COPY RIGHT

IJIEMR Transactions, online available on 26th Dec 2021. Link

:http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=Issue 12

10.48047/IJIEMR/V10/ISSUE 12/36

Paper Authors N.Sangeethapriya1, L.Bharathi2, S.Jagan Mohan Rao3, A.N.L.Harisha 4

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A ElectronicBar Code

WIRELESS SENSOR NETWORK TO IMPROVE SECURITY PERFORMANCE AND PACKET DELIVERY RATIO USING FCL-BOOST BASED CLASSIFICATION METHOD

N.Sangeethapriya[1], L.Bharathi[2], S.Jagan Mohan Rao[3], A.N.L.Harisha [4]

[1,2,3,4]**Department of ECE, Ramachandra College of Engineering, Eluru, Andra Pradesh, India.**

priyarathi2004@gmail.com, lbharathioptical@gmail.com

Abstract:

Wireless Sensor Networks are constantly monitoring such changes over a rapidly changing environment. This dynamic behavior is triggered by external factors or initiated by the system designer. In such situations, adapting sensor networks generally use machine learning techniques to reduce unnecessary redesign. Learn machines also trigger multiple practical solutions to maximize the utilization of resources and extend network life.This FCL-boost based classification algorithm is used to create a detailed authorization. The first classification level (FCL- Boost) according to the method, and different classifications to choose the name of the classification level or with the same type of FCL.The next step is to create a combined classification. FCL-Boost.L1 (Level 1) is to apply the user request level1 and FCL-Boost.L2 (Level 2) are being support under the route energy same or different classifications to support side. The According to the obtained results, the data is safe and reliable and written statements.K-Nearest Neighbor (KNN) has a lower accuracy rate, and Random Forest and Support Vector Machine (SVM) compared the previous methods slightly compared to the literature's number of protocols. Because of the many steps that the Foremost Classification Level FCL-boost algorithm process will be faster. Because of these advantages is the means of success.

Keywords: SVM, RF, KNN, FCL-Boost,Wireless Sensor Network, security, MLT.

1. INTRODUCTION

This study began with a useful question on improving wireless sensor networks' network life cycle using reinforcement learning enhanced power with sensor terminals. TheFCL-Boost algorithms to improve energy efficiency, problem-solving has been the main area of study in the various literature that has been discussed over the past few decades. Therefore, it is expected that the sensor nodes will improve and enable sleep and wake-up mechanisms to exploit their energy to improve the networks' life cycle.

In most cases, due to the multi-hop communication, it is a heavy load to the nearest base station as the senior center because they are centered in the middle of the base station and stay away and arrange the information sent to the remote sensor base station.The problem in this scenario is the problem area where the Sensor Node (SN)sends its information, such as different hub information near the center of the event tank. Of these contributions to the total pollution reduction worn by the remote sensor at the exhibition. Wireless Sensor Network Development and Problem Areas, Generally speaking, the head of the universal tank is required for each beam, information collection, and information transmission can't afford to take a long time to cross a long lifespan and uses little middle. Therefore, suggest learning support and data weight calculations.
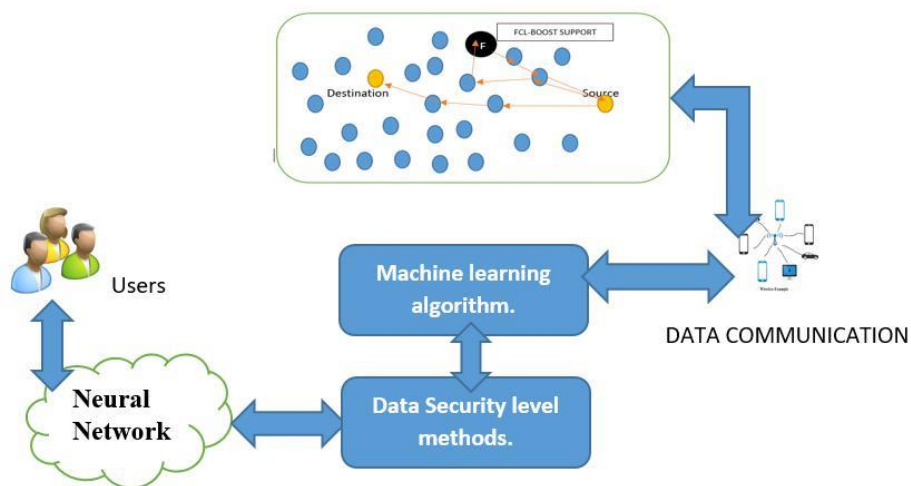
Figure 1: Architecture of WSN communication user to server [1]

A WSN sensor is a self-organized network of nodes that show the figure 1 communicate with a group of nodes that send a special node activator into their environment, communicate approximately spontaneously through the unconnected wire, fixed or scattered over a specific geographic area, and a set point of data, where the sensor node company is present in a field. The transfer of collected data done from time to time or In light of the application running's occasion-based nature. One end of the container, WSN, and end-client organize (e.g., a neighborhood or the Internet) is an interface between the extension between and is more than one system. The client to determine the sort of information gathered, for instance, through a water tank in the system, can be mentioned to send to another hub.For illustrations, a wireless sensor network type's one basic program engineering. The sensor center is located at the end of the plot area, and area Duty regarding acquiring the information gathered through the sensor field. Regularly, the tank in the data venture that has been gathered and composed in such an Away, only relevant data is sent to the customer. It can receive orders and run from its internal system (customer). The information collected is processed and broken down by the customer.

A wireless sensor is a small electronic device that can measure body level (such as temperature, light, pressure, etc.) and transmit it directly or through other sensor nodes to a set center that acts as a router. Given the advancements made in microelectronics, wireless transfer technology and software make smaller scale sensors that can create a few cubic millimeters. It can work the module in the system at a sensible cost. The sensor hub incorporates four fundamental units of two altered hand-held acquiring implies. Sensor and a Simple Computerized Converter (SCC): These have two subunits. The sensor transforms digital measurements of environmental factors, and Analog Transfer Collects the information. It consists of two units: the data storage unit that allows other sensors to be used for collection tasks, and the processor is responsible for processing data and control procedures.The unit corresponds,its capacity is data transfer and compilation. It has a transmitter/receiver pair. It is the internal communication system

that, in this case, allows this problem RW(Radio waves). In any case, solar panel power units' continuous testing attempts to answer extended sensor life. Mobilization. Alternatively, this task can be used to move the process. Location detection system to complete the hub. Alternatively, this application or possibly provides the required terrain data through guidance. This chapter is discussed above the wireless sensor data security and processing explains this topic is covered networks.

1.1 Machine learning algorithm.

What can be applied to calculate under the jurisdiction of Artificial Intelligence (AI), in the past, based on the guidelines on the use of naming, it is expected that in the future new information is realized. Known starting from the investigation of the prepared data set and to learn to calculate, create a derived ability to make predictions about the output self-esteem. The framework can give the focus to any new contributions after adequate preparation. Calculation of learning can also adjust the appropriate model, compare the rate of correct the model.

Interestingly, if they want to use it to prepare the data, calculating one of the groupings and the solo AI name is not available. The concentrated visual framework will learn how it is possible to induce the ability to portray the hidden structure of the non-labeled information. A framework does not make sense of the accuracy rate's return; it examines the information and pulls out the non-labeling of information from a data set that can attract derived from the hidden structure.

1.2 Security level of methods.

By radio communication of the mobile remote system, the simple screen can attack the attacker without being associated with the actual system. Attack, will pass through the access systems in the range of remote systems that are not protected. Some experts recognize any channel and the remote system interface card design security coordination degree.

1.3 Wireless Sensor Network Behavior

The goal is to change the universal arrival operation setting classification to calculate the remote sensor system's insight to show a sharp action. The quality of the remote sensor system provides several difficulties. For example, the number of sensor hubs, thick tissue to change the geographical structure is enormous, including power, computing, storage, and the corresponding ability is a specific constraint asset. Rules of all applications, vigor effective needed to run on a remote sensor system, universal but is violent, "tuned" to change conditions and settings. Without the application extension, action-filled with disposed insight in the middle between the other people and performance.

2. RELATED WORKS

The Personal Computer systems and the widespread use of online electronic information and safety appeals have called for a solid framework for [1] cross-discovery.. Muss rappels traitor de aboard Human issues, Society General de la combination affiliate unit, etc. proposes taxonomies [2] methods. Elfin, rational Les attends equal value, etc., ready to reduce particular la [3][4] difficult single generalizer fewer results. This technology's principle idea is to use the Relative Entropy (RE) principle to evaluate organized traffic to be distorted and identify the system's characteristics. Depending on the model, is also planned. Relative entropy is to expand increment the location rate, counterfeit the [5] alarm rate, which is more accurate and can reduce the inherent logical discrepancy between the most estimated errors in practice. Lincoln Laboratories Assessment Information Index shows that identification results can come at high levels and speeds due to the low false alarm rate strategy. Assault location innovation[6] depends on latent observing of traffic to implement a detective system based on hidden, active measurement, real-time detection without intrusion detection, and as much classification as possible for attacks. The contribution is calculated using the probability of responding to a request measured from the delay time series that relies on the original entropy function/echo. However, this method [7] evaluation showed a substantial number

of false positives. Then used to substantially reduce the probability of the number of false alarms using Hausdorff's distance enrichment taking place in the time series.

Using data processing [8] technologies such as nerve blur and radial base Support Vector Machines (SVMs) for IDs to help obtain a new method of high detection rate. The proposed technique [9] has four main steps: First, the K-means set is used to create different training subsets. Then, according to the training subcommittee obtained, different nerve ambiguity models were trained. Following that, a vector of SVM classification is generated, and finally, the radius is made to determine whether SVM classification infiltration has occurred or not. To illustrate this new method's compatibility and efficiency, the results of the experimental file dataset were demonstrated. Experimental [10] results show that a new method is a really good blood pressure neurological network, multi-class SVM, and other well-known methods, such as the Columbia model based on the decision trees' sensitivity and accuracy, especially the result.

Hypothesis [11] [12] from straightforward programming duplication provides a fascinating understanding of the question and enables us to determine O | E | Registration | E | the closest answer to time and self-esteem is to double the K-focal best value. The regulation in each area of information is implemented due [13, 21] to the Dumpster rule of combinations of these possible components. As a result, the first two datasets' order showed surprisingly high accuracy while other well-known strategies were not considered rigorous. The third set of data groups is non-digital and difficult. Still, completed by giving the structure and quality capabilities a great result to get the [14] combination for a carefully structured and accurate characterization. In all cases, the DS sources strategy gives almost the same performance as other well-known calculations. Still, the quality of production accuracy gives cost processing and expansion of new features. In general, the [15, 22] results suggest that the gives a large-scale capacity structure and size to mechanize the compatibility of calculating the structure of a reasonable [16] construction system and complex order issues. In this way, the success of

distinguishing interference under these conditions, unfortunately, requires a significant degree of accuracy and productivity with a preempted goal. Many interfering [17, 23] detection patterns in writing do not recommend continuous responses to manage the barriers mentioned above. This experiment and Denial of Service DoS encourages us to propose a lightweight interference recognition framework for attack locations.

Even an isolated [18] occasional source (for example, transportation arrangement) thinks about it alone when facing big data challenges. Attempts to use more diverse information sources represent a challenge that deserves a lot of attention with big data. Innovative infiltration detection of bulk [19] data can lead to the realization of these large diversified data challenges. This articleinvestigates the issue of diversified information, especially to the degree of big difference. This report is a precursor to an infiltration detection system.
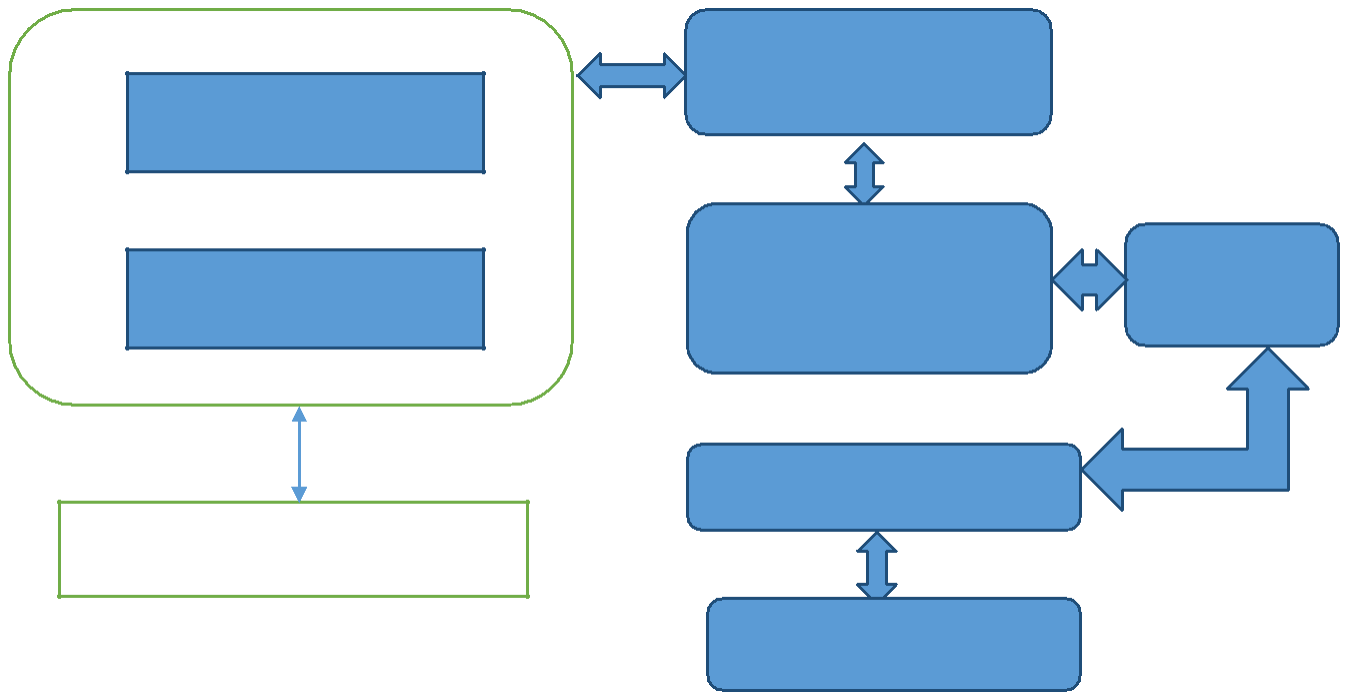
Details of possible attacks and [20, 21, 22,23] reactions were detected in the water at the beginning of a conversation about various components. In the long run, it will hint at the new concept of IPS (Intrusion Prevention System) and possible dialog ways to improve the existing structure.
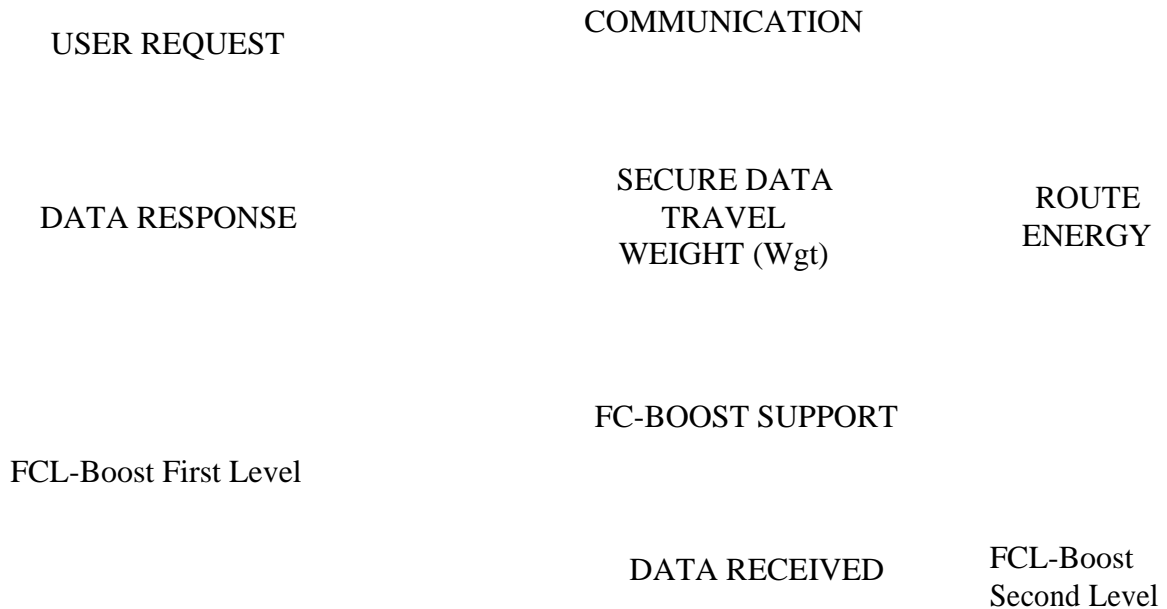
In this option, up to two unique techniques, particularly FCLBoost.L1 and be FCLBoost.L2, F-score calculation for judgment in the light of implementation, highlighting grown and ready to collect the classification can be upgraded. . 1. It is done. (This is a makeover whose process has at least three distinct classifications; finally, the classification of the three distinct classifications combine theater company. Along these lines, it is discharged from the production process to ensure that information can be meaningless. Equipment classification Yes, the project took a little later redesigned to be considered. Are a mixture of three types of unique types of collections in the long (The use rate of e-orphan classification is reduced by cost. The only applicable feature is the use of F-score recovery, including judgment calculations.

3. MATERIALS AND METHODS:

The proposed system to overcome the above problems efficiently. Recent detection minimizes show the figure 2 first discriminatory algorithm (FCL-Boost) algorithm using detection. It is adding data to a user request that the L1 level does not have a one-time data response. The second level of information to users on a server in the data travels safely. The stream performed the activity in Figure 2. Right off the bat, the records to be utilized in the examination were gathered. The highlights were chosen with the F-Class include choice calculation. At last, the information is arranged with various classifiers, and their exhibitions are determined. When these assignments are performed, the hardware has delegated a classification and presentation that is resolved at all levels and positions.


WIRELESS SENSOR NETWORKS   DATA

USER REQUEST

COMMUNICATION

DATA RESPONSE

SECURE DATA
TRAVEL
WEIGHT (Wgt)

ROUTE
ENERGY

FC-BOOST SUPPORT

FCL-Boost First Level

DATA RECEIVED

FCL-Boost
Second Level

Figure 2:The proposed system's architecture to the data security and Route energymethod using the FCL-boost algorithm.

3.1 Collection of data from the classifier

Outfit by engaging each classifier is a classifier to provide a safer, more stable frame made meter the classification framework is N 'may be single or double. Although characterized as indicated by the vector component, each classification yield creates self-esteem for each vector element 1. (Delivery yield respected figured out, the group classification yield resolved by votes of Opportunity closed on the classification of the even number is selected, the normal classification of the estimated adjustment, and the choice to solve the troupe classification. (A process it applies to all components of the carrier.

Expanded the range close to zero, the system image and nearest neighbor classifier start. (Self-esteem when you're far away from 0, multiple vectors, each with different information, the classified into consideration gives birth order. The extension range is limited to 0.01 in advance. After examination, the nature of the outskirt and usage of the

best execution framework has been resolved. Supported vector machines have better AI calculations. The Supportvector machines try to isolate a straight line and a dotted line from a set of data. The basic error information in the (Support Vector Machine) SVM calculation and an option must be recognized. Solution analysis is used in the Gaussian or Extended Conditional Work Random Forest (RF) area (RF). (The power box is set to 100 targets somewhere in the control box 1 is limited to the range and can be expected to be completed.
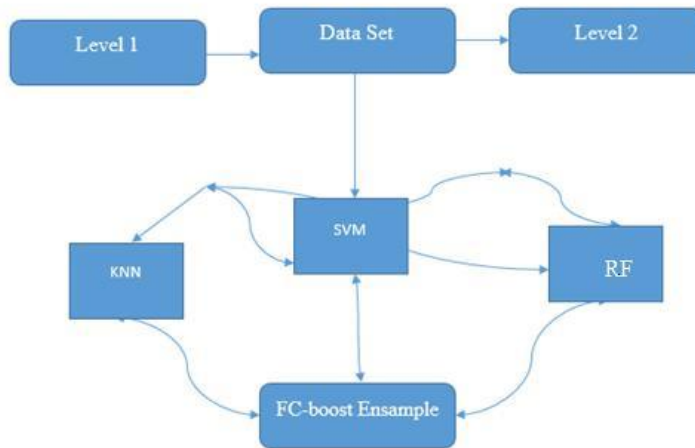
Figure3: Data flow of FCL-boost ensample algorithm

3.2. Classifier-Based Ensemble Classifier: FCLBoost.L1.

Method Simulation Steps Figure 3. Thus classified in the classifier (KNN) is shown in detail in this first set of data (a). The second step is to repeat the first edition featuring

and selected (KNN is categorized in a similar classification). In a third step, perform the first and second component determination repeating the classification (KNN) in the same category. Three different activities were divided in the US, but the same classification (KNN) was found. These three outcomes are consolidated to frame a k-closest neighbor gathering. Rehash a similar procedure Random ForestRF and SVM. Finally, Q Neighbor Set, RF [Random Forest] Group, and SVM Group combine into a single, integrated classification.

3.3. Functional integrated classifier: FCLBoost.L2.

The steps of this method are shown in Figure 3. Therefore, the data set (a) is first classified according to each classifier (adjacent ones, RF, and support vector machine k). These three categories are integrated type 1. The second aspect is integrated to get, the first aspect is selected, and the Handling is done in the initial step. In a third step, the first and second characteristic choice advance is executed together, at that point rehashes the primary formula. Order for bunch 1, 2, and 3 are combined to form a comprehensive recognition.

3.4. Route Energy Path

Collaboration identifies the overall vitality of the connected hub and has the best vitality process of photographing a priori information on the hub's surface position. The S- surface position hub will be occupied in the corresponding position to the closing of the opportunity. It updates the underwater neighbors to adopt the center of the then to the surface position of the replacement to avoid loss of information. From that point on, the hub's water will push the particular data to the storage hub and take another surface position of the hub. Finally, in advance of the hub to the surface position data, information is most transmitted in proficiency mode vitality most minimal jump contemplated the least limit of the separation process. In the end, information is loaded to pick up it is sent the shell from the hub.Besides, a once-over having information log is kept up by load center point, containing data about which data gets sent from which

explicit center point and at what repeat of time term the information was gotten, going before taking care of the proportionate the shell. The particular shell that goes about as pad stores the data advanced through the stack center point. Additionally, they are using divided data strong trade shows that achieve a reliable imperativeness amazing transmission of data in submerged sensor sorts out.
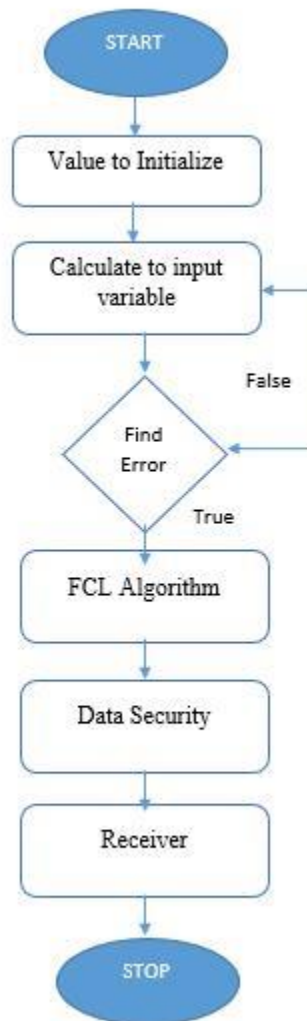
Figure 4: Flow chart of the FCL-BOOST algorithm process.

Figure 4expressions a flowchart of the Foremost Classification Level FCL-**BOOST**method algorithm and stages.

Algorithm:

Step 1: Assume that all the variables by the device are a prediction.

Step 2: Predict each tracking error from the average (latest forecast).

Step 3: To find the completely separable error, find the extractable value variable. This latest forecast is considered.

Step 4: Predict the classification (recent prediction) error from each observation on the marking page.

Step 5: Repeat steps 3 and 4 to enlarge/reduce the scope function.

Step 6: Take the weighted average of all the categories to come up with the final sample

3.1 Predicting is the client input distance based on the information obtained from the request example and.

3.2 The clients requested location and path code distance will be included in the ordered information

Input: source Client FileCF(text), LP (Location Path), Transfer dataT, Secure server SS.

Output: securedata transferSDT.

Start

The source inclient to load the fileinfoFCL-Boost-data,

Read Location Path LP, the nearest secure server verifies and clientNode connects level.

Make NC-Req path

CF -Req = {Starting IP, Ending IP} data verify to location and PC-Boost active

Map PathCF-Req

IF-Node PATH VERIFY runs

Node- PATH CF –Req

Node match active to PC-Boost

Else

SERVER NC -Req to its select another path.

Go to for current location and server map location active.

Find the Alder route on the detection of security.

Stop

4. RESULT AND DISCUSSION

The motivation behind this work is to build up another calculation to improve the general acknowledgment execution. The quicker, perform better execution, even though the calculation (FCL-support) presentation is comparable to the irregular interior framework with less exertion. Because of this strategy, there are two adaptations of the F-score include choice calculation (FCLBoost.L1 and FCLBoost.L2). (FCLBoost.L1 is broad recognition and development of a single taxonomy, Level 2) and FCLBoost.V2 into at least three types (Level 1). (Developed according to the FCL-Boost algorithm, double-select the features of the dataset using the F-level feature selection algorithm

Table 1 Parameter values

PARAMETERS	VALUE
Simulation	Cygwin

Propagation Model	DetrimentalInRadio Communication Systems
Area	800m x 800m
Broadcast Area	50-250 m
Transfer Pattern	UDP, CBR
Mobility Model	Random Mobility
Transfer per Packet	512 bytes
No of nodes	40

### 4.1. Implementation and Experimental Results

In this section, implement the main goal proposed system through the establishment and use of a parody of notification of the application is Network security.NS2Network simulator. The name of the Foremost Classification Level algorithm method (FCL-Boost) is. According to this method, the selection and classification of different classifiers or F level is the same assortment.The next step is to create a unified classification. Two versions, FCLBoost.L1 (Level 1) and FCLBoost.L2 (Level 2), under the same or different classifications have been developed.As per the outcomes got, the outcomes are predictable with writing reports.

FCLBoost.L1 and FCLBoost.L2 for exactness rate are the primary higher than FCL speeding up the calculation.FCLBoost.L1, 1-SVM joining strategy is the ideal way a higher position than the other upgrade calculations. The time has come to guarantee that it is utilized to re-check the aftereffects of various informational collections were gotten. (To build the FCL boosting calculation as the dispersion of the information collection is summed up in the consequences of three distinct informational collections that appeared in Table 1 is gotten from the reanalyzed. (Examination for correlation. According to the normal execution of the calculation, these outcomes are the best beneficial thing is FCLBoost.L1 level two bound together calculation.

4.2 FCL-boost Network performance.
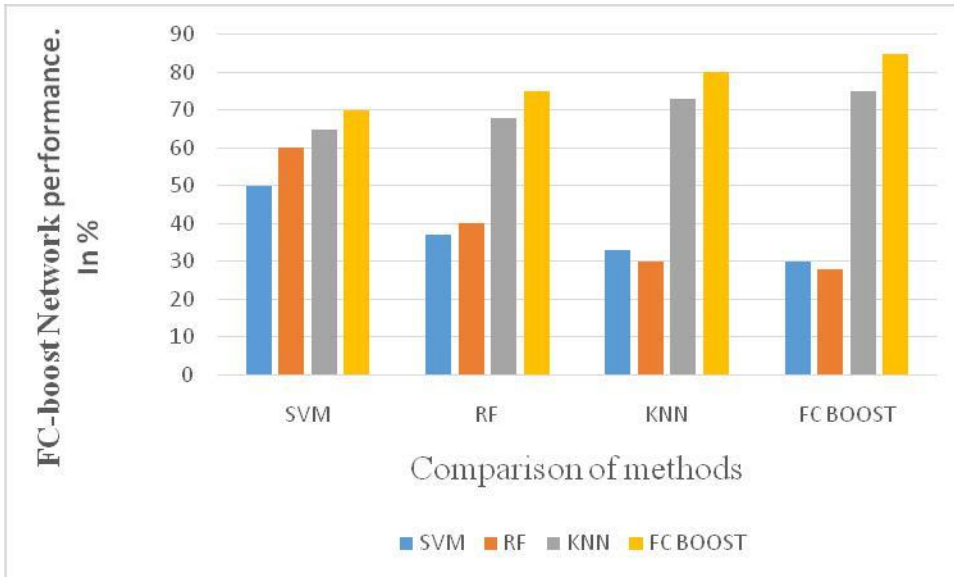
Figure 5: FCL-boost Network performance.

Support vector shows the Figure 5machine for measuring network performance of data protection system segment SVM and RF [Random Forest] and key nearest neighbor [KNN] and finally Foremost Classification Level [FCL-Boost] algorithm, method. In X-axis is the method of comparison with the unit of measurement algorithm and y-axis. The FCL-Boost network performance method differs from the focus of different data. Better than KNN. Tertiary performance ratio FCL-Boost ensample. Rate network performance increase for FCL-Boost 85% compared to SVM, RF, and KNN method.

4.3 Time Complexity

When one model is used, it is usually taken as a system identifier by the confirmation group collected from the information, while the other is used to produce the package. In these ways, I can collect different samples of my test information coding. The choice of technology, for example is due to accidental network security confirmation team-related training materials. My best example is drawn by a Figure [6] in the information list.
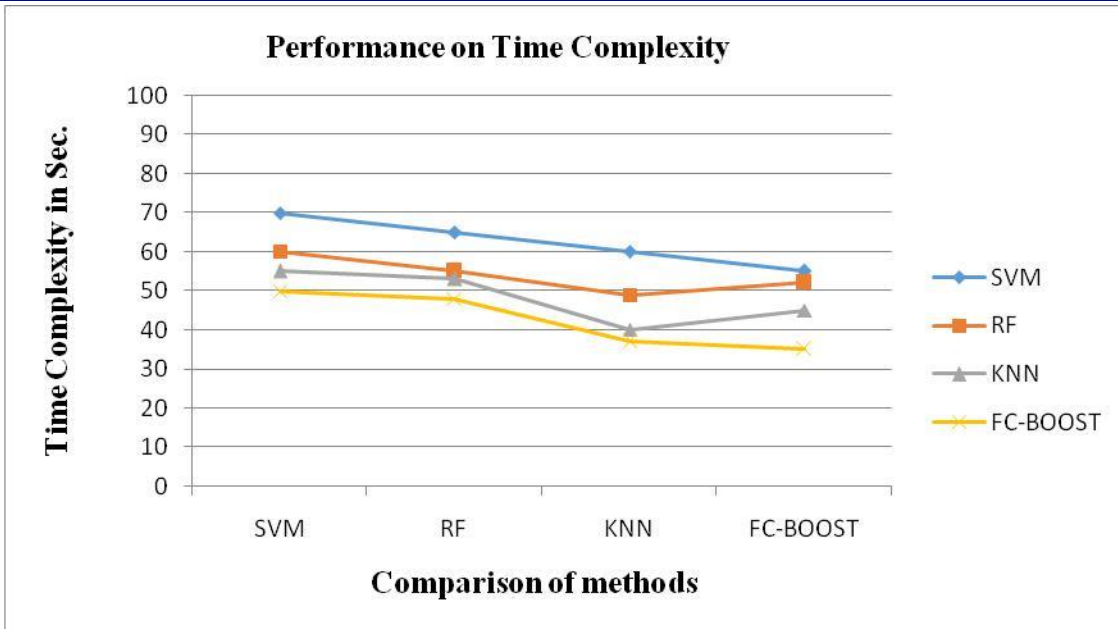
Figure 6 Time Complexity

Show the Figure 6 Evaluation SVM [Supported Vector Machine] and RF [Random Forest] and KNN [FCL-Compensation] Algorithm, Time Performance Team Performance Y Performance Algorithms. in State X Center Comparison Times. Methods Classification is proposed to measure the life extension at critical moments and critical moments when it is recommended that the radio product SVM 70 sec RF60 sec products one or two moments less incredible. KNN 55 sec, this structure than the previous strategy. Proposed FCL Accelerated Calculation, 50 sec Study Program Framework, Detection Best Performance FCL-Boost Half on Data Security Broadcast System, KNN 55%, and Random Forest 60%. FCL-boost performance 50% better timing for accessing the main goal of the proposed system.

4.4 Average Throughput

The number of typical open doors, give each time depends on the particular purpose. It how fast ratio characterizes the wheel hub, it can send the information through the system. Production normal throughput rate of the messages is sent via the wireless sensor network's corresponding multiplexer for a massive time.

Table 2 Throughput Analysis

Number of Nodes	SVM %	KNN %	RF %	FCL %
10	28	31	34	45
20	39	48	50	55
30	45	51	55	65
40	55	64	70	75

Table 2, the average output rate test, demonstrates the recommended configuration in the network. It would be the most proposed comparison of the number of existing node values in node processing.
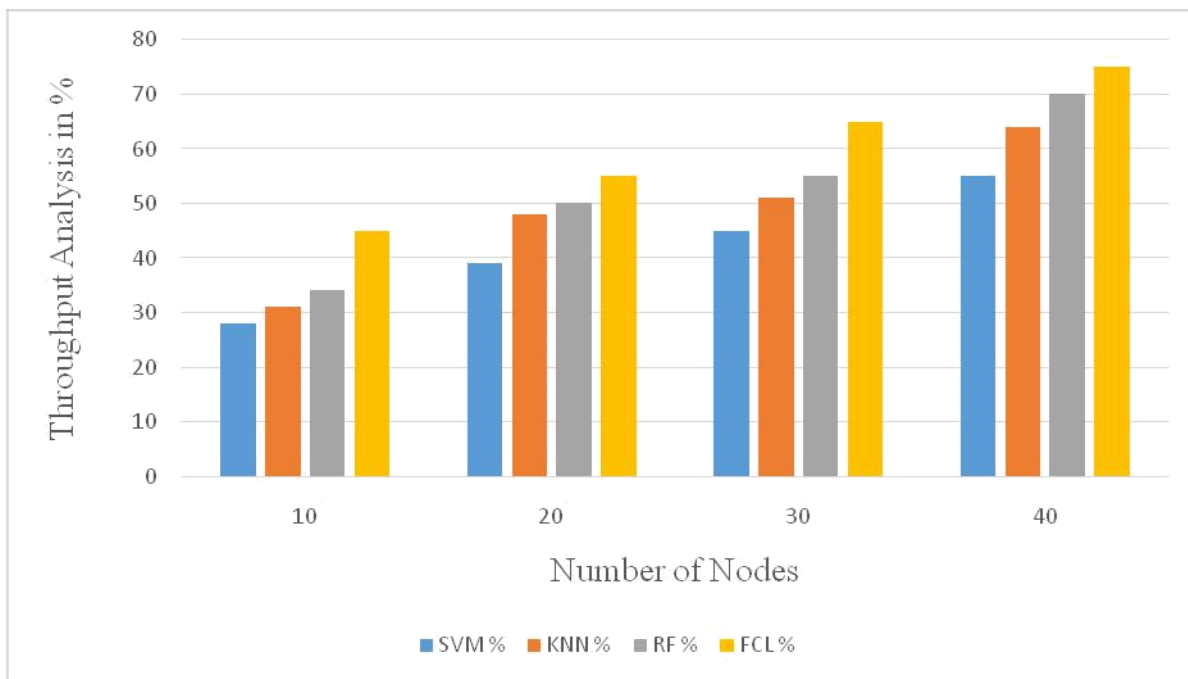

Figure 7 Throughput for Compares of Method.

The demo check is shown in Figure. 7. In this profile, the active test X is indicative of the Number of nodes and y-axis to indicate throughput analysis in the percentage of its turning speed count. These are dark orange and RF blue, and SVM from KNN. FCL compares best with yellow light and shade, for which the frame will make the current frame elite study recommended level.

4.5 Packet Transfer Ratio

A determined fixed number of pocket loop regions of the beam sent from the source end depends on being able to be the target rear. The estimated speed of the pocket movement, Pocket Transfer Rates are dark orange and RF blue and SVM from KNN. FCL compares best with yellow light and shade, for which the frame will make the current frame elite study recommended level.
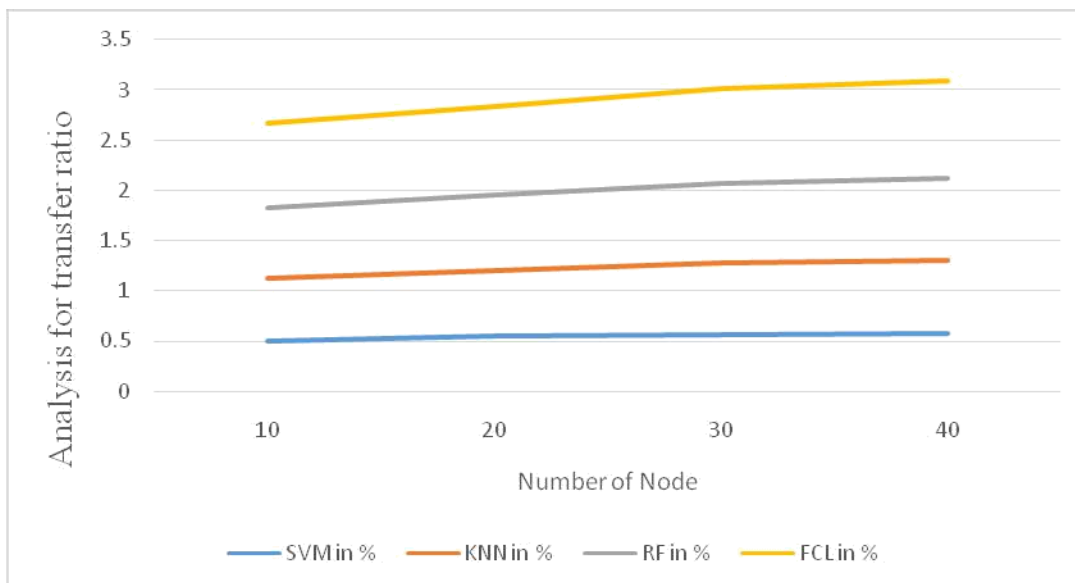
Figure 8 Packet transfer ratio

Figure 8 shows the packet transfer rate. Like the bundle number of x and nodes, this number is the number of talking centers centered on the y-axis pocket transfer rate. The color blue (SVM) and color orange (KNN), and emulsion (radio frequency) color oversee the percentage of yellow color compared to the system with the highest transfer rate proposed system from the problem in these previous methods. Multiple Lead Classification Level to support Foremost Classification Level has the best method (FCL).

5. CONCLUSION

The Foremost Classification Level [FCL Boost] might be created that the best computing. The strategy is not much progress has been just that, this gives quickly, high-accuracy, high-exactness, and quick outcomes. An especially invaluable situating calculation is valuable in a variety of system security data. In this way, FCL-acceleration might like it. FCL-Boost has lower, and steps accuracy ratio comparison is better and contains more than various computational calculations. Thinking about these attractions, FCL-acceleration may soon be the most frequently used calculation. FCL stimulus calculation is ideal for use as a symbol of clinical research in living, in-depth learning, and used consistently in computer communication. At least three classifications of FCL stimulus can be used. Also, FCL-Boost.L1 has an incentive level that can be used as an isolated classifier for FCL. It is FCL-Boost. The L1-specific bit reaches the highest standalone classifiers. The F score shows the judgment calculation to make this favorable position. By adding different highlights, similar details can be deciphered in unexpected ways. Once the opportunity closed, the classification performed in solid, FCL accelerated increments. Likewise, it is recommended to use powerful classifiers for calculations. Equipment classification often participates in the weak classification to draw a solid classification. The strong of FCL-Boost. This will say that FCL help is another approach to make a troupe arrangement. Improvement of the rate net presentation for FCL-Boost

85% compared to SVM, RF, and KNN method. Best Performance FCL-Boost Half on Data Security Broadcast System, KNN 55%, and Random Forest 60%. FCL-boost performance 50% better timing for accessing the main goal of the proposed system. A superior outfit classifier can be made with an incredible classifier, and the F-classifier includes choice calculation.

REFERENCE

1. A. Borji & "Combining Heterogeneous Classifiers for Network Intrusion Detection", Advances in Computer Science - ASIAN 2007. Computer and Network Security, pp. 254-260, 2007.

2. H. Zouari and L. Heutte & Y. Lecourtier & A. ALimi, "Un panorama des méithodes de combinaison de classifieurs en reconnaissance de formes", (French) [An overview of classifier combination methods in pattern recognition]. Proc. RFIA'2002, vol. 2, pp. 499-508, 2002.

3. Y. Zhang & Z. Han & J. Ren, "A Network Anomaly Detection Method Based on Relative Entropy Theory", Second International Symposium on Electronic Commerce and Security, pp. 231-235, 2009.

4. A. H. Hamamoto, A. Carvalho, L. D. H. Sampaio, L. Abrao and T. L. P. Mario, "Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic", Expert Systems with Applications, vol. 92, pp. 390-402, February 2018.

5. J. S. Paz & D. T. Roman and "On Entropy in Network Traffic Anomaly Detection", 2nd International Electronic Conference on Entropy and Its Applications, 2015.

6. C. Maklin and "KL Divergence Python Example", Towards Data Science, [online] Available: https://towardsdatascience.com.

7. Y. Labit & J. Mazel and "HIDDeN: Hausdorff distance based Intrusion Detection approach DEdicated to Networks", The Third International Conference on Internet Monitoring and Protection, pp. 11-16, 2008.

8. D. Dua & C. Graff and "UCI Machine Learning Repository" in Irvine, CA: the University of California, School of Information.

9. G. Wang and J. Hao, J. Ma & L. Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering," Expert Systems with Applications, vol. 37, pp. 6225-6232, September 2010.

10. C. F. L. Lima and F. M. Assis & C. P. de Souza, "A comparative study of the use of Shannon Réinyi and Tsallis Entropy for Attribute Selecting in Network Intrusion Detection," Springer Berlin Heidelberg Intelligent Data Engineering and Automated Learning, pp. 492-501, 2012.

11. D. S. Hochbaum & D.B. Shmoys and "A best possible heuristic for the k-center problem," Mathematics of Operations Research, vol. 10, no. 2, pp. 180-184, 1985.

12. M. Tavallaee and E. Bagheri W. Lu &A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", Second IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.

13. Q. Chen, A. Whitbrook and Uwe Aickelin & Chris Roadknight, "Data Classification Using the Dempster-Shafer Method," Journal of Experimental Theoretical Artificial Intelligence, 2014.

14. S. Surathong, S. Auephanwiriyakul & N. T. Umpon, "Decision Fusion Using Fuzzy Dempster-Shafer Theory," Recent Advances in Information and Communication Technology, pp. 115-125, 2018.

15. L. Xu, A. Krzyzak & C. Y. Suen, "Methods of Combining Multiple Classifiers and Their Applications to Handwriting Recognition," IEEE Transactions on Systems Man Cybernetics, vol. 22, no. 3, pp. 418-435, May-June 1992.

16. Tchakoucht TA & Ezziyyani M. Building a fast intrusion detection system for high-speed-networks: probe and DoS attack detection. Procedia Comput Sci. 2018;127:521–30.

17. Zuech R and Khoshgoftaar TM & Wald R. Intrusion detection and big heterogeneous data: a survey. J Big Data. 2015;2:3.

18. Sahasrabuddhe A and et al. Survey on intrusion detection system using data mining techniques. Int Res J Eng Technol. 2017;4(5):1780–4.

19. Dali L and et al. A survey of intrusion detection systems. In: 2nd world symposium on web applications and networking (WSWAN). Piscataway: IEEE; 2015. p. 1–6.

Scarfone K & Mell P. Guide to intrusion detection and prevention systems (idps). NIST Spec Publ. 2007;2007(800):94.

20. Debar H and An introduction to intrusion-detection systems. In: Proceedings of Connect, 2000. 2000.

21. L.Bharathi, N.Sangeethapriya, "Attribute Table based Energy- Efficient and qos-of Multipath Routing Protocol using in Loss- Free Optical Burst Switching Networks" in Journal of Advanced Research in Dynamical and Control Systems, ISSN 1943-023X Volume 11 Special Issue , June 2019.

22. L.Bharathi, N.Sangeethapriya, "An Improved Link Stability Based on Swift Exploring Packet Ratio Using Expected Time Matrix in Wireless Sensor Network" Journal of Computational and Theoretical Nanoscience 17 (12), 5528-5534, 2020

23. N SangeethaPriya, L Bharathi, "Optimal Multilevel Link Extend Umpiring Routing Based Secure Routing Protocol for Improving Privacy Standard in Wireless Sensor Networks" Journal of Computational and Theoretical Nanoscience 17 (12), 5543-5549, 2020