAC-BC	BDL-PPDT
100	1386	1492	1529	1588	1612	1793
200	1725	1807	1864	1918	2077	2218
300	2305	2271	2389	2405	2613	2756
400	2718	2789	2853	2885	3191	3362
500	3103	3326	3289	3463	3547	3633

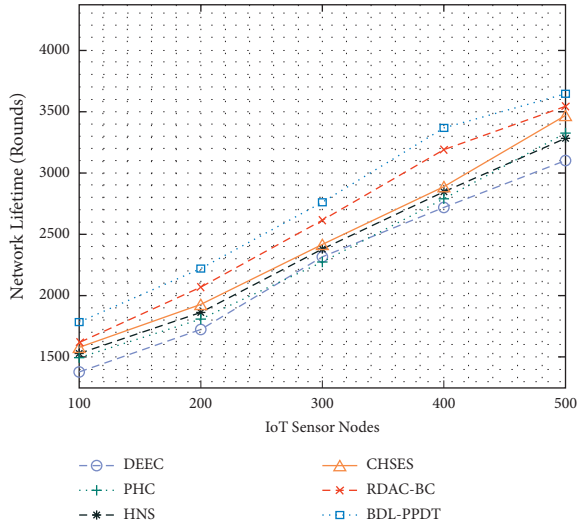


FIGURE 5: NLT analysis of BDL-PPDT technique with existing approaches.

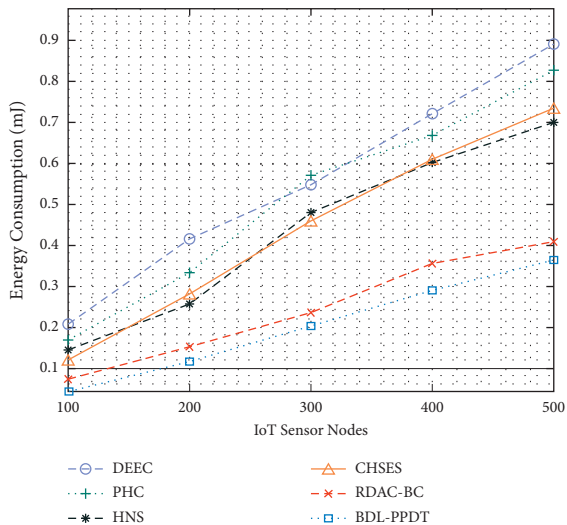


FIGURE 6: ECM analysis of BDL-PPDT technique with existing approaches.

TABLE 3: NASN analysis of the BDL-PPDT technique with different rounds.

No. of rounds	No. of alive sensor nodes					
	DEEC	PHC	HNS	CHSES	RDAC-BC	BDL-PPDT
400	404	406	451	476	500	500
800	384	394	436	458	495	499
1200	361	357	418	427	492	497
1600	322	359	390	412	486	492
2000	304	338	395	403	479	489
2400	205	227	288	259	451	470
2800	62	151	190	184	386	387
3200	20	32	37	50	309	320
3500	12	19	28	30	138	210

the BDL-PPDT technique has accomplished maximum NASN under every round. For instance, with 800 rounds, the BDL-PPDT technique has provided higher NASN of 499, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have gained lower NASN of 384, 394, 436, 458, and 495 nodes, respectively. Besides, with 3500 rounds, the BDL-PPDT technique has resulted in improved NASN of 210, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have led to reduced NASN of 12, 19, 28, 30, and 138 nodes, respectively.

The number of dead sensor node (NDSN) analysis of the BDL-PPDT technique with other methods under distinct rounds is given in Table 4 and Figure 8. The results implied that the BDL-PPDT technique has attained effective outcomes with the lower NDSN under all rounds. For instance, with 800 rounds, the BDL-PPDT technique has achieved minimal NDSN of 1, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have obtained maximum NDSN of 116, 106, 64, 42, and 5 nodes, respectively [28–31]. At the same time, with 3500 rounds, the BDL-PPDT technique has offered a least NDSN of 290, whereas the DEEC, PHC, HNS, CHSES, and RDAC-BC techniques have reached to an increased NDSN of 488, 481, 472, 470, and 362 nodes, respectively.

Here, the intrusion detection performance analysis of the BDL-PPDT technique is provided in Table 5 and Figure 9 [21, 22]. The results are tested using the KDDCup99 dataset

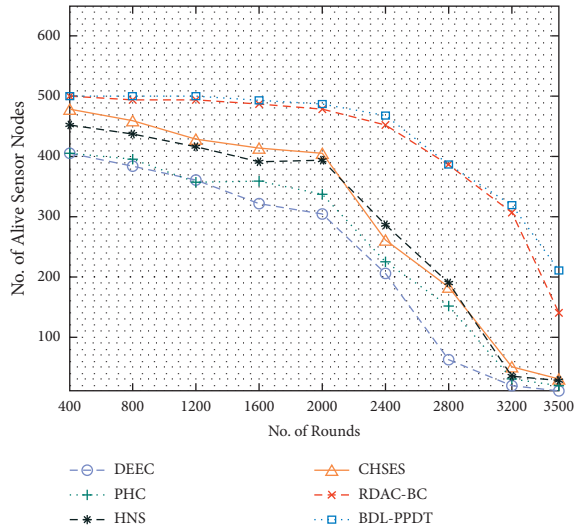


FIGURE 7: NASN analysis of BDL-PPDT technique with varying rounds.

TABLE 4: NDSN analysis of the BDL-PPDT technique with different rounds.

No. of rounds	No. of dead sensor nodes					
	DEEC	PHC	HNS	CHSES	RDAC-BC	BDL-PPDT
400	96	94	49	24	0	0
800	116	106	64	42	5	1
1200	139	143	82	73	8	3
1600	178	141	110	88	14	8
2000	196	162	105	97	21	11
2400	295	273	212	241	49	30
2800	438	349	310	316	114	113
3200	480	468	463	450	191	180
3500	488	481	472	470	362	290

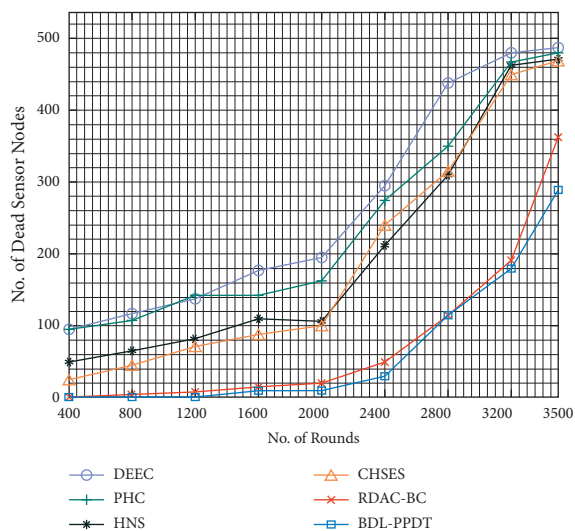


FIGURE 8: NDSN analysis of BDL-PPDT technique with varying rounds.

TABLE 5: Comparative analysis of BDL-PPDT technique with different measures.

Methods	Accuracy	Precision	Recall	F1-score	Far
DNN model	91.64	97.85	91.99	94.67	8.56
LSTM-RNN	93.39	98.11	94.41	96.12	6.81
GRU-RNN	92.63	97.52	93.45	95.34	7.57
DBN model	95.22	97.55	96.50	97.11	3.98
CNID	98.54	99.98	97.56	98.49	0.02
BDL-PPDT	98.15	99.99	98.64	98.96	0.01

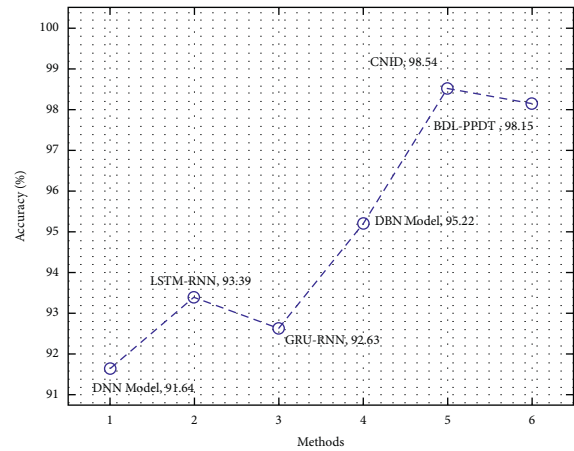


FIGURE 9: Accuracy analysis of BDL-PPDT technique with existing approaches.

[23] comprising different classes and 41 features. The results show that the DNN model has gained lower outcomes with the $accu_y$ of 91.64%, whereas the LSTM-RNN and GRU-RNN techniques have resulted in moderately reasonable $accu_y$ of 93.39% and 92.63%, respectively [35–38]. Moreover, the DBN and CNID models have accomplished considerable $accu_y$ values of 95.22% and 98.54%, respectively. However, the presented BDL-PPDT technique has reached to maximum outcome with the $accu_y$ of 98.15%. The abovementioned result analysis implied that the BDL-PPDT technique has outperformed the other existing techniques in terms of different measures.

5. Conclusion

In this study, an effective BDL-PPDT technique has been developed to accomplish secure data transmission in clustered IIoT environment. The BDL-PPDT technique has presented a new EMSA-C technique to choose a proper set of clusters in the IIoT system and construct clusters. Next, the MHA-BLSTM with SGDM model is utilized for intrusion detection and the hyperparameter tuning process is made by the SGDM model resulting in improved detection performance. To inspect the significant performance of the BDL-PPDT technique, a wide-ranging comparative analysis is made and the results are inspected in terms of different measures. The experimental outcome pointed out the improved performance of the BDL-PPDT technique over the recent methods in terms of different measures. In the future,

hyperparameter tuning process of the MHA-BLSTM model can be done by the meta-heuristic algorithms to improve the overall performance. Even though the BDL-PPDT method has an accuracy rate of just 98.15 percent, it still gives the best possible result. Because of the data analysis above, it was found that the BDL-PPDT technique outperformed the other current techniques on a wide range of different factors, and so it was recommended that people use it. Meta-heuristic methods will be utilized in the future to modify the hyperparameters of the MHA-BLSTM model, resulting in an overall improvement in overall performance.

Data Availability

The article contains all of the data.

Conflicts of Interest

The authors state that they do not have any conflicts of interest.

References

- [1] N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park, and J. H. Park, "A survey on cyber physical system security for iot: issues, challenges, threats, solutions," *J Inf Process Syst*, vol. 14, no. 6, pp. 1361–1384, 2018.
- [2] J. Rene Beulah, L. Prathiba, G. L. N Murthy, E. Fantin Irudaya Raj, and N. Arulkumar, "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model," *International Journal of Modeling, Simulation, and Scientific Computing*, 2020.
- [3] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," *IEEE Network*, vol. 28, no. 4, pp. 46–50, 2014.
- [4] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2015.
- [5] E. S. Madhan, S. Neelakandan, and R. Annamalai, "A novel approach for vehicle type classification and speed prediction using deep learning," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 5, pp. 2237–2242, 2020.
- [6] M. S. Hossain, M. Al-Hammadi, and G. Muhammad, "Automatic fruit classification using deep learning for industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 1027–1034, 2019.
- [7] D. Paulraj, "An automated exploring and learning model for data prediction using balanced CA-svm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1–12, 2020.
- [8] R. Iqbal, T. Maniak, F. Doctor, and C. Karyotis, "Fault detection and isolation in industrial processes using deep learning approaches," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 3077–3084, 2019.
- [9] R. S. Peres, A. Dionisio Rocha, P. Leitao, and J. Barata, "Idarts - towards intelligent data analysis and real-time supervision for industry 4.0," *Computers in Industry*, vol. 101, pp. 138–146, 2018.
- [10] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards blockchain-enabled security technique for industrial internet of things based decentralized applications," *Journal of Grid Computing*, vol. 18, no. 4, pp. 615–628, 2020.
- [11] M. S. Rahman, I. Khalil, N. Moustafa, A. P. Kalapaaking, and A. Bouras, "A blockchain-enabled privacy-preserving verifiable query framework for securing cloud-assisted industrial internet of things systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, 2021.
- [12] H. Zhang, G. Li, Y. Zhang, K. Gai, and M. Qiu, "Blockchain-based privacy-preserving medical data sharing scheme using federated learning," in *Proceedings of the International Conference on Knowledge Science, Engineering and Management*, pp. 634–646, Tokyo, Japan, August 2021.
- [13] B. D. Deebak and F. Al-Turjman, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements," *Journal of Information Security and Applications*, vol. 58, Article ID 102749, 2021.
- [14] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, p. 1, 2019.
- [15] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial iot systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.
- [16] R. Kumar and R. Tripathi, "DBTP2SF: a deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, Article ID e4222, 2021.
- [17] A.-A. A. Mohamed, Y. S. Mohamed, A. A. M. El-Gaafary, and A. M. Hemeida, "Optimal power flow using moth swarm algorithm," *Electric Power Systems Research*, vol. 142, pp. 190–206, 2017.
- [18] S. Neelakandan, M. A. Berlin, S. Tripathi, V. B. Devi, I. Bhardwaj, and N. Arulkumar, "IoT-based traffic prediction and traffic signal control system for smart city," *Soft Computing*, vol. 25, no. 18, pp. 12241–12248, 2021.
- [19] C. P. D. Cyril, J. R. Beulah, N. Subramani, P. Mohan, A. Harshavardhan, and D. Sivabalaselvamani, "An automated learning model for sentiment analysis and data classification of Twitter data using balanced CA-SVM," *Concurrent Engineering*, vol. 29, no. 4, pp. 386–395, 2021.
- [20] C. Ramalingam and P. Mohan, "An efficient applications cloud interoperability framework using I-anfis," *Symmetry*, vol. 13, no. 2, p. 268, 2021.
- [21] C. Han, Q. Lin, J. Guo, L. Sun, and Z. Tao, "A clustering algorithm for heterogeneous wireless sensor networks based on solar energy supply," *Electronics*, vol. 7, no. 7, p. 103, 2018.
- [22] V. Sindhu and M. Prakash, "A survey on task scheduling and resource allocation methods in fog based IoT applications," *Communication and Intelligent Systems*, vol. 120, pp. 89–97, 2020.
- [23] R. Kamalraj, S. Neelakandan, M. Ranjith Kumar, V. Chandra Shekhar Rao, R. Anand, and H. Singh, "Interpretable filter based convolutional neural network (IF-CNN) for glucose prediction and classification using PD-SS algorithm," *Measurement*, vol. 183, Article ID 109804, 2021.
- [24] S. Neelakandan, A. Arun, R. Ram Bhukya, B. M Hardas, T. Ch Anil Kumar, and M. Ashok, "An automated word embedding with parameter tuned model for web crawling," *Intelligent Automation & Soft Computing*, vol. 32, no. 3, pp. 1617–1632, 2022.
- [25] P. Asha, L. Natrayan, B. T. Geetha et al., "IoT enabled environmental toxicology for air pollution monitoring using AI

- techniques,” *Environmental Research*, vol. 205, Article ID 112574, 2022.
- [26] D. Venu, A. V. R. Mayuri, S. Neelakandan, G. L. N. Murthy, N. Arulkumar, and N. Shelke, “An efficient low complexity compression based optimal homomorphic encryption for secure fiber optic communication,” *Optik*, vol. 252, Article ID 168545, 2022.
- [27] S. Neelakandan, R. Annamalai, S. J. Rayen, and J. Arunajsmine, “Social media networks owing to disruptions for effective learning,” *Procedia Computer Science*, vol. 172, pp. 145–151, 2020.
- [28] S. Neelakandan, M. Prakash, S. Bhargava, K. Mohan, N. R. Robert, and S. Upadhye, “Optimal stacked sparse autoencoder based traffic flow prediction in intelligent transportation systems,” *Virtual and Augmented Reality for Automobile Industry: Innovation Vision and Applications*, vol. 412, pp. 111–127, 2022.
- [29] T. Kavitha, P. P. Mathai, C. Karthikeyan et al., “Deep learning based capsule neural network model for breast cancer diagnosis using mammogram images,” *Interdisciplinary Sciences: Computational Life Sciences*, vol. 14, no. 1, pp. 113–129, 2021.
- [30] G. Sunitha, K. Geetha, S. Neelakandan, A. K. S. Pundir, S. Hemalatha, and V. Kumar, “Intelligent deep learning based ethnicity recognition and classification using facial images,” *Image and Vision Computing*, vol. 121, Article ID 104404, 2022.
- [31] B. T. Geetha, P. Santhosh Kumar, B. Sathya Bama, S. Neelakandan, C. Dutta, and D. Vijendra Babu, “Green energy aware and cluster based communication for future load prediction in IoT,” *Sustainable Energy Technologies and Assessments*, vol. 52, Article ID 102244, 2022.
- [32] D. Oliva, S. Esquivel-Torres, S. Hinojosa et al., “Opposition-based moth swarm algorithm,” *Expert Systems with Applications*, vol. 184, Article ID 115481, 2021.
- [33] O. A. Alzubi, J. A. Alzubi, K. Shankar, and D. Gupta, “Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, Article ID e4360, 2021.
- [34] S. Wang, Y. Zhu, W. Gao, M. Cao, and M. Li, “Emotion-semantic-enhanced bidirectional LSTM with multi-head attention mechanism for microblog sentiment analysis,” *Information*, vol. 11, no. 5, p. 280, 2020.
- [35] A. Harshavardhan, P. Boyapati, S. Neelakandan, A. A. Abdul-Rasheed Akeji, A. K. Singh Pundir, and R. Walia, “LSGDM with biogeography-based optimization (BBO) model for healthcare applications,” *Journal of Healthcare Engineering*, vol. 2022, pp. 1–11, Article ID 2170839, 2022.
- [36] G. Liu and J. Zhang, “CNID: research of network intrusion detection based on convolutional neural network,” *Discrete Dynamics in Nature and Society*, vol. 2020, pp. 1–11, Article ID 4705982, 2020.
- [37] H. Singh, D. Ramya, R. Saravanakumar et al., “Artificial intelligence based quality of transmission predictive model for cognitive optical networks,” *Optik*, vol. 257, Article ID 168789, 2022.
- [38] University of California, *KDD CUP 1999 Data Set*, University of California, CA, USA, 1999, <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.