International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Optimistic Ensemble Federated Learning Based on Spread Spectral Support Vector Feature Selection with Multi Perceptron Neural Network for Anomaly Detection in Cloud Environment

S. Edwin Raja[1], R. V. V. S. V. Prasad[2] ,Gunaselvi Manohar*[3], V. Krishna Meera[4], G. Sathya[5], S. Gnanasambanthan[6]

Submitted: 08/10/2023 **Revised**: 29/11/2023 **Accepted**: 10/12/2023

Abstract: Wireless Sensor Network (WSN) plays an important role in identifying, monitoring, and securing scalable networks along the Internet of communication all over the world in a cloud environment. Integrating the cloud manages transmission and data control securely to make an effort using energy efficient techniques by various machine learning techniques. The anomalies take part due to malfunction of WSN nodes, leads an inappropriate activity to unsecure the communication. Identifying the anomalies is a big problem based on the feature dimension and behavioural analysis in the communication medium. Most of the prevailing techniques failed to analyze the anomaly properties and behavior response features, leading to increasing feature dimension to produce low-level detection accuracy, precision, and recall rate f1 score, with more false rates and time complexity. To resolve this problem, to propose an Optimistic Ensemble Federated Learning (OEFL) Based on Spread Spectral Support Vector Feature Selection (Ss-SSVFS) with Multi Perceptron Neural Network (MPNN) for anomaly detection in a cloud Environment. Initially, the preprocessing is carried out by min-max normalization techniques to make the affine transformation to reduce the unleased values in the dataset. The Spread spectral support vector feature selection (Ss-SCVFA) is applied to select the features by screening the Support Vector Machine (SVM) class spread with Decision Tree Neural Unit (DTNN) to form feature patterns. The patterns are ranked by ordered class depending on the outlier forming anomaly weight factor to choose the feature limits to reduce the dimension. The feature patterns are trained with a Perceptron Neural Network (MPNN) to identify the behavioral properties into class by reference. The proposed system achieves high performance in identifying the anomalies effectively with a high precision rate, recall rate, and f1-score with a low false rate, and redundant time complexity. Compared to the prevailing techniques, the identification accuracy is at a high level by attaining the accuracy level.

Keywords: *Ensemble federated learning, Support vector, feature selection and classification, neural network, anomaly detection.*

1. Introduction

In the cloud context, WSNs are critical for locating, tracking, and safeguarding scalable networks throughout the global internet of communication. Through cloud integration, transmission and data control are securely managed, enabling various machine learning approaches to be applied in an effort to use energy-efficient strategies. Anomalies resulting from WSN node malfunctions cause inappropriate activities that compromise communication security. The main issue is recognizing the anomalies using behavioral analysis in communication media and feature dimension.

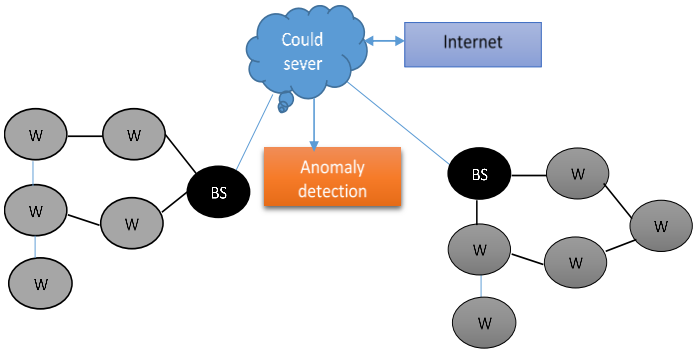

Fig.1 Anomaly detection formation

Discuss the figure. 1 lead to an anomaly detection formation architecture, where w1,w2,w3,w4,w5 are the wireless sensor nodes and, BS is the base station, the BS interface with wireless sensor networks, and BS interfaces

[1]*Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi , Chennai -600062, Tamil Nadu,India.Email:edwinrajas@gmail.com*
[2]*Professor. Department of Information Technology , Swarnandhra College of Engineering & Technology, Narsapur-534280, India. Email : ramayanam.prasad@gmail.com*
[3]*Professor, Department of Electronics and Instrumentation Engineering, Easwari Engineering College (Autonomous), Chennai,India. Email:gunaselvi.m@eec.srmrmp.edu.in* (Corresponding Author)*
[4]*Assistant Professor, Department of Electronics and communication engineering ,Ramco Institute of Technology, Rajapalayam, Tamil Nadu 626117,India.Email: krishnameera@ritrjpm.ac.in*
[5]*Assistant Professor, Department of Electronics and Communication Engineering P.S.R.R College of Engineering, Sivakasi-626140, Tamil Nadu, India. Email: sathya@psrr.edu.in*
[6]*Assistant Professor, Department of Electronics and Communication Engineering, P. S. R Engineering College, Sevalpatti, Sivakasi-626140,Tamil Nadu,India.Email:gnanasambanthan@gmail.com*

with a cloud server, and cloud interface with the Internet. Anomaly detection formation architecture: w1, w2, w3, w4, w5 are wireless sensor nodes, BS is the base station, BS interfaces with wireless sensor networks, BS interfaces with a cloud server, and the cloud interfaces with the Internet. On the other side, WSNs interface with the cloud and internet way through communications.

Provide a Bloom filter-based, fine-grained access control policy that confirms the character of approved clients while safeguarding their data. Moreover, in a re-appropriated climate, edge processing is coordinated into engineering as opposed to distributed computing to diminish reaction time among servers and clients. All in all, we show that the proposed secure AD gets the ID of anomalies in recordings while keeping up with the protection of the connected information. Moreover, our AD system's viability and security are shown by the reenactment results [1]. The highly unequal distribution of train traffic data is no longer a problem for our approach, which dynamically establishes a prediction error threshold to identify anomalies instead of depending on sparse anomaly labels. To assess performance, we conducted in-depth trials in a real metro operational setting. The findings of the experiment show that the suggested strategy is more successful than the current anomaly detection techniques and performs better overall [2].

2. Related Work

Our experiences are condensed into widely used cloud architecture patterns, such as service mesh topologies and load balancing. In complicated settings, autoencoders can identify abnormalities in the load balancer's behavior; LSTMs can infer an element of randomness from the processes they examine, and GNNs can take advantage of the extra topology-related data found in the service meshes [3].

Give a fast SDN-guarded arrangement that straightforwardly works on the focal regulator and utilizes game hypothesis to neutralize DDoS and port filtering attacks. We analyze the three techniques for location. We put our procedure under serious scrutiny utilizing IP traffic information created by the Mininet network emulator related to the Floodlight regulator, and the protection framework that was exhibited functioned admirably for both the identification and moderation tasks [4].

Using carefully chosen detection limits, these outcomes are then utilized to calculate each vehicle's total performance. Without training, MbRE is able to classify those actions with 100% accuracy, 98.5% to 100% accuracy, and 95.4% to 100% accuracy based on frequency, identity, and movement, respectively. To further illustrate IDS's viability in cloud and edge environments, this study also looks into Jetson Nano and Google Collaboratory [5].R(HD-MJPF) min. Additionally, to determine the smoothness at different compression levels, piecewise linear, piecewise nonlinear, and nonlinear predictors are used. An autonomous vehicle carrying out a task in a controlled environment has had our approach examined for lidar min[6].

An exception location module was made to recognize irregularities, for example, multi-objective situations, to improve the strength of our model in certifiable cases. Our methodology conveys striking execution as far as order precision, strength to the commotion, and peculiarity recognition exactness, as shown by trying results utilizing range-Doppler radar estimations and movement catch data sets [7]. The cloud recognizes secondary qualities that are useful for distinguishing the last abnormality by further investigating essential credits and intuitive relationship information. As far as power utilization, location time, and precision, our framework performs better compared to elective techniques, as shown by various preliminaries [8].

It solves the problem of the extremely unequal distribution of data about rail traffic. Performance is assessed by thorough testing in an actual underground operational environment. According to experimental data, the suggested approach is more effective than current anomaly detection techniques, demonstrating its efficacy [9]. A machine learning anomaly detection technique is used in the first component to model the quality of service values and remove any abnormal quality of service records. An effective and efficient metaheuristic algorithm is then used in the second component to identify the closest ideal combination. Information theory supports and grounds service quality through experimental findings derived from real-world data sets. Comparing our strategy to earlier research, such as techniques based on [10], it demonstrates that we can increase the joint scheme's quality of service value by an average of 30.64% at the same or lower cost.

Network traffic information handling is particularly essential with the headway of cloud computing technology (CCT). By and by, the adequacy of current interruption location frameworks (IDS) in analyzing network traffic information for abnormalities needs to be improved. To distinguish network irregularities, this study recommends an original information handling model. Exactness, misleading problem rate (FAR), review, accuracy, and number of Features (NF) can be generally improved by the model simultaneously [11]. Four angles should be adjusted to applications convey locators quietly: accessible limit, detecting necessities, lingering assets, and existing. This system accomplishes higher estimation and discovery exactness than past structures, as indicated by three correlation trials and investigations [12].

Moreover, to bring down reaction times among servers and clients in a rethought climate, edge registering, as opposed

to distributed computing, is coordinated into the design. Eventually, Mostly the Secure Promotion gets the recognizable proof of abnormalities in recordings while keeping up with the classification of the relevant information. Besides, the reenactment results show that our protected Promotion is protected and powerful [13].To achieve location while considering the cloud stage's handling climate, a superior and more adaptable grouping approach is introduced. Two arrangements of tests are run to check proficiency. Indeed, even with adjustments to the cloud stage sending climate, the exploratory discoveries show that the proposed inconsistency recognition technique may significantly build the location exactness rate [14].

A refined incremental and adaptive clustering approach is presented to carry out detection while accounting for the cloud platform's execution environment. To prove efficacy, two different kinds of experiments are run. The suggested anomaly detection method can considerably increase the detection accuracy rate even when the cloud platform execution environment changes, according to experimental data [15].

The ADRL uses anomaly detection techniques to identify aberrant conditions in the system and then initiate steps to increase stability for decision-makers. To oversee the required intensification efforts, two tiers of global and local decision-makers are implemented. With fewer actions and more system stability, ADRL can dramatically improve service quality, as demonstrated by a vast collection of trials for various anomaly problem kinds [16]. Software READ-IoT Minutes: Fire Detection Application Unsold Person Detection Application has been implemented and reviewed. Using simulated data from western multivariate events and anomaly scenarios, general NSL-KDD was conducted [17].

Log data can assist with figuring out which classifier is generally fit. Utilize a help vector machine to prepare various classifiers involving noticed information for different framework conditions. Our location moreover searches for peculiarities inside every window or period, so the highlights contain not just a couple of characteristic execution estimates but, in addition, the entropy and moving normal of the measurements' information inside every window. The viability of our strategy is routinely shown by our exploratory assessment [18]. A full arrangement works in a shut circle without requiring outside observing or statement. By finding out about the use examples of the framework, it creates information about odd conditions and channels and upgrades them naturally. Both the framework load and the cloud supplier's estimating design can be changed utilizing our answer. Utilizing data assembled from a real framework, it was assessed on Microsoft's Sky Blue cloud climate. In ten months, a 85% expense decrease was achieved, as per tests [19].

The overall way of behaving for different types of recognized TVM interruptions is produced by the utilization of an irregular woodland classifier. We utilized a Windows malware information assortment from the College of California and informational collections from the University of New Mexico (UNM) to foster a model and lead intensive investigation. The discoveries obtained are promising and show that VMGuard is material. We balance VMGuard with current innovations and go over their advantages [20]. Since marking an immense information stream starting from heterogeneous sensors is testing and tedious, the proposed approach can be straightforwardly used in genuine circumstances without the requirement for named information. In conclusion, genuine evaluations utilizing a true WSN show that the proposed technique is vigorous and compelling, beating regular profound learning approaches [21].

Several network traffic value sequences can be generated and simulated using the NS2 tool. Next, estimates of the CUSUM and multiclass CUSUM algorithm positivity rates for 2019 were made. Findings indicate that compared to WSNs, the suggested method achieves a greater and more precise detection rate and fewer false positives [22]. Identify conflicts accurately, with optimal performance and low network resource usage, whether in offline or online mode. To find outliers, several academics are currently employing machine learning algorithms [23].

By offering an integrated architecture that blends an Oracle detector, which is a costly and very accurate detector, with an area detector, which is less expensive and less precise, it offers the best possible solution. Using a first-order approximation method, a detection method was devised and optimized. According to the findings of simulations, in order to achieve minimal runtime, it is important to integrate numerous detectors in an ideal pattern [24].

The suggested approach, known as the AD (Anomaly Detection) approach, is made up of specific procedures for the establishment of secure clusters, re-clustering on a regular basis, effective monitoring of cluster membership, and eventual attack detection. Through simulations with a rule-based anomaly detection system, the efficacy of the AD algorithm in intrusion detection and detection is examined [25].

Table.1 Latest Reference and Some Metrics in a few surveys

paper	ML/DL	model	Result	Limitation
M. Ahmadi, et al.,(2010)	ML	AGPCA	achieves a low detection rate	High energy consumption
M. Xie, et al.,(20	ML	kNN-based AD schemes	complexity is reduced	Effective accuracy
X. Miao, et al.,(2019)	ML	one-class support vector machine (OCSVM)	not only show good anomaly detection	High memory consumption
T. -B. Dang et al. (2021)	ML	spatial-temporal correlation	8 % medium accuracy	square prediction error rates
T. Luo, et al.,(2018)	ML	autoencoder neural networks	solve the problem of the anomaly detection medium-level	low false alarm rate
M. Xie, et al.,(2015)	ML	segment-based manner	Reduce communication cost	Low accuracy
A. Abid, et al.,(2016)	ML	outlier measurements	low false alarm rate	Insufficient detection rate
T. Otsuka, et al.,(2015)	ML	autonomous distributed WSN systems	medium-level detection rate	Low false alarms are rare
Y. Xiao, et al., (2017)	ML	SVR-based regression	Low outlier detection accuracy	High error rate
A. Chirayil, et al.,(2019)	ML	statistical-based and cluster-bas	Low accuracy	Low detection rate
Y. -L. Tsou, et al.,(2018)	ML	one-class random forests	detection accuracy medium	Low detection rate
W. Raad, et al.,(2021)	ML	Crowd Anomaly Detection Systems	Low-frequency rate	Low detection rate
T. Sun, et al.,(2012)	ML	A probability-based approximate algorithm	Low-cost reduction	High-cost communication
M. Salvato, et al.,(2015)	ML	An adaptive immune-based anomaly detection algorithm	Large data stream used	Long-term variation in the monitored system

3. Proposed Methodology

The development of anomalies detection through DL model is enrich with feature selection model. Discussed in the figure.2 proposed architecture explains the wireless sensor-based cloud system and detect anomaly detection. Here, WSNs-1, WSNs-2, WSNs-3, and WSNs-4 are wireless sensor network interfaces with Base Station, and BS is connected to a cloud server. Then, preprocess the signals by using the min-max normalization method, select features by using the SS-SCVFA methods, and classify the results by using the MPNN method to classify the results of the detection.

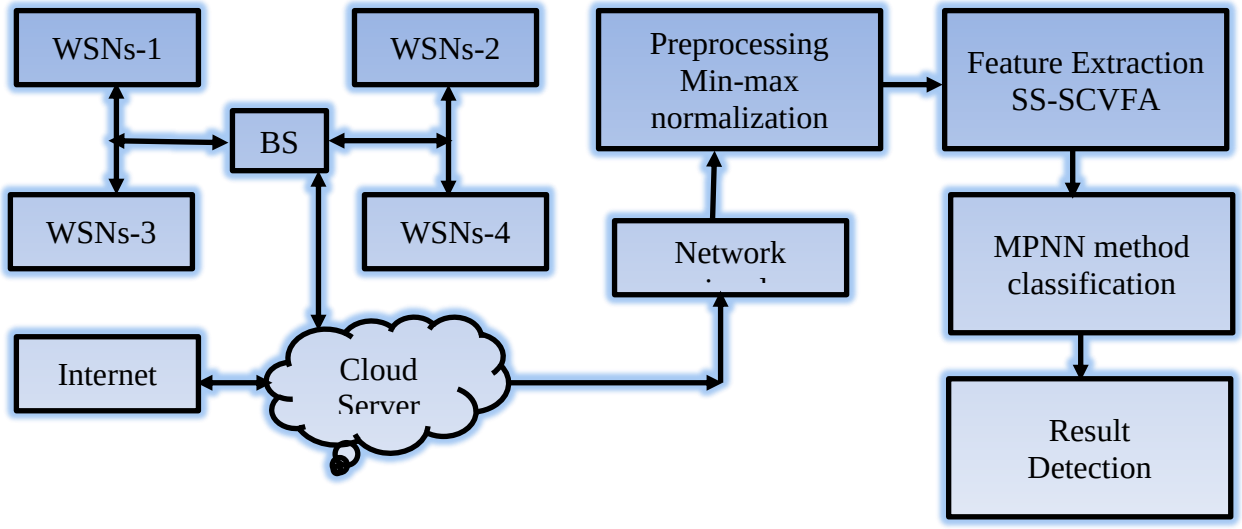

Fig.2 Proposed Architecture

3.1 Network formation of WSN and cloud

Cloud Computing is principally designed and promoted to be data center-centric and efficient interaction with the outside world is an area where improved solutions are being sought.

WSNs are designed to collect data in the real world, yet the the question arises as to what to do with the data when the an organization that collected the data no longer requires it. There are many reasons for the data to be kept, including historical, future research, and re-analysis at some future point in time.

There is a possible linkage between WSN and Cloud Computing and the eventual shift of data into the cloud and over time into the public domain Cloud Computing is principally designed and promoted to be data center-centric and efficient interaction with the outside world is an area where improved solutions are being sought.

WSNs are designed to collect data in the real world, yet, the the question arises as to what to do with the data when the an organisation that collected the data no longer requires it. There are many reasons for the data to be kept, including historical, future research, and re-analysis at some future point in time.

There is a possible linkage between WSN and Cloud Computing and the eventual shift of data into the cloud and over time into the public domainCloud Computing is principally designed and promoted to be data center-centric and efficient interaction with the outside world is an area where improved solutions are being sought.

WSNs are designed to collect data in the real world, yet, the the question arises as to what to do with the data when the an organisation that collected the data no longer requires it. There are many reasons for the data to be kept, including historical, future research, and re-analysis at some future point in time.

There is a possible linkage between WSN and Cloud Computing and the eventual shift of data into the cloud and over time into the public domain

The main goal of cloud computing is to function as a data center, and better solutions are sought in the field of efficient external interfaces. While WSNs are meant to gather real-world data, the question of what to do with the data comes up when the entity collecting it needs it no longer. Data preservation serves numerous purposes, such as future study, historical research, and reanalysis down the road. Cloud computing and wireless sensor networks (WSN) may be related, as may the eventual transfer of data to the cloud and public domain. Another information revolution and an explosion of data have resulted from a large sea of sensors connected to the global network and the communication logs are collected into dataset.

3.2 Preprocessing using min-max normalization

In this technique of data normalization, a linear transformation is performed on the original data to process the dataset. Minimum and maximum value from data is fetched, and each value is replaced according to the following formula.

$$V' = \frac{v - \min(A)}{\max(A) - \min(A)} ((\text{New\_max (A)} - \text{new\_min (A)}) + (\text{new\_min (A)}) \quad (1)$$

Where An is the property information, Min (A) and Maximum (A) are the base and most extreme outright worth of An individually. v' is the net worth of every passage in information. v is the old worth of every passage in information. new_max (A), and new_min (A) are the maximum and minimum worth of the reach separately. Increasing the efficiency of machine learning algorithms: By bringing the input features to a standard scale, normalization can assist in increasing the efficiency of machine learning algorithms. By doing so, you can increase model accuracy and lessen the effect of outliers. Improved handling of outliers: By bringing the data to a similar scale and therefore diminishing the influence of outliers, normalization can lessen their impact. Results can be more easily interpreted when they are normalized because the inputs will all be on the same scale. This is especially true for machine learning models.

3.2 Spread spectral support vector feature selection (Ss-SCVFA)

The Support vector is used to create membership function to create vector space V'based on the support features spectral limits, and incorporate learning biases from statistical learning theory. Finding a computationally efficient method to train well separating hyperplanes in hyperspace is the aim of feature selection using Ss-SCVFA, where best hyperplanes refer to optimizing the feature selection by spectral mean techniques that cope with sizes of the sample.

Let $(x_i, y_i)| < | < N$ is training of N each samples $x_i \in R^d$ each label class $y_i \in \{-1,1\}$

Here d is the dimension of feature space. This amounts to finding w and b so that

$$y_i(w.x_i + b) > 0, i = l \ldots N \quad (2)$$

In this rescale of w and b so that

$$min_{;<j<N}^{\ y_i(w.x_i+b)>0, i=l\ldots N} \quad (3)$$

So the close-set point equation (1) hyperplanes of distance

$$y_i(w.x_i + b) > l$$
(4)

Here find the optim Spread spectral support vector feature selection (Ss-SCVFA) and closed set of distance w

$$\frac{1}{||w||} = \frac{1}{5}||w||^2 + V'$$
(5)

Where minimizing the amount of is under constraints $||w||^2$ is under linear constraints equations (5) achieved with the multipliers. Denote by $\alpha = (\alpha_1 \dots \alpha_N)$ the N non-negative multiplier associated, optimization problem to maximizing to form membership function

$$W(\alpha) = \sum_{i=0}^{N} \alpha_i - \frac{1}{2} \qquad \sum_{i=0}^{N} \alpha_i, \alpha_j, y_i, y_j x_i . x_{j)} + V'$$
(6)

Here $\sum_{i=0}^{N} y_i \alpha_i$ is achieved by the standard quadratic programming Method. We denote the $\alpha^0 = (\alpha^0{}_1 \dots \alpha^0{}_N)$is solution for the maximum problem (6) found. Here, Spread spectral support vector feature selection (Ss-SCVFA) (w^0, b^0), the following expression is

$$w_0 = \sum_{i=0}^{N} \alpha^0 y_i x_{i+V'}$$
(7)

The Ss-SCVFA are points for which $\alpha_i > 0$ satisfies the equation (7) with equality.

From equation (7), the decision plane is to be written as

$$f(x) = [\sum_{i=0}^{N} \alpha^0 y_i x_i + b^0] + V'$$
(8)

The input is mapped. The nonlinear high-dimensional feature has been selected here

Replace x is feature selection
$\Phi(x), taken\ equation(8)$ combined here.

$$W(\alpha) = \sum_{i=0}^{N} \alpha_i - \frac{1}{5} \qquad \text{Ss} - \text{SCVFA} \sum_{i=0}^{N} \alpha_i, \alpha_j, y_i, y_j \Phi x_i . \Phi x_{j+V'}$$
(9)

here k $= \Phi x_i . \Phi x_j is\ feature\ selection\ of\ mapping\ \Phi$. Symmetric

Position kernel K(x,y) it mapped with existing Mercer's theorem

Mapping Φ shows that

$$K(x, y) = \Phi x . \Phi y$$
(10)

$$W(\alpha) = \sum_{i=0}^{N} \alpha_i - \frac{1}{5} \qquad \text{Ss} - \text{SCVFA} \sum_{i=0}^{N} \alpha_i, \alpha_j, y_i, y_j K(x_i, y_i) + V'$$
(11)

Here, the decision function becomes k is the Position kernel mapped

$$f(x) = \text{Ss} - [\sum_{i=0}^{N} \alpha^0 y_i x_i + x_i x + b] + V'$$
(12)

Construction of support vector machines for binary feature selection. A good multiclass approach is required when working with multiple classes, such as in object identification and signals of networks.

The point x is the arguments of $f(x)$ the highest SCVFA steps for feature selection

$$w_{b_{ij}}^{ij} F(x') = \frac{1}{2}(w^{ij} . w^{ij}) + C - \text{SCVFA} \sum_t \xi_{ij}^{ij} + V'$$
(13)

Equation (13) outlines the presumption that every network signal has just one label, meaning that every network signal belongs to just one class. However, since a network signal's contents are not unique, it can be classified into several classes. Multiclass learning can be strengthened and expanded to the feature selection.

3.3 MPNN method of classification

The feature selection sustains the dimensionality and classification is done with Multi Perceptron Neural Network to identify the anomalies. We provide an overview of node G, feature $x_{i,j}$, and edge feature $w_{b_{ij}}^{ij} F(x')$. Adding directed multigraphs to the formalism is an easy task. A multi perceptron phase and a reading phase make up the forward pass. The multi perceptron processing unit phase is specified in terms of functions M_T and vertex update functions Ut, and it occurs throughout T time steps. Hidden states $w_{b_{ij}}^{ij} f(x')$that each node in the graph is updated depending on perceptron m_v^{t+1}according to throughout the data processing phase.

$$m_v^{t+1} = \sum_{w \in N(U)} M_T(h_v^t, h_w^t, e_{vw}) + w_{b_{ij}}^{ij} f(x')$$
(14)

$$h_v^{t+1} = U_t(h_v^t, m_v^{t+1}) + w_{b_{ij}}^{ij} F(x')$$
(15)

Where in the sum, $N(v)$denotes the neighbors of U_t in graph G. The readout phase computes a feature vector for the whole graph using some readout function R according to the final classification steps is

$$y = Rc(h_v^t | V \in G|) + w_{b_{ij}}^{ij} f(x')$$
(16)

The classier retain functionsR_c, vertex update functionsw_b, and readout function R are all learned differentiable functions. Each functions has create marginal weigh classes to identify the anomalies.

4. Result and Discussion

The proposed system discusses the previous method to compare the classification. The existing methods are SecureAD, LSTM, and Incremental-Clustering Anomaly Detection Algorithm (ICADA) compared to the proposed system MPNN, and the best classification of the WSNs and cloud computing networks. The simulating tools are NS2, the network simulator, and uses 100 nodes pointed to calculate the results. The result is based on the high performance of identifying the anomalies effectively with a high precision rate, recall rate, f1-score with a low false rate, and redundant time complexity. Compared to the prevailing techniques, the identification accuracy is at a high level by attaining the accuracy level.

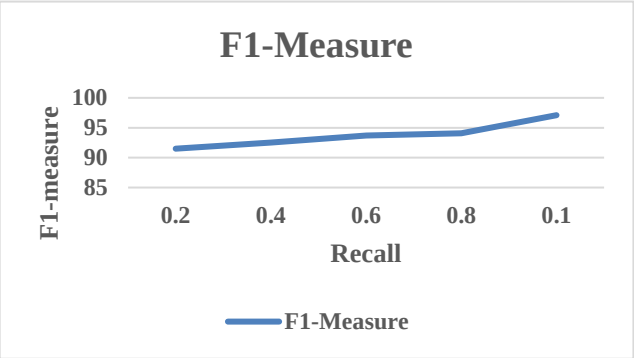

Fig..3 F1- Measure for proposed system

Discuss the figure.2 tell about the F1- Measurement for the proposed system, Recall value is 0.2 and the performance of F1-measure is 91.5%, and Recall value is 0.4 and the performance of F1-measure is 92.5%, and Recall value is 0.6 and the performance of F1-measure is 93.7%, and Recall value is 0.8 and the performance of F1-measure is 94.5%. And Recall value is 0.1 and the performance of F1-measure is 97.1%.

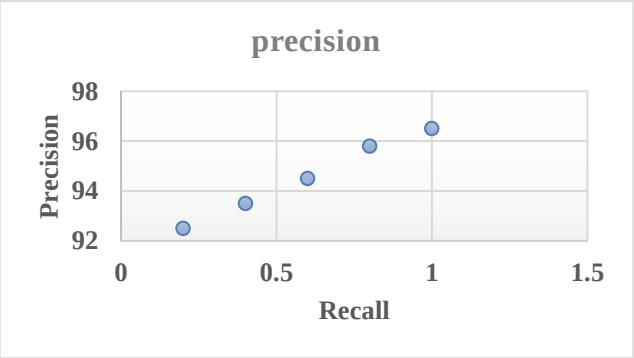

Fig.4. Precision and recall performance

Discuss the figure.2 tell about the for precision and recall performance proposed system, Recall value is 0.2 and the performance of precision is 92.5%, and Recall value is 0.4 and the performance of precision is 93.5%, and Recall value is 0.6 and the performance of precision is 94.5%, and Recall value is 0.8 and the performance of precision is 95.8%. And Recall value is 1.0 and the performance of precision is 96.5%.

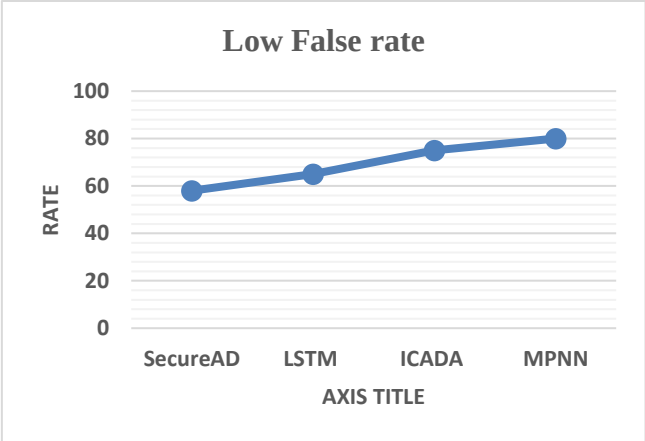

Fig.5. Low false rate

Discuss about the figure.5 is performance of low false rate detection. The performance is secured-AD method is 58% low false rate and, the performance is LSTM method is 65% low false rate, and. the performance is ICADA method is 75% low false rate, and . The performance is MPNN method is 80% low false rate.

Table.2 Classification Performance

Methods	Classification Accuracy (%)
Secured-AD	94%
LSTM	95%
ICADA	96%
MPNN	98%

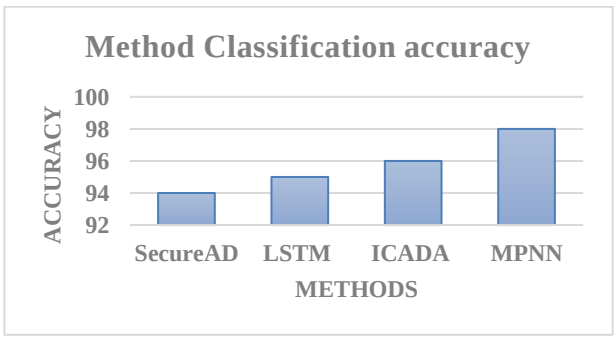

Fig.6. Classification Accuracy

Discuss about the figure.6 and table.2 performance of classification accuracy. The secure-AD performance classification accuracy is 94%, and the LSTM performance of classification accuracy is 95%, and the ICADA performance of classification accuracy is 96%, and MPNN performance of classification accuracy is 98%.

5. Conclusion

In the cloud context, Wireless Senior Networks (WSN) are critical for locating, tracking, and safeguarding scalable networks throughout the global internet of Communication. Through cloud integration, transmission and data control are securely managed, enabling various machine learning approaches to be applied in an effort to use energy-efficient strategies. Anomalies resulting from WSN node malfunctions cause improper behavior that compromises communication security. The main issue is recognizing the anomalies using behavioral analysis in communication media and feature dimension. The system Performance of classification accuracy. The secure-AD performance classification accuracy is 94%, and the LSTM performance of classification accuracy is 95%, and the ICADA performance of classification accuracy is 96%, and MPNN performance of classification accuracy is 98%. The suggested system performs well in terms of accurately identifying anomalies with high recall, precision, and f1-score rates, as well as low false rates and redundant time complexity. By reaching the accuracy level, the identification accuracy is higher than that of the currently used procedures.

References

[1] H. Cheng, X. Liu, H. Wang, Y. Fang, M. Wang and X. Zhao, "SecureAD: A Secure Video Anomaly Detection Framework on Convolutional Neural Network in Edge Computing Environment," in IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 1413-1427, 1 April-June 2022, doi: 10.1109/TCC.2020.2990946.

[2] Y. Wang, X. Du, Z. Lu, Q. Duan and J. Wu, "Improved LSTM-Based Time-Series Anomaly Detection in Rail Transit Operation Environments," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9027-9036, Dec. 2022, doi: 10.1109/TII.2022. 3164087.

[3] R. Lovas, E. Rigó, D. Unyi and B. Gyires-Tóth, "Experiences With Deep Learning Enhanced Steering Mechanisms for Debugging of Fundamental Cloud Services," in IEEE Access, vol. 11, pp. 26403-26418, 2023, doi: 10.1109/ACCESS.2023.3243201.

[4] M. V. O. De Assis, M. P. Novaes, C. B. Zerbini, L. F. Carvalho, T. Abrãao and M. L. Proença, "Fast Defense System Against Attacks in Software Defined Networks," in IEEE Access, vol. 6, pp. 69620-69639, 2018, doi: 10.1109/ACCESS.2018.2878576.

[5] A.Chougule, V. Kohli, V. Chamola and F. R. Yu, "Multibranch Reconstruction Error (MbRE) Intrusion Detection Architecture for Intelligent Edge-Based Policing in Vehicular Ad-Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 11, pp. 13068-13077, Nov. 2023, doi: 10.1109/TITS.2022.3201548.

[6] H. Iqbal, D. Campo, P. Marin-Plaza, L. Marcenaro, D. M. Gómez and C. Regazzoni, "Modeling Perception in Autonomous Vehicles via 3D Convolutional Representations on LiDAR," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 14608-14619, Sept. 2022, doi: 10.1109/TITS.2021.3130974.

[7] M. Li, T. Chen and H. Du, "Human Behavior Recognition Using Range-Velocity-Time Points," in IEEE Access, vol. 8, pp. 37914-37925, 2020, doi: 10.1109/ACCESS.2020.2975676.

[8] J. Tang, L. Wei, W. Liu, Z. Zhou and J. Gu, "Correlation Anomaly Detection With Multiple Primary Attributes in Collaborative Device–Edge–Cloud Network," in IEEE Internet of Things Journal, vol. 10, no. 6, pp. 4922-4936, 15 March15, 2023, doi: 10.1109/JIOT.2022.3221086.

[9] Y. Wang, X. Du, Z. Lu, Q. Duan and J. Wu, "Improved LSTM-Based Time-Series Anomaly Detection in Rail Transit Operation Environments," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9027-9036, Dec. 2022, doi: 10.1109/TII.2022. 3164087.

[10] M. Razian, M. Fathian, H. Wu, A. Akbari and R. Buyya, "SAIoT: Scalable Anomaly-Aware Services Composition in CloudIoT Environments," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3665-3677, 1 March1, 2021, doi: 10.1109/JIOT.2020.3023938.

[11] Z. Zhang, J. Wen, J. Zhang, X. Cai and L. Xie, "A Many Objective-Based Feature Selection Model for Anomaly Detection in Cloud Environment," in IEEE Access, vol. 8, pp. 60218-60231, 2020, doi: 10.1109/ACCESS.2020.2981373.

[12] J. Liu, H. Zhang and G. Xu, "An Anomaly Detector Deployment Awareness Detection Framework Based on Multi-Dimensional Resources Balancing in Cloud Platform," in IEEE Access, vol. 6, pp. 44927-44933, 2018, doi: 10.1109/ACCESS.2018.2865114.

[13] H. Cheng, X. Liu, H. Wang, Y. Fang, M. Wang and X. Zhao, "SecureAD: A Secure Video Anomaly Detection Framework on Convolutional Neural Network in Edge Computing Environment," in IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 1413-1427, 1 April-June 2022, doi: 10.1109/TCC.2020.2990946.

[14] H. Zhang, J. Liu and T. Wu, "Adaptive and Incremental-Clustering Anomaly Detection

Algorithm for VMs Under Cloud Platform Runtime Environment," in IEEE Access, vol. 6, pp. 76984-76992, 2018, doi: 10.1109/ACCESS.2018.2884508.

[15] H. Zhang, J. Liu and T. Wu, "Adaptive and Incremental-Clustering Anomaly Detection Algorithm for VMs Under Cloud Platform Runtime Environment," in IEEE Access, vol. 6, pp. 76984-76992, 2018, doi: 10.1109/ACCESS.2018.2884508.

[16] S. Kardani-Moghaddam, R. Buyya and K. Ramamohanarao, "ADRL: A Hybrid Anomaly-Aware Deep Reinforcement Learning-Based Resource Scaling in Clouds," in IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 3, pp. 514-526, 1 March 2021, doi: 10.1109/TPDS.2020.3025914.

[17] A.Yahyaoui, T. Abdellatif, S. Yangui and R. Attia, "READ-IoT: Reliable Event and Anomaly Detection Framework for the Internet of Things," in IEEE Access, vol. 9, pp. 24168-24186, 2021, doi: 10.1109/ACCESS.2021.3056149.

[18] D. Sun, M. Fu, L. Zhu, G. Li and Q. Lu, "Non-Intrusive Anomaly Detection With Streaming Performance Metrics and Logs for DevOps in Public Clouds: A Case Study in AWS," in IEEE Transactions on Emerging Topics in Computing, vol. 4, no. 2, pp. 278-289, April-June 2016, doi: 10.1109/TETC.2016.2520883.

[19] P. Osypanka and P. Nawrocki, "Resource Usage Cost Optimization in Cloud Computing Using Machine Learning," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 2079-2089, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3015769.

[20] P. Mishra, V. Varadharajan, E. S. Pilli and U. Tupakula, "VMGuard: A VMI-Based Security Architecture for Intrusion Detection in Cloud Environment," in IEEE Transactions on Cloud Computing, vol. 8, no. 3, pp. 957-971, 1 July-Sept. 2020, doi: 10.1109/TCC.2018.2829202.

[21] M. Matar, T. Xia, K. Huguenard, D. Huston and S. Wshah, "Multi-Head Attention based Bi-LSTM for Anomaly Detection in Multivariate Time-Series of WSN," 2023 IEEE 5th International Conference on Artificial Intelligence Circuits and Systems (AICAS), Hangzhou, China, 2023, pp. 1-5, doi: 10.1109/AICAS57966.2023. 10168670.

[22] Y. Bo and W. Xueyuan, "Research on Multiclass CUSUM Algorithm for Anomaly Detection of WSN," 2010 International Conference on Intelligent Computation Technology and Automation, Changsha, China, 2010, pp. 40-44, doi: 10.1109/ICICTA.2010.522.

[23] G. Li, Y. Liu and Y. Wang, "Analysis of the Count-Min Sketch Based Anomaly Detection Scheme in WSN," 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, China, 2014, pp. 961-966, doi: 10.1109/TrustCom.2014.127.

[24] R. K. Dwivedi, A. K. Rai and R. Kumar, "A Study on Machine Learning Based Anomaly Detection Approaches in Wireless Sensor Network," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 194-199, doi: 10.1109/Confluence47617.2020.9058311.

[25] M. A. Amrizal, L. Guillen and T. Suganuma, "Toward an Optimal Anomaly Detection Pattern in Wireless Sensor Networks," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 2019, pp. 912-913, doi: 10.1109/COMPSAC.2019.00137.

[26] A. Balakrishnan and P. C. Rino, "A Novel Anomaly Detection Algorithm for WSN," 2015 Fifth International Conference on Advances in Computing and Communications (ICACC), Kochi, India, 2015, pp. 118-121, doi: 10.1109/ICACC.2015.29.

[27] M. Salvato, S. De Vito, S. Guerra, A. Buonanno, G. Fattoruso and G. Di Francia, "An adaptive immune based anomaly detection algorithm for smart WSN deployments," 2015 XVIII AISEM Annual Conference, Trento, Italy, 2015, pp. 1-5, doi: 10.1109/AISEM.2015.7066840.

[28] T. Sun, W. Chen, Y. Liu and H. Sun, "A probability-based approximate algorithm for anomaly detection in WSN," 2012 World Congress on Information and Communication Technologies, Trivandrum, India, 2012, pp. 1109-1114, doi: 10.1109/WICT.2012.6409241.

[29] W. Raad, A. Hussein, M. Mohandes, B. Liu and A. Al-Shaikhi, "Crowd Anomaly Detection Systems Using RFID and WSN Review," 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Alkhobar, Saudi Arabia, 2021, pp. 1-5, doi: 10.1109/ISAECT53699.2021.9668517.

[30] Y. -L. Tsou, H. -M. Chu, C. Li and S. -W. Yang, "Robust Distributed Anomaly Detection Using Optimal Weighted One-Class Random Forests," 2018 IEEE International Conference on Data Mining (ICDM), Singapore, 2018, pp. 1272-1277, doi: 10.1109/ICDM.2018.00171.A

[31] A. Chirayil, R. Maharjan and C. Wu, "Survey on Anomaly Detection in Wireless Sensor Networks

(WSNs)," 2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Toyama, Japan, 2019, pp. 150-157, doi: 10.1109/SNPD.2019.8935827.

[32] Z. Xiao, C. Liu and C. Chen, "An Anomaly Detection Scheme Based on Machine Learning for WSN," 2009 First International Conference on Information Science and Engineering, Nanjing, China, 2009, pp. 3959-3962, doi: 10.1109/ICISE.2009.235.

[33] A. Abid, A. Kachouri, A. Ben Fradj Guiloufi, A. Mahfoudhi, N. Nasri and M. Abid, "Centralized KNN anomaly detector for WSN," 2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15), Mahdia, Tunisia, 2015, pp. 1-4, doi: 10.1109/SSD.2015.7348091.

[34] T. Otsuka, T. Inamoto, Y. Torii and T. Ito, "A High-Speed Sensor Resources Allocation Method for Distributed WSN," 2015 IEEE 8th International Conference on Service-Oriented Computing and Applications (SOCA), Rome, Italy, 2015, pp. 242-246, doi: 10.1109/SOCA.2015.34.

[35] M. Xie, J. Hu and S. Guo, "Segment-Based Anomaly Detection with Approximated Sample Covariance Matrix in Wireless Sensor Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, pp. 574-583, Feb. 2015, doi: 10.1109/TPDS.2014.2308198.

[36] T. Luo and S. G. Nagarajan, "Distributed Anomaly Detection Using Autoencoder Neural Networks in WSN for IoT," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-6, doi: 10.1109/ICC.2018.8422402.

[37] T. -B. Dang, D. -T. Le, T. -D. Nguyen, M. Kim and H. Choo, "Monotone Split and Conquer for Anomaly Detection in IoT Sensory Data," in IEEE Internet of Things Journal, vol. 8, no. 20, pp. 15468-15485, 15 Oct.15, 2021, doi: 10.1109/JIOT.2021.3073705.

[38] X. Miao, Y. Liu, H. Zhao and C. Li, "Distributed Online One-Class Support Vector Machine for Anomaly Detection Over Networks," in IEEE Transactions on Cybernetics, vol. 49, no. 4, pp. 1475-1488, April 2019, doi: 10.1109/TCYB.2018.2804940.

[39] M. Xie, J. Hu, S. Han and H. -H. Chen, "Scalable Hypergrid k-NN-Based Online Anomaly Detection in Wireless Sensor Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 8, pp. 1661-1670, Aug. 2013, doi: 10.1109/TPDS.2012.261.

[40] M. Ahmadi Livani and M. Abadi, "An energy-efficient anomaly detection approach for wireless sensor networks," 2010 5th International Symposium on Telecommunications, Tehran, Iran, 2010, pp. 243-248, doi: 10.1109/ISTEL.2010.5734031.