Computers, Materials & Continua
DOI: 10.32604/cmc.2022.030825
Article

Tech Science Press

Privacy Preserving Blockchain with Optimal Deep Learning Model for Smart Cities

K. Pradeep Mohan Kumar[1], Jenifer Mahilraj[2], D. Swathi[3], R. Rajavarman[4], Subhi R. M. Zeebaree[5], Rizgar R. Zebari[6], Zryan Najat Rashid[7] and Ahmed Alkhayyat[8,*]

[1]Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai, 603203, India
[2]Department of Computer Science and Information Technology, School of Engineering and Technology, Kebridehar University, Kebridehar, 250, Ethiopia
[3]Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Tiruchirappalli, 621112, India
[4]Department of Computer Science and Engineering, K.Ramakrishnan College of Technology, Tiruchirappalli, 621112, India
[5]Energy Department, Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq
[6]Computer Science Department, College of Science, Nawroz University, Duhok, Iraq
[7]Computer Network Department, Technical College of Informatics, Sulaimani Polytechnic University, Sulaimani, Iraq
[8]College of Technical Engineering, The Islamic University, Najaf, Iraq
*Corresponding Author: Ahmed Alkhayyat. Email: ahmedalkhayyat85@iunajaf.edu.iq
Received: 02 April 2022; Accepted: 25 May 2022

Abstract: Recently, smart cities have emerged as an effective approach to deliver high-quality services to the people through adaptive optimization of the available resources. Despite the advantages of smart cities, security remains a huge challenge to be overcome. Simultaneously, Intrusion Detection System (IDS) is the most proficient tool to accomplish security in this scenario. Besides, blockchain exhibits significance in promoting smart city designing, due to its effective characteristics like immutability, transparency, and decentralization. In order to address the security problems in smart cities, the current study designs a Privacy Preserving Secure Framework using Blockchain with Optimal Deep Learning (PPSF-BODL) model. The proposed PPSF-BODL model includes the collection of primary data using sensing tools. Besides, z-score normalization is also utilized to transform the actual data into useful format. Besides, Chameleon Swarm Optimization (CSO) with Attention Based Bidirectional Long Short Term Memory (ABiLSTM) model is employed for detection and classification of intrusions. CSO is employed for optimal hyperparameter tuning of ABiLSTM model. At the same time, Blockchain (BC) is utilized for secure transmission of the data to cloud server. This cloud server is a decentralized, distributed, and open digital ledger that is employed to store the transactions in different methods. A detailed experimentation of the proposed PPSF-BODL model was conducted on benchmark dataset and the outcomes established the supremacy of the proposed PPSF-BODL model over recent approaches with a maximum accuracy of 97.46%.

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Keywords: Blockchain; smart city; security; intrusion detection system; chameleon swarm optimization; deep learning; parameter tuning

1 Introduction

Globally, technological advancements has brought improvements in lifestyle while sensing technology has changed the way of life in particular. This next-gen technology helps the industries and economies to explore much more opportunities [1]. While the individuals are linked with one another via smartphones, laptops, and tabs, on the other hand, smart gadgets, meters, and appliances are commonly used in almost all the cities across the globe [2]. Motor vehicles and community systems, moreover services, are most probably associated thus forming a new paradigm called 'internet of things' (IoT). Additionally, researchers, scholars and institutions are enhancing their standards and IoT protocols to standardize their gadgets' associations [3]. Subsequently, cities are on expansion mode in terms of infrastructure, control systems, services, and monitoring systems so as to adopt the changes introduced recently. Location services, smart traffic, weather, and smart transportation are also linked among with each other [4]. But, this sort of uncontrolled development of the cities brings forth totally new circumstances and problems which should be taken into account by government officials as well as stakeholders. Smart city concepts are completely based on embedded structures, intelligent technologies, and sensing technology. Generally, smart cities use information technologies and fixed infrastructures to enhance the living standards. There exists two chief problems such as security and electrical crime concerns [5]. Smart city security is ensured by three elements such as governance, technology and society.

Intrusion Detection Systems (IDS) are highly efficient tools in terms of monitoring network activities, identification of unauthorized usage, detection of information system destruction, and system protection from interior and exterior intrusions (intrusions from inside or outside the network) [6,7]. Meanwhile, IDS is recommended as a highly important security solution for newly-developed online web-based applications in relation to smart cities and Internet of Things (IoT) atmosphere. In general, IDS-based systems commence a greater quantity of unsuitable and fake alarms, whenever abnormal performances are identified [8]. If the activated fake alarm rate is too high, I t tend to diminish the performance of IDS in contrast to cyber-attacks and makes the job of security analysts completely challenging. Further, it also incurs heavy cost for detection, management and computation of intrusions. In addition to these, the risks for failure are high when using traditional IDS-based methodology for IoT since the latter does not approve the speedy development of smart city applications [9]. Thus, a powerful information security system model is required to be specific that allows the fast development of smart city applications under IoT environment [10].

In literature [11], the researchers proposed a smart city intrusion detection architecture based Restricted Boltzmann Machines (RBM). RBM is employed owing to its capacity to learn high-level features from original information in an unsupervised manner and the ability to depict the information generated by smart sensors and meters. Additionally, the extracted features and distinct classifications are trained in this method. In the study conducted earlier [12], the researchers proposed a video-based IDS with DL. Now, You YOLO approach is employed for object recognition whereas intrusion is detected using the presented method by shifting the centre of mass of the identified objects. Furthermore, Simple Online and Real-time Tracking (SORT) approach is utilized to track real-time intruders. Ramadan [13] proposed a simple and two light approaches for detection and prevention of intrusions in smart city—multipath-based IDS (MBIDS) and Threshold-based IDS

(TBIDS). The researcher applied cross-layer method between network and the application layers for intrusion detection.

Gupta et al. [14] presented a hybrid optimization and DL-centric IDS to resolve the problem in IoT-assisted smart cities. Initially, the dataset endures pre-processing to obtain accurate and effective IDSs. Next, clustering and FS are implemented by MinK-means Algorithm and Hybrid Chicken Swarm Genetic Algorithm (HCSGA). Qureshi et al. [15] aimed at managing a minimum of three components in smart cities such as smart living, security provision, and smart mobility by designing three natural-inspired solutions. Daniel et al. [16] presented Cognitive Smart City Network (CSC-Net) structure that describes how information is gathered from the application of smart cities and it is examined through cognitive computation. The study forecasted Mobile Edge Computing solution (MEC) that allows node cooperation among IoT gadgets to ensure reliable and secure transmission between fog layer and smart device and equally between cloud and fog layers. In literature [17], an IDS was presented for detecting the injection attacks in IoT applications. Here, two kinds of FS approaches (recursive feature elimination and constant removal) were utilized and were validated using several ML classification methods such as Decision Tree, SVM, and Random Forest. Few other models based on blockchain are also available in the literature [18–25].

In this background, the current study designs Privacy Preserving Secure Framework using Blockchain with Optimal Deep Learning (PPSF-BODL) model for smart cities. The proposed PPSF-BODL model uses z-score normalization to transform the actual data into useful format. Also, Chameleon Swarm Optimization (CSO) with Attention-based Bidirectional Long Short Term Memory (ABiLSTM) model is engaged for detection and classification of intrusions. Moreover, Blockchain (BC) is utilized for secure transmission of the data to cloud server. A detailed experimentation of the proposed PPSF-BODL model was conducted on benchmark dataset.

2 The Proposed Model

In this study, a novel PPSF-BODL technique has been developed for both identification and classification of intrusions in smart city environment. The proposed PPSF-BODL model includes the collection of primary data using sensing tools. Also, z-score normalization is utilized to transform the actual data into useful format. Next, ABiLSTM model is employed for intrusion detection and classification. Finally, CSO is employed for optimal hyperparameter tuning of ABiLSTM model.

2.1 ABiLSTM Based Classification

Once the input data is pre-processed, ABiLSTM model is employed for intrusion detection and classification [26]. BiLSTM model is employed to enhance the learning abilities of conventional LSTM model by considering bidirectional relationship of the data. It helps in attaining more structural data via gating scheme which in turn improves the efficiency. Further, it also performs data encoding to obtain data features that enhance the generalization abilities. It begins with input series after which the inverse form of the input series is combined with LSTM model. BiLSTM approach is produced via forward h_t and backward layers h'_t. At last, the end outcome can be a product at every instance via the integration of outcomes at the respective forward and backward layer moments. It is mathematically defined as follows

$$h_t = f(w_1 x_t + w_2 h_{t-1} + b)$$

$$h'_t = f(w_3 x_t + w_5 h_{t-1} + b')$$

$$y_t = w_4 h_t + w_6 h'_t + b_y$$

Here, $w_1 - w_6$ denotes the respective weight coefficients; $h_t,\ h'_t, x_t,\ and\ y_t$, represent the vectors for forward propagation, backward propagation, input and output layers respectively; b, b′, and b_y denote the biases.

ABiLSTM model enables the learning of related data in various representative sub-spaces. It processes the data concurrently to reduce computation complexity. Based on the final hidden layer h_i^r outcome of BiLSTM model, the present data can be defined by h_1^t, h_2^t,. . ., h_N^t. Afterward, it is fed into multi-head self-attention, a new representation s_t for data which is attained using the succeeding equations.

$$\begin{aligned} s_t &= MultiHeadAttention\ \left(h_1^t,\ h_2^t,\ \ldots,\ h_N^t\right) \\ &= Concat\ \left(head_1\left(h_N^t\right),\ head_2\left(h_N^t\right),\ \ldots,\ head_k\left(h_N^t\right)\right) W^0, \end{aligned} \tag{1}$$

where $head_i\left(h_N^r\right)$ represents the i-th attention head value and W^0 denotes linearization mapping matrix. For $head_i\left(h_N^t\right)$ $(i\ =\ 1, 2,\ \ldots, N)$, it is determined as follows.

$$\begin{aligned} &\alpha_1, \alpha_2, \ldots, \alpha_N = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right) y, \\ &head_i\left(h_N^t\right) = \sum_{j=1}^{N} \alpha_j v_j, \end{aligned} \tag{2}$$

where, K, and y represent the query, key, and value matrix respectively. The respective vectors q, k_i and v_i are defined below

$$q,\ k_i,\ v_i = W^q h_N^r,\ W^k h_i^t,\ W^v h_i^r, \tag{3}$$

where W^q, W^k, and W^v denote the weight matrix that vary in different attention heads. Fig. 1 illustrates the structure of BiLSTM.

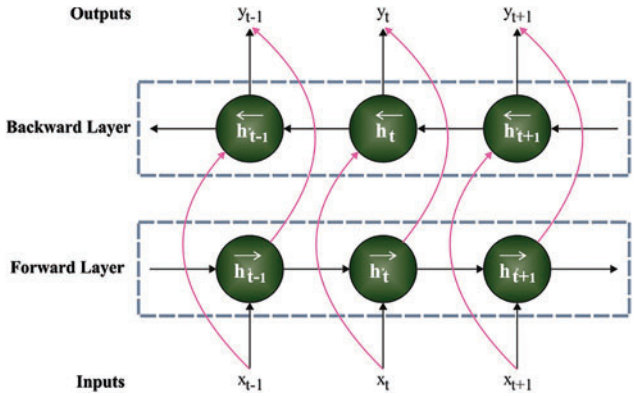

Figure 1: Structure of BiLSTM

2.2 CSO Based Hyperparameter Optimization

In the final stage, CSO is employed for optimal hyperparameter tuning of ABiLSTM model. In order to optimally determine the hyper-parameters, CSO technique is utilized which enhances the efficiency of the entire classifier. CSO [27] technique is a meta-heuristic approach that follows the

initialization of population to determine the optimization process. Consider that the total number of populations is C which exists in the searching space of D. An initial population is generated from the dimension composed from arbitrary initialization in the searching space as given below.

$$a^i = L_j + rand \times \left(U_j - L_j\right) \tag{4}$$

An initial vector of i^{th} chameleon is demonstrated as a^i. The lower and upper limits of the searching area are denoted by L_j and U_j in j^{th} dimension correspondingly. *rand* denotes the arbitrarily-produced number that decreases in the range of zero to one.

An improved capability of chameleons to search from the searching space is formulated as follows

$$\rho = \delta \exp^{(-\alpha t/R)} \tag{5}$$

Now, ρ represents the parameter employed during iteration which diminishes with enhancing iterations. δ, α, and β illustrate the presenting parameters employed for accomplishing exploration as well as exploitation stages. The rotating-centred co-ordinate, employed for the upgradation of location of the chameleons in searching space is offered as follows.

$$arand_r^i = m \times ac_r^i \tag{6}$$

$arand_r^i$ signifies the rotating centered co-ordinate of chameleons. m is employed to denote the rotation matrix and ac_r^i is employed to represent the center co-ordinates at r^{th} iteration. The inertia weight of the iterations is offered as given below.

$$W = (1 - r/R)^{\left(\lambda\sqrt{r/R}\right)} \tag{7}$$

At this point, W signifies the weight of inertias, λ indicates the arbitrary number used to control the exploitation capability. The value of λ corresponds to one. The acceleration rate of the chameleon is calculated as follows.

$$y = 2590 \times \left(1 - \exp^{-\log(r)}\right) \tag{8}$$

whereas y is used to define the acceleration of chameleons. It can be understood that the CSO initialized the optimization and the chameleon locations are upgraded using the formulas given below.

$$a_{r+1}^{ij} = \begin{cases} a_r^{ij} + p_1\left(P_r^{ij} - G_r^j\right) rand_1 + p_2\left(G_r^j - a_r^{ij}\right) rand_2 & rand_i \geq P \\ a_r^{ij} + \rho\left(U^j - L^j\right) rand_3 + L_b^j sgn\left(rand - 0.5\right) & rand_j < P \end{cases} \tag{9}$$

$$a_{r+1}^i = arand_r^i + \bar{a}_r^i \tag{10}$$

$$a_{r+1}^i = \bar{a}_r^i + \left((v_r^{ij})^2 - \left(v_{r-1}^{ij}\right)^2\right) / (2y) \tag{11}$$

Here, G_r^j indicates the global optimal location of chameleons and v_r^{ij} signifies the novel velocity of r^{th} chameleon. When some chameleon goes to the exterior of searching space, then it can be sent back for constraint defined earlier. Fitness Function (FF) is measured during every iteration to forecast the chameleon with optimum fitness. Though it may be frequent, it still fulfills the complete iteration cycles. Fig. 2 depicts the processes involved in CSO technique.

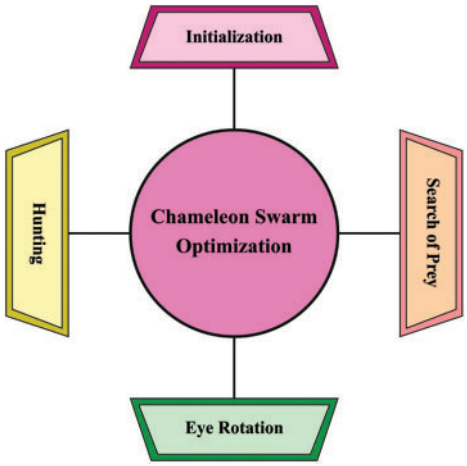

Figure 2: Processes of CSO technique

2.3 Blockchain Technology

Blockchain (BC) is used for secure transmission of the data to cloud server. This cloud server is a decentralized, distributed, and open digital ledger that is employed to store the transactions in different ways. BC is a set of blocks where each block is made up of timestamp, hash values of the existing and current blocks, and transaction details (bitcoin, ethereum). BC is a shared, decentralized and a public digital ledger which is employed to store the transaction details in a distinct manner. Therefore, an intruder record could not be modified for every block that is made up of cryptographic values of the current block. Fig. 3 demonstrates the structure of BC. BC provides the ability to distribute the ledger of information in a trusted, shared, safe, and decentralized manner. Decentralized storage is a kind of BC which is employed to store the maximum information that is interconnected with current and previous blocks through smart contract code. LitecoinDB, Swarm, SiacoinDB, MoneroDB, BigchainDB, IPFS, and so on, have been employed for decentralized data. Interplanetary File System (IPFS) is determined as shared, Point-to-Point, and decentralized dataset that is connected and transmits typical files. IPFS is employed with BC method for IoT function to gain maximal throughput.

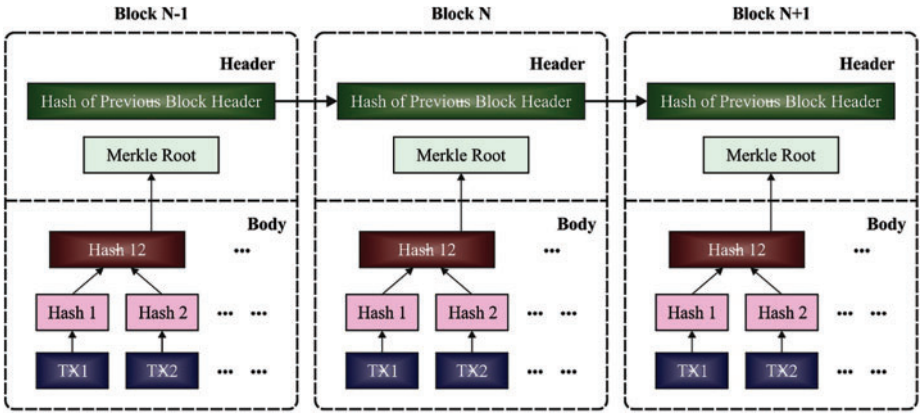

Figure 3: Structure of BC

3 Performance Validation

In this section, the intrusion detection performance of the proposed PPSF-BODL model was validated using NSL-KDD 2015 dataset. It includes 41 features and 125973 samples under two classes (normal-67343 and anomaly-58630).

Fig. 4 demonstrates the confusion matrices generated by PPSF-BODL model on distinct ratios of training set (TRS) and testing set (TSS). With 80% of TRS, the proposed PPSF-BODL model identified 52411 samples as normal and 45536 samples as samples with anomalies. In addition, with 20% of TSS, PPSF-BODL model categorized 13195 samples as normal and 11318 samples as anomalies. Next, with 70% of TRS, PPSF-BODL model found 45892 samples under normal category while 39995 samples as anomalies. With 30% of TSS, the proposed PPSF-BODL model classified 19,710 samples under normal and 17123 samples under anomalies.

Tab. 1 displays the comprehensive IDS classification results accomplished by PPSF-BODL model with 80% of TRS and 20% of TSS. Fig. 5 provides the thorough classification results accomplished by PPSF-BODL model with 80% of TRS. The figure infer that proposed PPSF-BODL model identified normal class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.19%, 97.37%, 97.37%, and 97.37% respectively. Further, PPSF-BODL model recognized anomaly class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.19%, 96.99%, 96.98%, and 96.99% respectively. Moreover, the proposed PPSF-BODL model achieved average $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.19%, 97.29%, 97.27%, and 97.28% respectively.

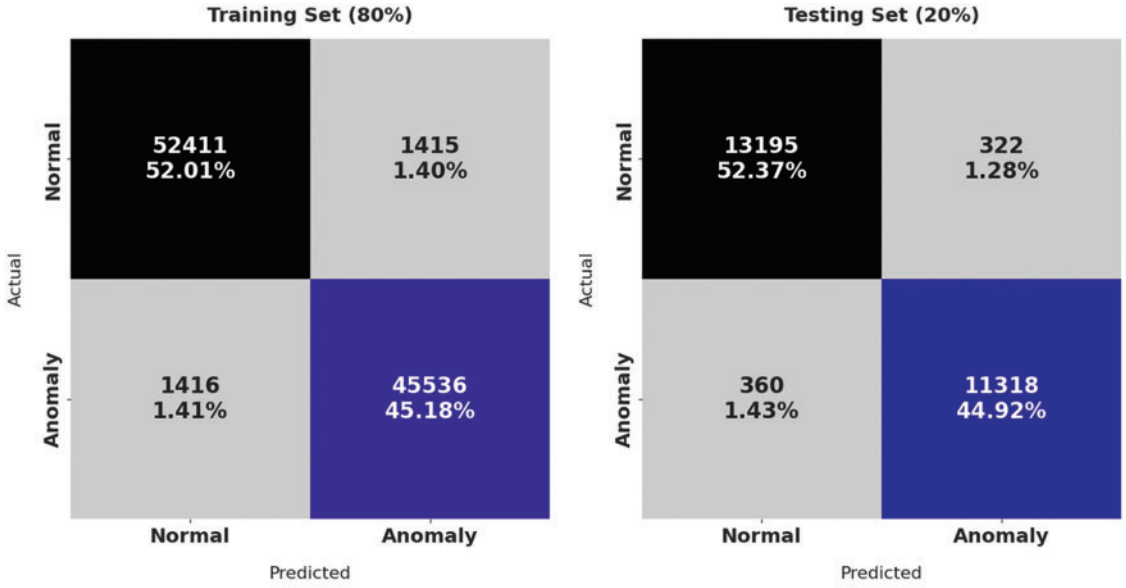

Figure 4: (Continued)

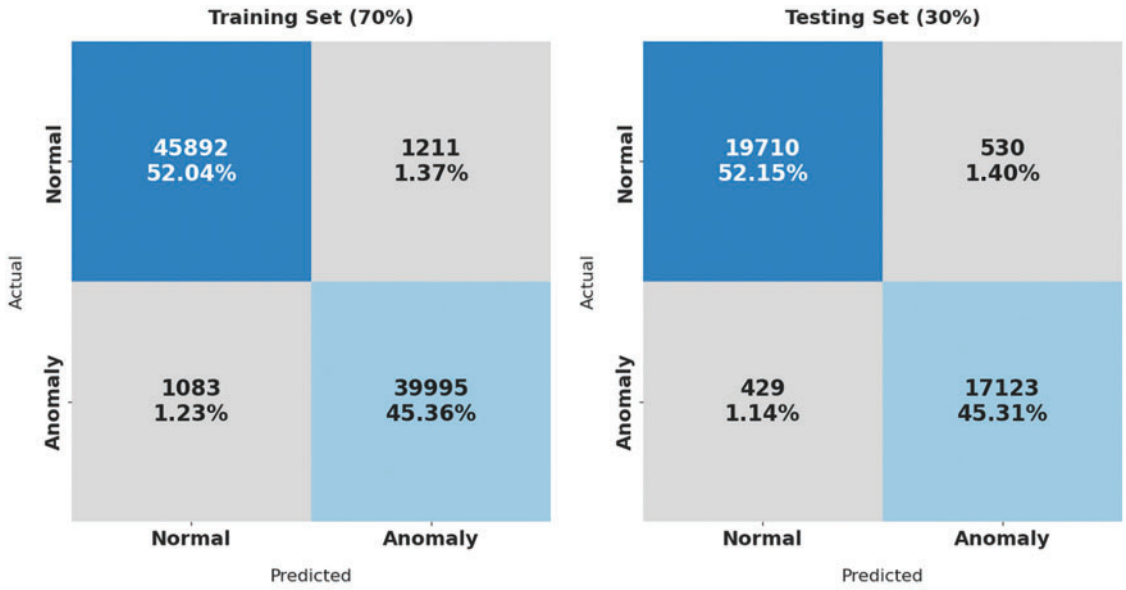

Figure 4: Confusion matrix of PPSF-BODL technique under distinct TRS and TSS

Table 1: Results of the analysis of PPSF-BODL technique under distinct measures on 80% of TRS and 20% of TSS

Class labels	Accuracy	Precision	Recall	F-score
Training set (80%)				
Normal	97.19	97.37	97.37	97.37
Anomaly	97.19	96.99	96.98	96.99
Average	97.19	97.18	97.18	97.18
Testing set (20%)				
Normal	97.29	97.34	97.62	97.48
Anomaly	97.29	97.23	96.92	97.08
Average	97.29	97.29	97.27	97.28

Fig. 6 exhibits the comprehensive classification results accomplished by PPSF-BODL model with 20% of TSS. The figure corresponds that the proposed PPSF-BODL model acknowledged normal class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.29%, 97.34%, 97.62%, and 97.48% respectively. Likewise, PPSF-BODL model recognized the anomaly class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.29%, 97.23%, 96.92%, and 97.08% respectively. Furthermore, the proposed PPSF-BODL model achieved average $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.29%, 97.29%, 97.27%, and 97.28% respectively.

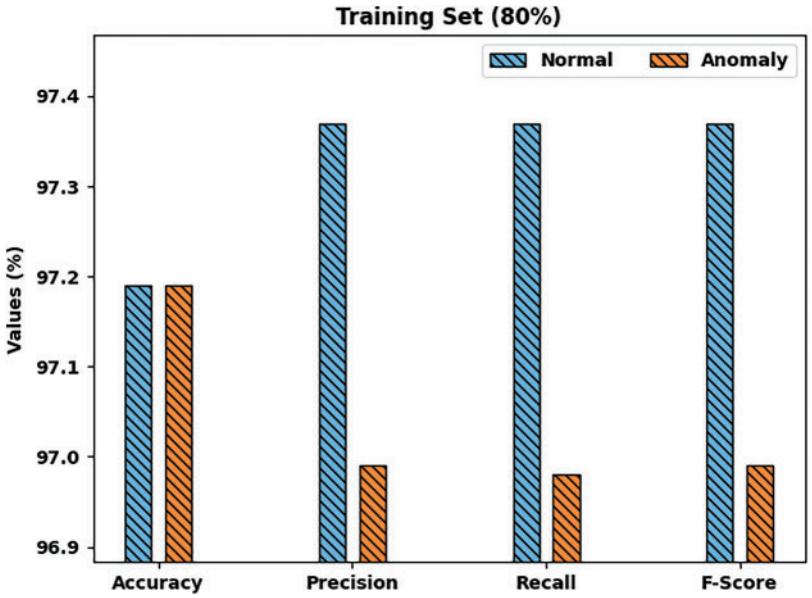

Figure 5: Results of the analysis of PPSF-BODL technique on 80% of TRS

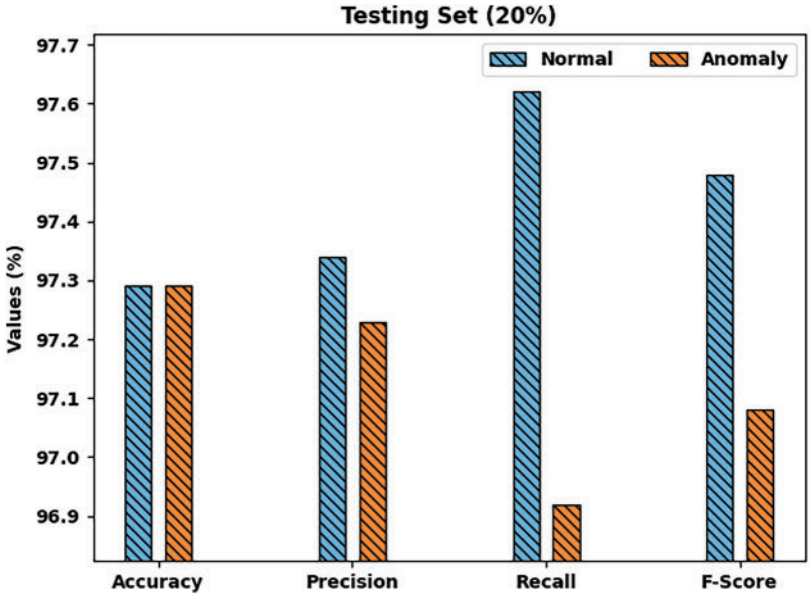

Figure 6: Results of the analysis of PPSF-BODL technique on 20% of TSS

Both Training Accuracy (TA) and Validation Accuracy (VA), attained by the proposed PPSF-BODL model on 80:20 of TRS/TSS data, were assessed and the results are demonstrated in Fig. 7. The experimental outcomes imply that the proposed PPSF-BODL model gained the maximum TA and VA values. To be specific, VA seemed to be higher than TA.

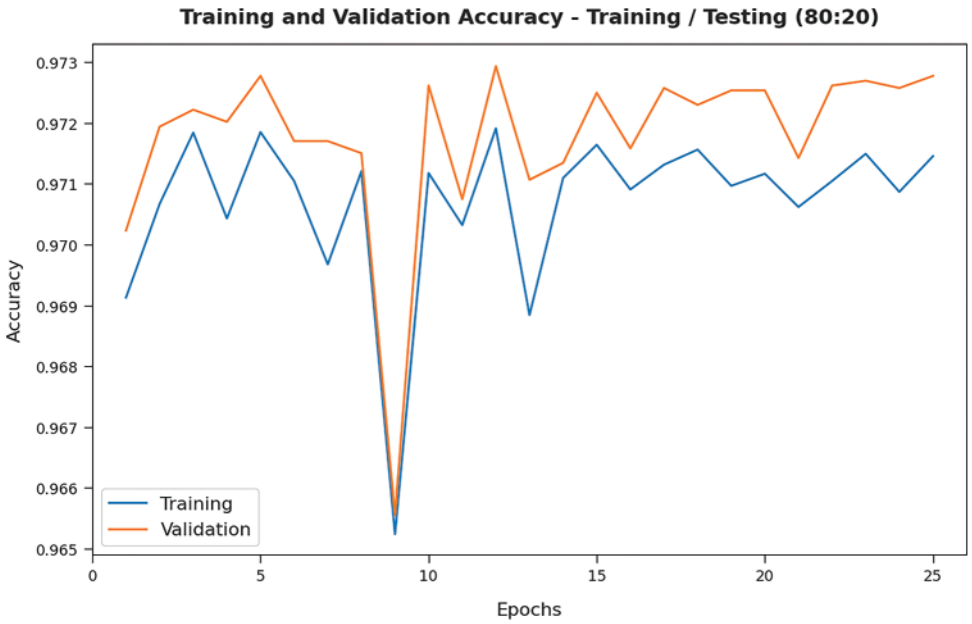

Figure 7: TA and VA analyses results of PPSF-BODL technique on TRS/TSS of 80:20

Both Training Loss (TL) and Validation Loss (VL), achieved by PPSF-BODL model on 80:20 of TRS/TSS data, were analyzed and the results are showcased in Fig. 8. The experimental outcomes infer that the proposed PPSF-BODL model accomplished the least TL and VL values. To be specific, VL seemed to be lower than TL.

Figure 8: TL and VL analyses results of PPSF-BODL technique on TRS/TSS of 80:20

Tab. 2 provides a brief overview of IDS classification outcomes accomplished by PPSF-BODL model with 70% of TRS and 30% of TSS.

Table 2: Results of the analysis of PPSF-BODL technique on 70% of TRS and 30% of TSS

Class labels	Accuracy	Precision	Recall	F-score
Training set (70%)				
Normal	97.40	97.69	97.43	97.56
Anomaly	97.40	97.06	97.36	97.21
Average	97.40	97.38	97.40	97.39
Testing set (30%)				
Normal	97.46	97.87	97.38	97.63
Anomaly	97.46	97.00	97.56	97.28
Average	97.46	97.43	97.47	97.45

Fig. 9 demonstrates the detailed classification results attained by the proposed PPSF-BODL model with 70% of TRS. The figure indicates that PPSF-BODL model identified normal class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.40%, 97.69%, 97.43%, and 97.56% respectively. Besides, PPSF-BODL model recognized anomaly class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.40%, 97.06%, 97.36%, and 97.21% respectively. Moreover, the proposed PPSF-BODL model attained average $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.40%, 97.38%, 97.40%, and 97.39% respectively.

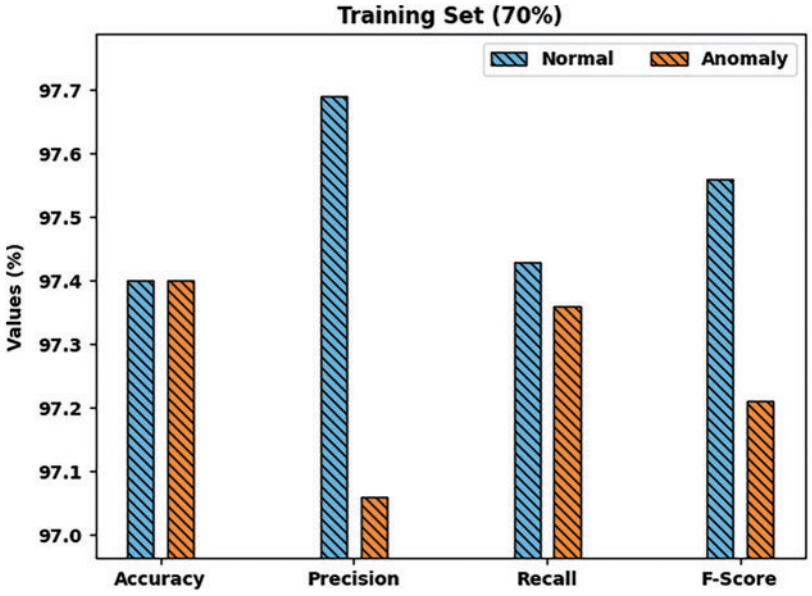

Figure 9: Results of the analysis of PPSF-BODL technique on 70% of TRS

Fig. 10 exhibits the comprehensive classification results achieved by PPSF-BODL model with 30% of TSS. The figure shows that PPSF-BODL model recognized normal class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.46%, 97.87%, 97.38%, and 97.63% respectively. Also, PPSF-BODL model recognized anomaly class with $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.46%, 97.00%, 97.56%,

and 97.28% respectively. Furthermore, PPSF-BODL model attained average $accu_y$, $prec_n$, $reca_l$, and F_{score} values such as 97.46%, 97.43%, 97.47%, and 97.45% respectively.

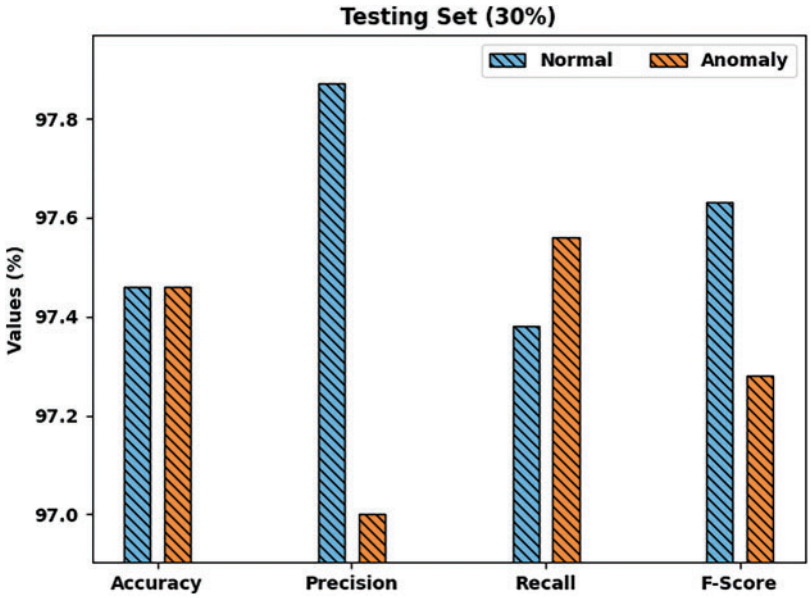

Figure 10: Results of the analysis of PPSF-BODL technique on 30% of TRS

The TA and VA values gained by the proposed PPSF-BODL algorithm on 70:30 of TRS/TSS data are demonstrated in Fig. 11. The experimental outcomes infer that the proposed PPSF-BODL model gained the maximum TA and VA values. To be specific, VA seemed to be higher than TA.

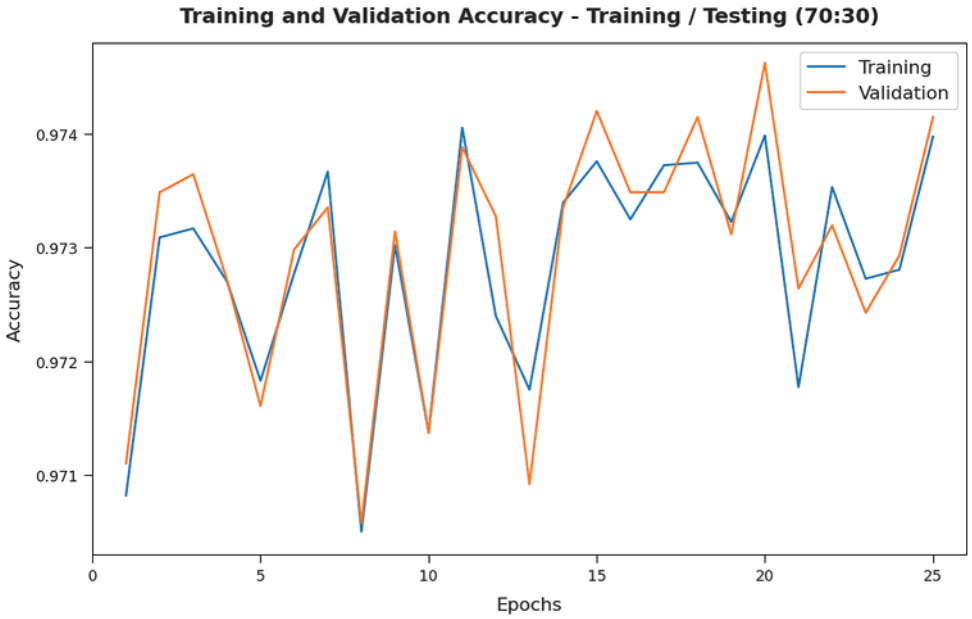

Figure 11: TA and VA analyses results of PPSF-BODL technique on TRS/TSS of 70:30

TL and VL values, achieved by the proposed PPSF-BODL technique on 70:30 of TRS/TSS data, are portrayed in Fig. 12. The experimental outcomes infer that PPSF-BODL technique accomplished the minimal TL and VL values. Specifically, VL appeared to be lesser than TL.

Figure 12: TL and VL analyses results of PPSF-BODL technique on TRS/TSS of 70:30

Finally, Tab. 3 and Fig. 13 highlight the comparative analysis results accomplished by PPSF-BODL model and other recent models [20]. As per the results, CS-PSO and GB models achieved less $accu_y$ values such as 76.37% and 84.47%. At the same time, Gaussian model, DNN-SVM, and soft K-means models exhibited slightly improved $accu_y$ values. Though DBN, Cuckoo opt., BIDS, and genetic algorithm models reached moderately closer $accu_y$ values such as 96.89%, 96.56%, 96.13%, and 96.04% correspondingly, the proposed PPSF-BODL system outperformed other methodologies with a maximum $accu_y$ of 97.46%.

Table 3: Comparative analysis results of PPSF-BODL model and other recent approaches

Methods	Accuracy (%)
PPSF-BODL	97.46
DBN model	96.89
Cuckoo opt. algorithm	96.56
CS-PSO algorithm	76.37
BIDS model	96.13
Gaussian model	90.37
DNN-SVM model	92.81
Genetic algorithm	96.04
Soft K-means	94.46
GB model	84.47

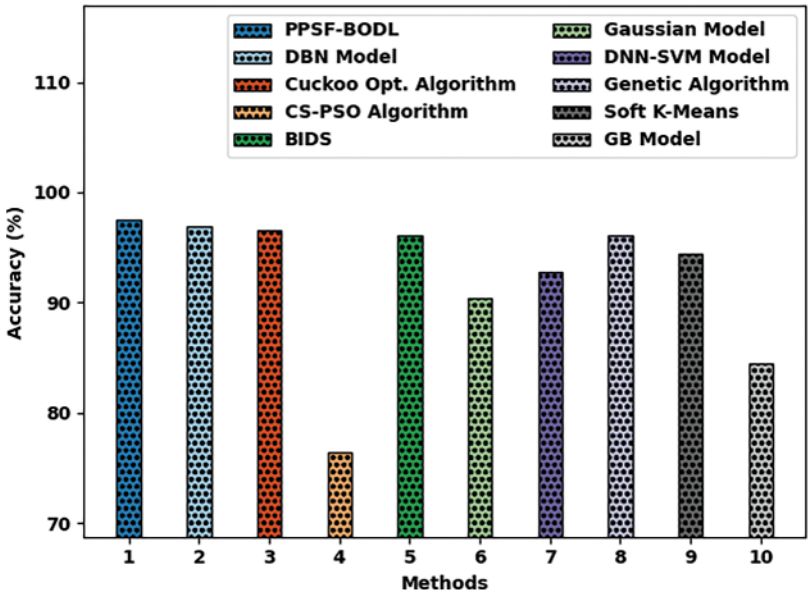

Figure 13: Comparative analysis results of PPSF-BODL technique and other recent models

The above mentioned results and discussion ensured the superiority of the proposed PPSF-BODL model over other methods.

4 Conclusion

In this study, a novel PPSF-BODL approach has been developed for identification and classification of intrusions in smart city environment. The proposed PPSF-BODL model includes primary data collection with the help of sensing tools. Further, z-score normalization is also utilized to transform the actual data into useful format. Next, ABiLSTM model is employed for detection and classification of intrusions. Finally, CSO is employed for optimal hyperparameter tuning of ABiLSTM model. BC is utilized for secure transmission of the data to cloud server. This cloud server is a decentralized, distributed, and open digital ledger that is employed to store the transactions through different methods. A detailed experimentation of the proposed PPSF-BODL model was carried out on benchmark dataset and the outcomes established the supremacy of the proposed PPSF-BODL model over recent approaches with a maximum accuracy of 97.46%. In future, CSO algorithm can be applied to feature subset selection so as to enhance the intrusion detection results.

Funding Statement: The authors received no specific funding for this study.

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

References

[1] D. Li, L. Deng, M. Lee and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *International Journal of Information Management*, vol. 49, pp. 533–545, 2019.

[2] S. Vimal, A. Suresh, P. Subbulakshmi, S. Pradeepa and M. Kaliappan, "Edge computing-based intrusion detection system for smart cities development using IoT in urban areas," in *Internet of Things in Smart Technologies for Sustainable Urban Development*, EAI/Springer Innovations in Communication and Computing Book Series, Cham: Springer, pp. 219–237, 2020.
[3] M. Aloqaily, S. Otoum, I. A. Ridhawi and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, vol. 90, pp. 101842, 2019.
[4] V. Subbarayalu, B. Surendiran and P. Arun Raj Kumar, "Hybrid network intrusion detection system for smart environments based on internet of things," *The Computer Journal*, vol. 62, no. 12, pp. 1822–1839, 2019. https://doi.org/10.1093/comjnl/bxz082.
[5] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung and M. K. A. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: A review," *Procedia Computer Science*, vol. 171, pp. 1251–1260, 2020.
[6] A. Procopiou and T. M. Chen, "Explainable ai in machine/deep learning for intrusion detection in intelligent transportation systems for smart cities," in *Explainable Artificial Intelligence for Smart Cities*, Boca Raton: CRC Press, pp. 297–321, 2021.
[7] W. Kaddah, E. S. Gooya, M. Elbouz and A. Alfalou, "Securing smart cities using artificial intelligence: Intrusion and abnormal behavior detection system," in *Pattern Recognition and Tracking XXXII*, United States, Springer, vol. 11735, pp. 17, 2021. https://doi.org/10.1117/12.2586774.
[8] S. Venkatraman, P. Muthusamy, B. Balusa, T. Jayasankar, G. Kavithaa *et al.,* "Time dependent anomaly detection system for smart environment using probabilistic timed automaton," *Journal of Ambient Intelligence and Humanized Computing*, vol. 2021, pp. 1–9, 2021. https://doi.org/10.1007/s12652-020-02769-3.
[9] N. Al-Taleb and N. Saqib, "Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments," *Applied Sciences*, vol. 12, no. 4, pp. 1–16, 2022.
[10] P. Kumar, G. P. Gupta and R. Tripathi, "TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," *Journal of Systems Architecture*, vol. 115, pp. 1–21, 2021.
[11] A. Elsaeidy, K. Munasinghe, D. Sharma and A. Jamalipour, "Intrusion detection in smart cities using restricted boltzmann machines," *Journal of Network and Computer Applications*, vol. 135, pp. 76–83, 2019.
[12] R. Nayak, M. M. Behera, U. C. Pati and S. K. Das, "Video-based real-time intrusion detection system using deep-learning for smart city applications," in *2019 IEEE Int. Conf. on Advanced Networks and Telecommunications Systems (ANTS)*, Goa, India, pp. 1–6, 2019.
[13] R. A. Ramadan, "Efficient intrusion detection algorithms for smart cities-based wireless sensing technologies," *Journal of Sensor and Actuator Networks*, vol. 9, no. 39, pp. 1–22, 2020.
[14] S. Gupta, M. Tripathi and J. Grover, "Hybrid optimization and deep learning based intrusion detection system," *Computers and Electrical Engineering*, vol. 100, pp. 1–16, 2022. https://doi.org/10.1016/j.compeleceng.2022.107876.
[15] K. N. Qureshi, A. Ahmad, F. Piccialli, G. Casolla and G. Jeon, "Nature-inspired algorithm-based secure data dissemination framework for smart city networks," *Neural Computing and Applications*, vol. 33, no. 17, pp. 10637–10656, 2021.
[16] D. Daniel, N. Preethi, A. Jakka and S. Eswaran, "Collaborative intrusion detection system in cognitive smart city network (CSC-net)," *International Journal of Knowledge and Systems Science*, vol. 12, no. 1, pp. 60–73, 2021.
[17] T. Gaber, A. E. Ghamry and A. E. Hassanein, "Injection attack detection using machine learning for smart IoT applications," *Physical Communication*, 2022. https://doi.org/10.1016/j.phycom.2022.101685.
[18] P. Singla, M. Duhan and S. Saroha, "An ensemble method to forecast 24-h ahead solar irradiance using wavelet decomposition and BiLSTM deep learning network," *Earth Science Informatics*, vol. 15, no. 1, pp. 291–306, 2022.
[19] J. Wang, B. Wei, J. Zhang, X. Yu and P. K. Sharma, "An optimized transaction verification method for trustworthy blockchain-enabled IIoT," *Ad Hoc Networks*, vol. 119, pp.102526, 2021.

[20] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj *et al.,* "Data secure storage mechanism of sensor networks based on blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.
[21] J. Wang, W. Chen, Y. Ren, O. Alfarraj and L. Wang, "Blockchain based data storage mechanism in cyber physical system," *Journal of Internet Technology*, vol. 21, no. 6, pp. 1681–1689, 2020.
[22] J. Y. Zhang, S. Q. Zhong, T. Wang, H. C. Chao and J. Wang, "Blockchain-based systems and applications: A survey," *Journal of Internet Technology*, vol. 21, no. 1, pp. 1–14, 2020.
[23] J. Zhang, S. Zhong, J. Wang, X. Yu and O. Alfarraj, "A storage optimization scheme for blockchain transaction databases," *Computer Systems Science and Engineering*, vol. 36, no. 3, pp. 521–535, 2021.
[24] Z. Xu, W. Liang, K. C. Li, J. Xu and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 149, pp. 29–39, 2021.
[25] D. Zhang, J. Hu, F. Li, X. Ding, A. K. Sangaiah *et al.,* "Small object detection via precise region-based fully convolutional networks," *Computers, Materials and Continua*, vol. 69, no. 2, pp. 1503–1517, 2021.
[26] M. S. Braik, "Chameleon swarm algorithm: A bio-inspired optimizer for solving engineering design problems," *Expert Systems with Applications*, vol. 174, pp. 1–25, 2021.
[27] G. Nguyen, N. Viet, M. Elhoseny, K. Shankar, B. Gupta *et al.,* "Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing*, vol. 153, pp. 150–160, 2021.