[1]Dr D Nagaraju

[2] Dr. Harsh Pratap Singh

[3]Dr. Lokendra SinghSongare

[4]Dr. V V R Maheswara Rao

[5]Amit Gangopadhyay

[6]Dr. M. Sasikumar

[7]Ziaul Haque Choudhury

[8]Dr.Balambigai Subramanian

An Optimized Fraud Identification Framework Using DCNN For Wireless Communication

Journal of Electrical Systems

Abstract: - Convolution Neural Network (Cnn) Is The Powerful Framework To Solve The Lot Of Issues Of Link Detection In Unlabeled Wireless Communication. Last Few Decades Lot Of Fraud Detection Strategies Has Been Projected Bit That All Are Inefficient For Detecting The Frauds. Therefore, The Great Need For Effective And Fast Fraud Detection Scheme With Higher Detection Accuracy. In This Research, Spider Based Convolution Neural Network (Sbcnn) Model To Detect The Frauds In The Wireless Communication. Initially, Create The Wireless Channel To Transmit The Messages From Source To Destination. Here, The Fraudulent Activities Are Detected Based On The Packet Delivery Time Of The Source To Destination Of The Wireless Medium. Moreover, The Proposed System Implementation Is Done In The Matlab Frame Work Additionally; The Obtained Results Are Validated With Prevailing Methods For Evaluating The Efficiency Of The Proposed Sbcnn Approach.

Wireless communication fraud poses a significant threat as unauthorized use of services, compromising the security of cellular networks and infrastructure. With the surge in online services and users, the reliance on wireless communication for high-speed internet applications has grown. Despite the convenience brought by technologies like net banking, credit cards, and online services, financial frauds and unauthorized payments remain substantial risks. The intricate nature of wireless communication, illustrated in Fig. 1, where devices use signals between source and destination nodes, leads to challenges like network interference and loss rate, often exacerbated by fraudulent activities. Numerous techniques, including Artificial Intelligence (AI), hybrid ensemble models, oversampling, and machine learning, have been explored but haven't provided satisfactory solutions. In this study, an optimization-assisted intelligent framework is proposed to maximize communication performance, addressing the limitations of existing approaches. The subsequent sections analyse related research, identify issues with conventional methods, elaborate on the functioning of the proposed framework, discuss results, and conclude with research inferences

Keywords: Wireless Communication, Convolution Neural Network

[1] [1]Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering and Technology, Puttur, Andhra Pradesh, India.

[2]Assistant Professor in Computer Science and Engineering, Medi-Caps University, Indore, Madhya Pradesh-453331.

[3]Assistant professor, Department of Computer Science and engineering, Medicaps University, Indore,

[4]Professor, Dept. of Computer Science and Engineering, Shri Vishnu Engineering College for Women (A), Bhimavaram,

[5]Professor, Department of Electronics and Communication Engineering, Mohan Babu University (Sree Vidyanikethan Engineering College), Tirupati, Andhra Pradesh, India.

[6]Principal, C. Abdul Hakeem College of Engineering &amp; Technology, Melvisharam-632509, Ranipet District, Tamilnadu, India.

[7]Assistant professor, Department of Information technology, School of computing and informatics, Vignan's Foundation, for Science, Technology and Research (Deemed to be University), Guntur, AP, India.

[8]Associate Professor, Department of ECE, Kongu Engineering College, Perundurai, Tamilnadu, India - 638060

[1]raj2dasari@gmail.com, [2]drharshprataps@gmail.com, [3]lokendra.songare@gmail.com, [4]mahesh_vvr@yahoo.com,
[5]amitgangopadhyay@mbu.asia, [6]pmsasi77@gmail.com.[7]ziaulms@gmail.com, [8]sbalambigai@gmail.com

I. INTRODUCTION

Wireless communication frauds can be termed as unauthorized and criminal utilization of wireless communication services like the security of the cellular networks and particular services of the infrastructure intention. In recent days, wireless communication can offer more and more services that are basics in the high speed of internet applications. Moreover, the wireless access throughput lower depends upon the terminal mobility. Recently, the quantity of organizations, online administrations, and web clients has detonated. Lately, everybody has used net banking frameworks for cash moves, charge and Master cards for shopping, and online services [1]. This innovation makes lives simpler with different advantages like shopping without cash, staying away from long lines while covering bills or buying tickets, etc [2, 3]. Nonetheless, monetary cheats and unapproved instalments are causing huge dangers in spite of the positive viewpoints engaged with on the web exchanges. It emphasises the common obstacles and dangers experienced in online financial transactions, highlighting the critical necessity for strong fraud detection measures. The study focus on Deep Convolutional Neural Networks (DCNN) to provide an optimised framework for combating fraud in wireless communication networks. It intends to improve the security and dependability of online transactions in the realm of wireless communication networks by addressing the persistent problems of monetary deception and unauthorised transactions, ultimately contributing to a safer and more secure online financial ecosystem.

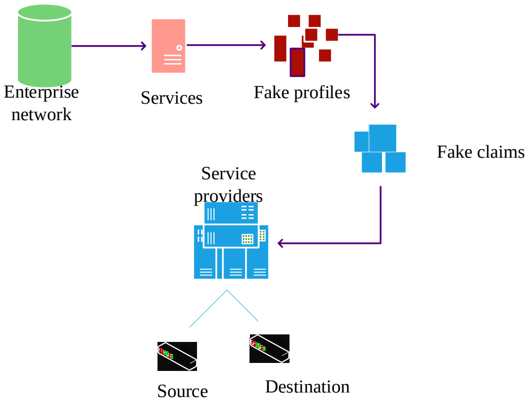

Fig 1. Basics of wireless communication

Most of the wireless devices commonly utilize the signals that are associated with source destination nodes. Moreover, development of wireless communication has various complicated problems such as loss rate, network interference etc., these all problems are occur based on the fraudulent activities. Fundamental structure of the wireless communication is illustrated in fig.1. Previously lot of techniques has developed; those techniques are Artificial Intelligence (AI) [17], hybrid ensample (HE) model [18], oversampling technique [19], machine learning models [20], etc. But still the suitable solutions are not found. Therefore, in the presented study an optimization-assisted intelligent framework was modelled for maximizing the communication performance. Wireless communication is integral to modern life, providing the backbone for a myriad of services, including high-speed internet applications, net banking, and online transactions. However, the pervasive use of wireless technology has given rise to a substantial threat in the form of fraud [18], [19]. Over the last few decades, numerous fraud detection strategies have been proposed, yet they often prove inefficient in identifying and preventing fraudulent activities. This inefficacy underscores the urgent need for an effective and rapid fraud detection scheme, characterized by heightened accuracy. In response to this imperative, recent research introduces a Spider-Based Convolution Neural Network (SbCNN) model tailored specifically for detecting frauds in wireless communication [19]. The methodology involves creating a wireless channel for message transmission from source to destination, with fraudulent activities pinpointed based on the packet delivery time within the wireless medium. Notably, the implementation of this novel approach is executed within the MATLAB framework, and the results obtained undergo thorough validation against prevailing methods, offering a comprehensive evaluation of the proposed SbCNN approach [20]. The escalating risks associated with unauthorized use of wireless services, particularly in the realm of financial transactions, highlight the need for innovative solutions. Despite advancements in Artificial Intelligence (AI) and machine learning models, existing techniques fall short, prompting the exploration of optimization-assisted intelligent frameworks. This study delves into addressing the intricate challenges of wireless communication fraud, analysing related research, identifying shortcomings in conventional methods, and proposing a novel approach to enhance communication performance while mitigating fraudulent activities.

The remaining section of the study is organized as; the most relevant research articles interconnected with present study is analysed in 2nd section, the concerns of the conventional approaches are defined in 3rd section, the functioning of the modelled framework is elaborated in 4th section, the results estimation and validation are deliberated in 5th section, and the research inference is described in 6th section.

II. Related works

A few current studies related to the fraud detection in wireless communication is described below:

In WSNs energy conservation is the most significant phenomena also it is the challenging task because the reliable communication achievement is too hard. Therefore, selvi et al . [21] have introduced the energy-awake routing protocol for securing the information from malicious activities. Moreover, the spatio- temporal elements are used to detect the malicious event over the WSN nodes. Consequently, the developed technique achieves efficient packet transmission ratio and security performance.

Alarifi et al. [22] have proposed the optimized killer based Alex Net CNN module to detect the falls in the WSNs. Here, the various IoT device are connected thorough the different location for finding the dimensionality of the features. Initially, the wearable device datasets are collected and processed the feature extraction process. Besides, Principle Component Analysis (PCA) is used to reduce the feature dimensionality.

Ayshaet al. [23] have proposed the quantum computing based cognitive suspicious detection method to secure the proper responding for all transferred data. Here, the neuro system is connected and deals with lot of issues. Moreover, the neuro system is classified in three categories such as motor neuro system, sensory neuro system and inters neuro system. The proposed technique is secure, reliable and very effective but, this scheme is reduce the fraud rates.

According to the digital world fraudulent patterns can cause the financial institutions. Therefore, the existing approaches are sought to find the ordinary fraudsters. Reem et al. [24] introduced the tree based ML approach has efficiently detect the fake transactions. Here, the real world datasets are adapted and highly applicable for fraud detection process. Moreover, the developed techniques always incorporated with addition tree classifiers and oversampling concepts.

Owolafe et al. [25] have developed the recurrent based long short term memory model to prevent the misclassification rate of the financial sectors. Here, Kaggle datasets used as fraudulent detection. Implementations done by python platform additionally, PCA and Min-Max scalar algorithm is used for normalization. Also, this technique has obtained 80% recall and precision rate for fraud detection.

Problem statements

In a wireless communication, fraud detection is classified in to types such as online fraud and offline frauds. Here, in this paper mainly discuss about the online fraud during the data transmission process. This fraud may be occur in terms of wasted capacity, transmission time and lost income. Moreover, in the online fraud superimposed and subscription are the two important frauds in wireless communication. These challenges in the current studies have encouraged modelling this innovative fraud identification strategy by evaluating their communication level.

III. Methodology

Designed SbCNN Framework

In this article, a novel optimized secure Spider Based Convolution Neural Network (SbCNN) model has developed to protect the data transferring in wireless communication. Primarily, the set of nodes are created in the wireless region that includes unknown nodes and known nodes.

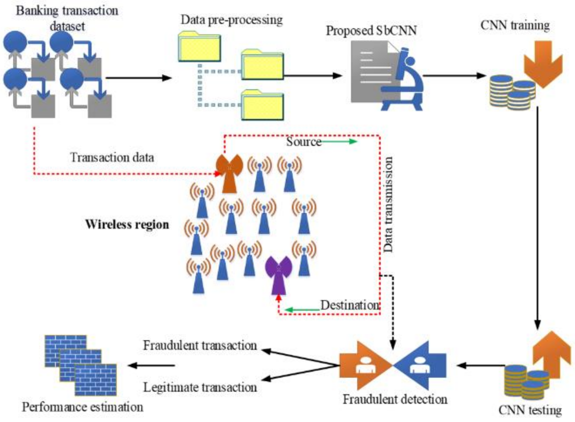

Fig 2. Proposed SbCNN structure

Moreover, the developed SbCNN strategy is tracking the fraudsters and removes that it from the wireless channel for safety communication. Further, in CNNs classification surface, the spider fitness is upgraded. Consequently, the developed model has situates the unknown nodes from the wireless medium. Therefore, the proposed model has achieves better accuracy for detection the frauds from the developed wireless medium. The basic model of proposed structure is demonstrated in fig.2.

The diagram delineates a comprehensive process focused on banking transactions, featuring essential components and a structured workflow designed for efficient fraud detection. At its nucleus lies the central banking transaction process, where transaction data is originated. This data undergoes crucial pre-processing steps to optimize its suitability for subsequent analysis. A noteworthy aspect is the integration of a specialized Convolutional Neural Network (CNN) model, referred to as the Proposed SbCNN, specifically crafted for the purpose of fraud detection. The significance of training and evaluating the Proposed SbCNN model is underscored by the inclusion of a CNN Training Dataset. The trajectory of transaction data involves wireless transmission, suggesting the potential use of wireless communication channels. The process then diverges into the identification of potentially fraudulent transactions through Fraudulent Detection, permitting legitimate transactions to proceed seamlessly. Subsequent stages include a detailed scrutiny of flagged transactions, culminating in a rigorous evaluation of the CNN model's performance through CNN Testing, utilizing a dedicated dataset. This thorough assessment contributes to the comprehensive perspective offered by the Performance Estimation stage, ultimately gauging the system's overall effectiveness in detecting and mitigating fraudulent activities. The diagram's meticulous representation ensures a methodical approach to fraud detection within the domain of banking transactions.

A) Process of developed SbCNN strategy

Initially, the nodes are developed according to the random manner which is created to broadcast the messages. Here, 200 nodes are created over the wireless communication as well as the developed SbCNN is proposed to protect the message during the transmission. In the wireless medium so many nodes are connected which is denoted as, is the known nodes and unknown nodes respectively. Here, we have used DL technique and optimization algorithm both are combined together to developed the novel optimized framework. Besides, the Spider Monkey Optimization (SPO) [26] algorithm is the global inspiration also, one of the met heuristic scheme depends upon the monkey's behaviours.

Consequently, the CNN framework is used the structure includes input layer, convolution layer, pooling layer, dense layer and finally output layer. But, the developed CNN framework is efficiently detect the fraudsters from the developed wireless medium by increasing the layer. Therefore, the proposed CNN model is developed with a depth of 10 layers. Which are, input layer, three convolution layer (Conv1, Conv2, and Conv3respectively), two max pooling layer (Pooling1 and Pooling2 respectively), three dense layer (Dense1, Dense2, and Dense3 respectively) and output layer. Consequently, the softmax activation function is utilized in output layer. Moreover, the current investigation the detection function is used to predict the faulty nodes that are fraudster's node from the developed wireless channel based on the spider fitness function. Initially, the developed nodes are updated in the input layer of the SBCNNthat includes both known node and unknown node. Updating of nodes is represented in eqn. (1),

$$W(n) = (1,2,3,4,\ldots\ldots\ldots\ldots\ldots\ldots\ldots n) \tag{1}$$

Here, nodes are considered and developed the wireless medium then; the message packets are equally allocated in the source node to transmit the message packets. Moreover, the message delivery time is evaluated in eqn.(2),

$$M(d)_t = s_t'(n) - d_t'(n) \tag{2}$$

Where, is denoted as transferring time of each message packets, is expressed as transferring time of source node and is represented as delivered time of the destination node. Additionally, the delivering time of the message packets are fixed based on the proposed optimization fitness function. Here, update the local leader (LL) fitness is classification layer of the CNN module.

$$SM_{LL} = SM_n + \{[u(0,1) * LL_n] + [u(-1,1) * LL_n]\} \tag{3}$$

Where, dimension of each node randomly select the message packets are between [0, 1] and [-1,1]. Here, the spider monkeys components are maintained the packet delivery time and continuously monitor the fraudsters. After updating the local leader fitness objective function is initiated in the same layer. Objective function is performs based on the probability selection process. The evaluated message packets based on the objective function of gradient calculation of spider monkey objective function is given by eqn. (4),

$$F_f = fit_n = \begin{cases} \frac{1}{1+M(d)_t} M(d)_t \geq 0 \\ 1 + M(d)_t M(d)_t \leq 0 \end{cases} \tag{4}$$

Here, using the eqn. (4) the optimal solution is achieved and to acquire optimum results, the fitness operation is reiterated utilizing the above criteria. Based on the delivery time of the each messages the fraud can be detected. Moreover, the maximum delivery time of one packet is five seconds. If the packets are transmitting within five seconds here is no fraud between these sources to destination nodes. But, it can cross that time limit the fraudsters can be hacked the data packets that is shown in algorithm.1.

Algorithm 1. Proposed SbCNN

```
Start
    Initialization (Population_monkeys)        // input layer
    Count=0
        While (count< population_size)do
                for
    If (LL limit > LL count) then
            LL count = 0; LL limit = [1,0]        // randomly select

     else
                                        // classification layer
    End if
    If
            Fraud will occur
    else
            No fraud
    End if
        End for
                End while
Stop
    Output: fraud action detected
```

IV. Result and discussion

Proposed S-CNN replica is very important to examine the function of the system efficiently. Here, the primary concern of the developed study is to plan a unique framework to predict the fraudulent activities in the wireless communications. Moreover, the proposed work is efficiently enhancing the detection process of the developed wireless medium. Additionally, the proposed system implementation is done in the MATLAB framework.

A) case study

Fraudster utilizes at least one Premium Rate Numbers or High Tariff numbers to create an enormous number of missed message packets to particular or different scopes of wireless medium having a place with a wireless administrator. These objective numbers are typically obscure to the supporters that get the drop messages.

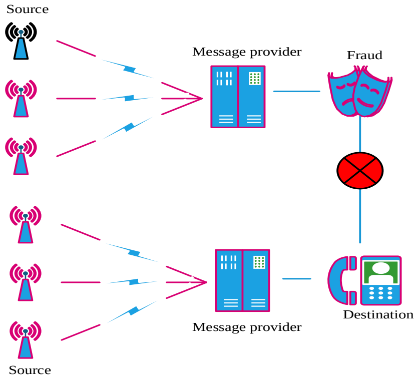

Fig 3. Flow of fraud detection

It is feasible to decide extortion and goes after, for example, fake messages, guest id ridiculing, and administration in eruption, settling on the unapproved decision, dropping the approved messages, unbilled messages, and strategy infringement by dissecting the gathered information in the proposed foundation. Factual examination strategies were acted in the information to perceive message designs that act strange way of behaving with respect to some messages explicit properties. The traits used to characterize client conduct are call type such as public, global, portable, and so forth, message date, message term, message count, and message objective. The illustration outlines a system designed for the detection of fraudulent banking transactions. Initial data, potentially transmitted wirelessly, undergoes pre-processing to ready it for analysis. Subsequently, the processed data is input into a specially crafted convolutional neural network (CNN) model, intricately tailored for the identification of fraudulent transactions. This CNN model scrutinizes the data, flagging transactions deemed suspicious as potentially fraudulent. Flagged transactions likely undergo additional investigation, ensuring a thorough examination of potential fraud cases, while transactions deemed legitimate are permitted to proceed.

Furthermore, the diagram incorporates components dedicated to assessing the CNN model's performance through testing, utilizing a specific dataset. Additionally, there is a component for estimating the overall effectiveness of the entire system. Despite the comprehensive overview, the diagram lacks explicit details regarding the intricacies of the system, such as the methods employed for data pre-processing and the underlying architecture of the CNN model. Clarification of these specifics would provide a more comprehensive understanding of the intricate workings of this complex system aimed at identifying and addressing fraudulent banking transactions.

Here, let us consider fraud behaviours and user behaviours are disseminating based on the message transmission time of the each message, which is tabulated in table.1.

Table 1. Fraud behaviors and user behaviors

Fraud behaviour	**Fraudulent user behaviour**
F-1	A small number of messages with higher duration
F-2	Many messages with lower duration
F-3	Short message and sparse to same reaching point in short duration
F-4	Short message and sparse to same reaching point in long duration
F-5	Many messages and sparse to same reaching point in long duration
F-6	Many messages and sparse to same reaching point in short duration

B) Performance estimation

The modelled approach processed the fraud detection examination results are compared in terms of accuracy, execution time, recall, F-measure, confidential rate, error rate and precision. Besides the comparison of techniques are named as Heterogeneous Ensemble Learning replica (HELR) [27], Sequential Minimal Optimization based Logistic Regression (SMO-LR) [28] model, Transfer Learning (TL) model [29].

5.2.1 Accuracy

The accuracy measure of fraud identification is improving based on the designed SbCNN module. Moreover, the proposed SbCNN technique has achieved high accuracy and it has best performance for detect the unwanted activities like malicious etc. According to the message formats the proposed method is attained 99% of the fraud detection accuracy. Accuracy is calculation using eqn. (5),

$$A = \frac{TP' + TN'}{TP' + TN' + FP' + FN'} \tag{5}$$

Where, TN is True Negative, for true positive, FN is false negative and FP is for false positive. Therefore, validation of accuracy is demonstrated in fig.4 and table.2.

Here, the proposed SbCNN method accuracy measurement is compare with existing techniques such as HELR, SMO-LR and TL. Consequently, the HELR attained an accuracy measurement rate as 79.4%, SMO-LR is getting 84.9% of accuracy measurement and TL attained an accuracy measurement as 67%. Moreover, the proposed strategy achieved accuracy measurement as 99%.

Table.2 Correlative accuracy analysis

Sl.no	**Methodologies**	**Accuracy (%)**
1	HELR	79.4
2	SMO-LR	84.9
3	TL	67
4	Proposed SbCNN	99

5.2.2 Precision

Precision quantifies the exact identification of fraudsters in communication module using the modelled SbCNN framework. In addition, it is computed by dividing the correct positive categorization with the total positive detection. The relative precision analysis is revealed in fig.5.

$$P = \frac{TP'}{TP' + FP'} \tag{6}$$

Table 3. Precision assessment

Sl.no	**Methods**	**Precision (%)**
1	HELR	78
2	SMO-LR	83.5
3	TL	67.9
4	Proposed SbCNN	99

To verify the proficiency of the modelled SbCNN, the precision percent acquired by this algorithm was equated and matched with the current models like HELR, SMO-LR and TL. HELR. These approaches earned precision rate of 78%, 83.5%, and 67.9%, respectively. Subsequently, the modelled SbCNN approach incurred greater precision percent of 99% and the statistical relative assessment is listed in Table 3.

5.2.3 Recall

Recall estimation based on wrong and accurate detection of the fraudsters in wireless communication. In this measurement is efficiently improving the entire system performance. Consequently, validation of recall measure is shown in fig.6 and table.4.

$$R = \frac{TP'}{TP' + FP'} \tag{7}$$

Table 4. Comparison of recall

Sl.no	**Techniques**	**Recall (%)**
1	HELR	88.8
2	SMO-LR	86.2
3	TL	85
4	Proposed SbCNN	99.1

Here, the projected SbCNN procedure recall measure is compare with existing techniques such as HELR, SMO-LR and TL. Moreover, the validation, the HELR attained the recall measure as 88.8%, SMO-LR is getting 86.2% of recall measure and TL attained a recall measure as 85%. Therefore, the proposed strategy achieved recall measure is 99%.

5.2.4 F-measure

F-measure is directly proportional to multiplication of both precision and recall as well as inversely proportional to sum of both precision and recall. Thus, the value of F1-measure is evaluated in eqn. (8),

$$F1\_measure = 2\left(\frac{P \times R}{P + R}\right) \tag{8}$$

Moreover, the estimation of memory utilization and its comparison is shown in table.5.

Table 5. Comparison of F-measure

Sl.no	**Techniques**	**F-measure (%)**
1	HELR	75
2	SMO-LR	85
3	TL	82
4	Proposed SbCNN	97.23

Here, the projected SbCNN procedure F-measure is compare with existing techniques such as HELR, SMO-LR and TL. Moreover, the validation, the HELR attained the F-measure as 75%, SMO-LR is getting 85% of F-measure and TL has attained an F-measure as 82%. Therefore, the proposed strategy achieved F-measure is 91.74%.

5.2.5 Computation time

Computation time is defined as total time taken to complete the entire process based on the fraud detection process. Moreover, the proposed method requires less time to reduce the test case also, identify the bug detection based on the regression testing process. The calculation of execution time is in eqn.(9),

$$C_t = \frac{S_t - E_t}{T_t} \tag{9}$$

Where, is the starting time of the, is the exit time of the s and is represented as total time taken to the entire process. Moreover, the validation and the graphical representation are shown in table.6.

Consequently, the proposed SbCNN technique computation time is compare with existing techniques such as HELR, SMO-LR and TL. Moreover, the validation, the HELR attained the computation time as 65s, SMO-LR is getting 78s of computation time and TL attained computation time as 89s. Moreover, the proposed strategy achieved computation time as 26s.

Table 6. Comparison of computation time

Sl.no	Techniques	Computation time (s)
1	HELR	65
2	SMO-LR	78
3	TL	89
4	Proposed SbCNN	26

Therefore, other recent techniques are attained more time duration but the proposed model attained less time to execute the entire process.

5.2.6 Error rate

To identify the errors the developed SbCNN approach is utilized to perform the software testing process. Comparison values and graphical representation is shown in fig.9 and table.7. Error rate, which is evaluated using the eqn.(10),

$$E_r = 1 - \left(\frac{S_1E_1+S_2E_{2+\dots\dots\dots\dots\dots\dots}+S_nE_m}{mn}\right) + \frac{1}{2m} \tag{10}$$

Where, denoted as wireless nodes based on the performance calculation, m represented as total number of errors, which is recognized in the software programming and n is total number nodes respectively.

Table 7. Comparison of error rate

Sl.no	Techniques	Error rate (%)
1	HELR	0.56
2	SMO-LR	0.046
3	TL	0.09
4	Proposed SbCNN	0.014

Subsequently, the proposed SbCNN procedure error rate is compare with existing techniques such as HELR, SMO-LR and TL. Moreover, the validation, the HELR attained the error rate as0.56%, SMO-LR is getting 0.046% of error rate and TL attained an error rate as 0.09%. Therefore, the proposed strategy achieved error rate is 0.014%.

5.2.7 Confidential rate

Here, the transferred messages are verified with the help of optimization fitness function as well as binary representation. Moreover, these verified data sets are preserved in the long range of computation channel of the information. Consequently, the confidential rate is the measure of high reliability of the protection based information. Comparison values and representation of confidential rate is shown in table.8.

Table 8. Comparison of confidential rate

Sl.no	Techniques	Confidential rate (%)
1	HELR	75
2	SMO-LR	56

3	TL	67
4	Proposed SbCNN	97

HELR attained 75%, SMO-LR achieved 56% and TL attained 67% of confidential rate. Moreover, the comparison figure shows that the proposed method attained better the table compares the confidential rates (%) of different techniques. HELR, SMO-LR, and TL show rates of 75%, 56%, and 67%, respectively. The Proposed SbCNN demonstrates a significantly higher rate of 97%.

V. Conclusion

In this article, a novel optimized fraud detection mechanism has been developed and executed for recognizing and detecting the fraudsters effectively in wireless communication. The introduced fraud detection mechanism utilizes a newly developed module termed SbCNN scheme and prevailing CNN for processing fraud detection. The main aim of this article is to selecting the significant features, which are utilized to improve the classification accuracy of the DL strategy. Besides, the proposed CNN module also support for enhancing the performance in terms of attack detection and execution time. Consequently, the developed method attained 99% of detection accuracy which is compared to other models. Also, the proposed model has attained 0.26s of execution time and 97% of confidential rate. In future, this work will directed to be cloud with the use of intelligent agents for creating the efficient decisions and improving the communication speed of the entire data. The effectiveness of the Spider-Based Convolution Neural Network (SbCNN) model in detecting fraudulent activities within wireless communication is evident. With an outstanding accuracy rate of 99%, the SbCNN model surpasses current methods, displaying superior precision, recall, and F-measure, while also significantly reducing computation time. This approach successfully tackles the challenges posed by wireless communication fraud, providing a reliable and timely solution for the detection of fraudulent activities.

Compliance with Ethical Standards

Conflict of interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Informed Consent

Informed consent does not apply as this was a retrospective review with no identifying patient information.

Funding: Not applicable

Conflicts of interest Statement: Not applicable

Consent to participate: Not applicable

Consent for publication: Not applicable

Availability of data and material:

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Code availability: Not applicable

VI. Reference

[1] You, Xiaohu, et al. "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts." Science China Information Sciences, vol.641, pp.1-74, 2021.

[2] He, Peng, et al. "Developing MXenes from wireless communication to electromagnetic attenuation." Nano-Micro Letters, vol.13.1, pp. 1-34,2021.

[3] Dai, Jun Yan, et al. "Wireless communication based on information met surfaces." IEEE Transactions on Microwave Theory and Techniques, 2021.

[4] You, Changsheng, and Rui Zhang. "Wireless communication aided by intelligent reflecting surface: Active or passive?" IEEE Wireless Communications Letters, vol. 10.12, pp. 2659-2663, 2021.

[5] Furqan, Haji M., et al. "Wireless communication, sensing, and REM: a security perspective." IEEE Open Journal of the Communications Society, vol.2, pp. 287-321, 2021.

[6] Xu, Jianchun, et al. "Metamaterial mechanical antenna for very low frequency wireless communication." Advanced Composites and Hybrid Materials, vol. 4.3, pp. 761-767, 2021.

[7] Lee, Mengyuan, Guanding Yu, and Huaiyu Dai. "Decentralized inference with graph neural networks in wireless communication systems." IEEE Transactions on Mobile Computing, 2021.

[8] Bahramali, Alireza, et al. "Robust adversarial attacks against DNN-based wireless communication systems." Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021.

[9] Ye, Hao, Geoffrey Ye Li, and Biing-Hwang Juang. "Deep learning based end-to-end wireless communication systems without pilots." IEEE Transactions on Cognitive Communications and Networking, vol. 7.3, pp. 702-714, 2021.

[10] Ye, Hao, Geoffrey Ye Li, and Biing-Hwang Juang. "Deep learning based end-to-end wireless communication systems without pilots." IEEE Transactions on Cognitive Communications and Networking, vol. 7.3, pp. 702-714, 2021.

[11] Rodríguez, Demóstenes Z., et al. "Incorporating wireless communication parameters into the E-model algorithm." IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 29, pp. 956-968, 2021.

[12] Zhang, Jun, et al. "Large system achievable rate analysis of RIS-assisted MIMO wireless communication with statistical CSIT." IEEE Transactions on Wireless Communications, vol. 20.9, pp.5572-5585, 2021.

[13] Almohamad, Tarik Adnan, et al. "Dual-determination of modulation types and signal-to-noise ratios using 2D-ASIQH features for next generation of wireless communication systems." IEEE Access 9, pp.25843-25857, 2021.

[14] Almohamad, Tarik Adnan, et al. "Dual-determination of modulation types and signal-to-noise ratios using 2D-ASIQH features for next generation of wireless communication systems." IEEE Access 9, vol. 25843-25857, 2021.

[15] Sengan, Sudhakar, et al. "Security-aware routing on wireless communication for E-health records monitoring using machine learning." International Journal of Reliable and Quality E-Healthcare (IJRQEH), vol. 11.3, pp.1-10, 2022.

[16] Zhao, Ming-Min, et al. "Exploiting amplitude control in intelligent reflecting surface aided wireless communication with imperfect CSI." IEEE Transactions on Communications, vol. 69.6, pp.4216-4231, 2021.

[17] Wang, Jun, et al. "A general 3D space-time-frequency non-stationary THz channel model for 6G ultra-massive MIMO wireless communication systems." IEEE Journal on Selected Areas in Communications, vol. 39.6, pp.1576-1589, 2021.

[18] Hu, Shuyan, et al. "Distributed machine learning for wireless communication networks: Techniques, architectures, and applications." IEEE Communications Surveys & Tutorials, vol. 23.3, pp. 1458-1493, 2021.

[19] Choi, D., & Lee, K. “An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation.” Security and Communication Networks, 2018.

[20] Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S. K., & Kim, J. I. (). Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. Expert Systems with Applications, vol.128, pp. 214-224, 2019.

[21] Chakrabarty, Navoneel, and Sanket Biswas. "Navo Minority Over-sampling Technique (NMOTe): A Consistent Performance Booster on Imbalanced Datasets." Journal of Electronics, vol. 2, no. 02, pp. 96-136, 2020.

[22] Selvi, M., Thangaramya, K., Ganapathy, S. et al. An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks. Wireless PersCommun,vol. 105,pp. 1475–1490 2019. https://doi.org/10.1007/s11277-019-06155-x

[23] Alarifi, Abdulaziz, and AyedAlwadain. "Killer heuristic optimized convolution neural network-based fall detection with wearable IoT sensor devices." Measurement, vol 167, pp. 108258, 2021.

[24] Shabbir, Aysha, et al. "Suspicious transaction detection in banking cyber–physical systems." Computers & Electrical Engineering, vol. 97, pp. 107596,2022.

[25] Own, Reem M., Sameh A. Salem, and Amr E. Mohamed. "TCCFD: An Efficient Tree-based Framework for Credit Card Fraud Detection." 2021 Computer Engineering and Systems (CES). IEEE, 2021.

[26] Owolafe, Otasowie, OluwaseunBosedeOgunrinde, and AderonkeFavour-Bethy Thompson. "A Long Short Term Memory Model for Credit Card Fraud Detection." Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities. Springer, Cham, pp.369-391, 2021.

[27] Xie, Yalong, et al. "A Heterogeneous Ensemble Learning Model Based on Data Distribution for Credit Card Fraud Detection." Wireless Communications and Mobile Computing 2021, 2021.

[28] Hussein, Ameer Saleh, et al. "Credit Card Fraud Detection Using Fuzzy Rough nearest Neighbor and Sequential Minimal Optimization with Logistic Regression." International Journal of Interactive Mobile Technologies, pp. 15.5, 2021.

[29] Li, Sijia, et al. "Transfer learning based attack detection for wireless communication networks." Concurrency and Computation: Practice and Experience, vol. 33.24, pp. e6461, 2021.