Journal of Intelligent Systems and Internet of Things
Vol. 11, No. 02, PP. 42-62, 2024
DOI: https://doi.org/10.54216/JISIoT.110205

Advanced Intrusion Detection in Vehicular Networks: Empowering Security through Hybrid Off-loading Techniques and Enhanced Radial Bias Neural Network

Prashant Kumar Shukla [1, *], Ratish Agarwal [2]

[1, 2]Department of Information Technology, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, MP, India,
Emails: prashantshukla2005@gmail.com, ratish@rgpv.ac.in
[*]Corresponding Author: prashantshukla2005@gmail.com

Abstract

Over the last several decades, the implementation of ITS has shown to be the most efficient and successful strategy for expanding the variety of current transportation networks. Vehicle-based offloading of data going to be essential for forthcoming networking innovations like D2D and 5G due to the substantial contribution it makes to efficiently using network capability while wasting minimal power. Information transmissions that would normally need a cellular network's infrastructure may instead be made using alternative networking mechanisms including Bluetooth, WiFi, and opportunistic communications. Data offloading has the ability to significantly increase the efficiency with which network resources are used. The offloading of data from vehicles has a considerable impact on the strain on cellular networks. It helps the network achieve higher throughput by facilitating the simultaneous reception of data by a large number of users. First, we must establish that the problem of Vehicular data offloading is an NP-hard target set selection (TSS) issue before we can even begin to characterize it. Using a combination of Hybrid PSO and GWO, TSS selects a small group of nodes to do the redundant data exchange (Particle Swarm Optimization with Gray Wolf Optimization). Collaboration between individuals and ISPs to identify effective aim sets may provide useful insights. If malicious users are present in the target group, they may slow down network activity by spoofing or by reducing the network's offloading capacity. It is possible that the whole network's performance would suffer as a direct result of these malicious users. In this study, we suggest a hybrid approach to communication for specifying the intended audience. We take use of the characteristics of opinion dynamics amongst users to get around the issue of overlapping community detection. Trust-based metrics inferred from users' activities are used to ensure the safety of the target set. In order to call 911, the suggested work additionally incorporates a method of sorting and classifying the offload limitations through Radial Bias Neural Network (RBNN). The following may be determined with the use of the proposed work's performance indicators: precision, entropy, and delay.

Received: September 05, 2022 Revised: December 13, 2022 Accepted: January 16, 2024

Keywords: Accuracy and Entropy; offload limitations, delay; Improved Reduced Round Advanced Encryption; Radial Bias Neural Network (RBNN); NP-hard target set selection (TSS) problem

1. Introduction:

Personal computer (PC) networks, and the Internet in particular, have assumed an increasingly important role in many spheres of human activity during the last several decades. Two of the most important barriers in the present are communication and teamwork. Data and information end up becoming the most crucial assets [1]. Since more data is being stored and produced on network-based frameworks, the world is becoming more subservient to the data. People

make use of the Internet and other network services from the moment they get up until far after midnight. On the other hand, the Internet has presented hitherto unknown security challenges. [2] point out that keeping, communicating, and automating the processing of data becomes a critical challenge. The widespread use of web-based software has made it imperative to take data security very seriously. The security mechanisms of a framework must be created to prevent unauthorized access to its resources and data. However, in reality, it is impossible to prevent security breaches entirely. And now, we can try to tell these incursion attempts apart so that action may be taken to repair the damage. This motivates an interest in the automated approach proposed by [3] for spotting security loopholes and malicious coding practices. Different layers of security are established depending on the relevance of the data. Prepared data security swiftly evolves from personal to commercial to military standards. Serious unintended consequences may result from compromises in data privacy, security, and transparency. Several tried-and-true approaches and processes developed throughout time to protect PC architectures. Computer networks are typically protected by a combination of measures, including a firewall, encryption, secure organizational conventions, secret phrase-based verification, and an access control list. However, even with these safeguards in place, an intrusion that deviates even slightly from the review information's example may go undetected. Traditional firewall techniques are not capable of providing 100% security, thus including intrusion detection in your overall security strategy is crucial. Even after taking all these precautions, a determined attacker could still be able to get entry into your business. This calls for further aid in the form of the detection of numerous security flaws. According to Bhuse and Gupta [2006], intrusion detection systems (IDS) [4] are a crucial security technique.

Most commercial IDS are so-called "Abuse Detection Systems," designed to spot typical threats alone. Experts and intrusion examiners compile a database of previously identified indicators of compromise to be used in this technique. This database compares the volume of traffic across the arrangement of cycles within the computer to different types of organizational structures. If there is a correlation with database entries, the IDS will issue a warning. While this kind of architecture reduces false positive alerts, it is still incapable of identifying completely new forms of assault. Abuse detection approaches have two advantages: they are effective at identifying assaults without generating an overwhelming number of false positives, and they can reliably examine the usage of a specific attack tool, as described by Mamun and Kabir [2010]. However, these methods of abuse detection come with a price: they are limited to identifying the kind of assaults that are already documented in the database. Consequently, the data warehouse has to be regularly updated with indicators of new assaults.

Since the computation and data, the executive need varies from organization to organization, so do their security requirements. Over the last decade, the scientist has been in charge of the administration of a handful of computers. It has been found that security requirements for medium-sized educational networks vary greatly from one region to the next. Various security threats have been faced and proposed solutions throughout this tenure. While antivirus software protects against well-known threats and firewalls guarantee by only allowing authorized services through, what about the growing threat posed by unknown attacks? Up to a point, IDS is the proper answer. It's hardly a miracle cure, however. Scientists have run across some problems when trying to put IDS plans into action. This motivates in-depth exploration both inside and outside of conventional IDS paradigms. Recently, a lot of effort has been put into intrusion detection, but no major progress has been made. IDS has a problem in spotting typical attacks. When trying to identify unknown assaults using an anomaly detection strategy, false positives become a problem. Limitations in identifying insider attacks are another major problem. Most existing IDS [5] fail miserably over a lengthy period when confronted with multistep assaults. However, enough data exists or may be obtained to help network executives spot violations of the plan. Sadly, the directors can't see everything and find the important data since the data size is too large and the investigation measures are too slow. Having massive resources to proactively review the data for strategy violation is not rational given the large amounts of false positives that result from doing so.

Anomaly detection methods have limited value because of serious discrepancies in how researchers use peculiarity identification. The key challenge in anomaly detection is, therefore, to identify a reliable identification and classification method that minimizes false positives while maintaining a high degree of accuracy. Finding appropriate feature vectors that faithfully depict the odd wonder or the region of irregularity producing expert in frequency or time-space using some area change or wavelets is essential. After distinguishing the element vectors, we may use clustering, classification, or regression analysis to rank the anomalous and typical patterns of behavior or sign.

The field of IDS is seeing a great deal of development and advancement. Organizations should thus make an effort to precisely define what it is they want to achieve with the IDS implementation. IDS development has not advanced to the extent that it is able to operate without people assistance. Current IDS technology does allow for some automation,

such as notifying the administrator of a detected malicious action, blocking the offending connection for a period that the administrator specifies, and gradually updating a switch's access control list to prevent the offending connection. [6] note that monitoring IDS logs regularly is necessary for maintaining control in the face of incidents. The nature of malevolent actions recognized through the IDS over some time can only be studied by regularly reviewing the logs. However, current IDS technology is still lacking in areas such as providing reliable investigations into detected intrusions over extended periods. At the moment, you have to do this by hand. Therefore, a well-defined mission statement is crucial for every organization. Response strategy and incident management in the event that an intrusion is found and notified by the IDS. In addition, the organization must have competent safety personnel to cope with the crisis. How an IDS has been sent has a significant impact on its effectiveness. Both the planning and the actual doing of anything need a great deal of preparation. To get the benefits of both organization-based and have-based IDS, a hybrid setup is often desirable. In reality, each new development complements the others. However, as demonstrated by [7] his decision might vary from one organization to the next. Many businesses use network-based IDSs due to their versatility in system inspection.

In contrast to host-based IDS, there is no requirement for software during the production phase. The vast majority of companies nowadays use hybrid approaches. They plan to use host-based IDS as a remedy. That intrusion detection system [8] software uses a lot of resources. All required features should be present in the system. Pre-installation of host-related sensors is common practice.

The ratio of sensors to managers is an important consideration. There is no general rule of thumb for determining this ratio. It is important to know how many different types of traffic each sensor is monitoring and under what circumstances. Before initiating IDS use, it is crucial to prepare the gauging technique to prevent incorrect positives. A poorly arranged IDS detector might report many false positives. iv) The IDS technology is still passive rather than active. Attack scores may be reduced thanks to IDS technology. Attack markers are instances of assaults that have already occurred. When a new kind of attack is discovered and a solution to it becomes available, the mark database should be updated to reflect this.

[9] how the responsibility for updating trademarks often passes from retailer to vendor. One crucial aspect of the organization's IDS in a foreign atmosphere must be kept in mind when arranging to deploy it. However, in an exchanged organization, hosts on different ports cannot view each other's traffic since they are in different effect zones, in contrast to a centralized organization where hosts on different ports may see each other's traffic at the central point. To detect malicious data, an enterprise-based IDS sensor must monitor all traffic over a port. This can only be done by the use of a port reflecting or spreading over in a climate swap. The organization-based IDS sensor may be installed on a single port that handles traffic for an entire VLAN. Although this is a result, [10] warns that a busy company may have issues with performance. The IDS device may reject transportation if every 10/100 Mbps port in a VLAN is matched to other 10/100 Mbps port in the same VLAN since the over-all throughput of all those ports might be higher 100 Mbps. This is at present a much more challenging exam with the availability of Gigabit port speed. To filter traffic right off the switch backplane, Cisco frameworks have developed an IDS module for the Catalyst 6000 arrangement switch. However, this configuration is still in line with Gigabit speeds. Starting right now, this module can support data transfer rates of up to 100 Mbps. The extent to which enterprise-based IDS can adapt to a changing environment remains a concern. Here is the paper's outline. Section 2 discusses prior research, Section 3 defines the approach to the suggested study, Section 4 details the experimental analysis and findings, and Section 5 offers a summary and recommendations for upcoming investigations.

2. Related Work

The Internet of Things (IoT) is a rapidly expanding web that transforms everyday tangible objects into cyber-enabled "smart" ones. The devices in this network use a variety of communication protocols, making the network a heterogeneous one. Even if encryption and authentication make the IoT network secure, it still isn't immune to cyberattacks, which is why intrusion detection systems are necessary. The history, framework, and tools of Internet of Things and intrusion detection systems (IDS) are the primary topics of discussion in the works cited section. Topics related to the IoT have been introduced in some previously published books. Data interchange requirements and the IoT architecture were first established in [11]. The application programming interface (API) decouples services from the protocols and network components to which they are traditionally tied. The capacity to move services across systems is a prerequisite for assigning them. [12] provide a summary of the IETF standard for the Internet of Things that was introduced in 2013. The vision and motives for the Internet of Things were discussed in a 2013 paper by

Gubbi et al., which also provides a list of IoT application categories and a new way of thinking about how to identify them. Transportation, smart home automation, smart health, smart city, electronic governance, assisted living, electronic education, retail, logistics, agriculture, automation, industrial development, business or process management, etc. are only some of the sectors the writers have investigated. Extending the many IoT applications, [13] presents an overview of IoT and its prospects and challenges. It covers a wide range of topics related to the Internet of Things, such as its architecture, its business potential, its standard application fields, its components, its communication technologies, its significant concerns, and its open research challenges. There are obvious upsides to using IoT solutions. In 2015, Ray presented a standard framework for sports-related IoT devices. Assumptions for this study include IoT's ability to improve the connectivity, intelligence, orchestration, service, and analytics of sporting equipment and the people using it. Sensors, microcontrollers, the Internet, the cloud, coaches, electronic devices, smart devices, and medical professionals are all brought together in the IoT for sports.

With its multifaceted design, IoT, or the Internet of Things, has the potential to take sports to the next level of intelligence. The results of this study showed that the number of nodes (players) had a direct bearing on the amount of time it took for data to converge, and it also addressed a wide range of problems associated with sports. According to this theory, the IoT strategy's widespread appeal is because it can be used in such a wide range of contexts (e.g., human industry, commerce, medical, agriculture, lifestyle, etc.). [14] analyzed numerous commercial IoT frameworks and provided a comparative study based on consumption techniques, application development, industrial use, supported protocols, etc. The widespread use of various Internet of Things–based solutions has greatly improved the quality of human existence. Over the past few years, IoT has had an important impact on the progress of connected homes, vehicles, enterprises, and other facets of modern life.

High productivity with improved quality is one of the most visible benefits of the IoTs in manufacturing and other services provided in the industrial sector. The advantages of the IoTs outlined above have emerged without a hitch, but its global adoption will need overcoming some obstacles. Hacker security is often cited as the biggest problem facing the IoTs. Problems with standards, addressability, scalability, and so forth have also been noted in the IoT. [15] studied IoT in a wider sense, with emphasis on protocols, technologies, and applications; they also addressed associated challenges, highlighting the need for more study. The concept of the IoT centers on the consolidation of its many disparate components. The authors also lay out a plan for how various protocols interact with the Internet of Things and other cutting-edge technologies in their infancy, such as large

The goal of this investigation was to find ways to organize ID that could be used universally and precisely. The use of data mining techniques and ML computations to discover useful framework highlight designs displaying network behavior is central to this line of thinking. Then, within this context, you can recognize anomalies and known intruders. To prove that the new methods are more persuasive than older ones, it is recommended to use the publicly available Knowledge Discovery in Database (KDD) [16] Cup 99 dataset. There are three main categories through which this investigation may be broken down. i. A multi-dimensional hierarchical K-Means clustering-based hybrid ABC-DT approach to solving the optimum cluster selection issue of IDS (MKM-ABDT).

The process of identifying instances within a dataset whose behavior deviates from the norm is known as anomaly detection. Differentiating evidence is informational foci, objects, experiences, or events that deviate from the norm or standard of a group. These deviations are rare but may signify serious threats like cyber intrusion [17] or blackmail if ignored. Finding the precise location of a strange occurrence is a vital part of any sociological study, as is using other methods of research to learn more about the phenomenon in question. The goal of this study is to provide a powerful IDS that makes use of and integrates many widely used ML techniques to detect and prevent malicious activity on network nodes and members.

3. Research Methodology

The task of clustering is to divide a collection of items into smaller groupings called clusters. Items within the same group should be "similar," whereas objects across groups should be as dissimilar as possible. To further improve routing performance, the clustering method divides the network into numerous clusters, similar to the Key-Match Algorithm (KMA) [19]. Figure 1 is an illustration of a cluster. An adversary may trick nearby nodes into thinking a hacked node is a close neighbor by broadcasting a bogus neighbor value. A selective forwarding attack may be launched if the hacker's node appears along the route and uses a low rank to lure in traffic. In addition, hackers may launch other attacks on the system, such as placing their node in the routing route to syphon off traffic and drain the

power of trusted nodes via loops. Encryption [20] might help stop these attacks, but it could still be possible to conciliate a real node. While asymmetric cryptography is a viable option in an ideal world, it is typically impractical due to resource constraints. We use a clustering approach to partition the network into various clusters, which helps with routing, in addition to the Key Match Algorithm. For lossy networks, we assess the vulnerability to routing along route matrix assaults [21] by generating cluster heads.

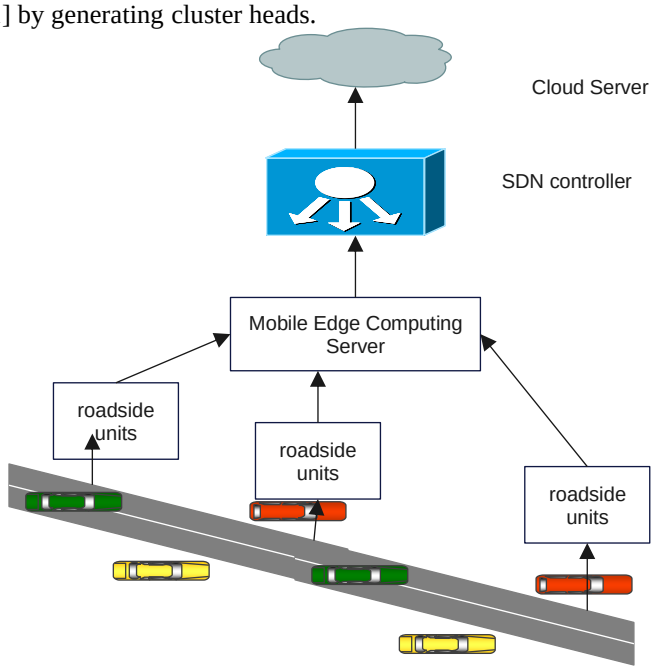

Figure 1: Collection of Data from Vehicular Networks

3.1 Data Collection Model

Protecting a computer network against intruders, both external and internal, is the job of software designed to detect network intrusions. The goal of the learning job known as an intrusion detector is to create a prediction model (a classifier) that can identify malicious connections (intrusions or assaults) from benign ones. MIT Lincoln Labs was responsible for developing and overseeing the DARPA Intrusion Detection Evaluation Program [22]. The goal was to conduct a literature review on intrusion detection. An auditable data set representative of a military network was supplied, complete with simulated incursions of varying types. A part of this dataset was used in the KDD intruder detection task in 1999. Lincoln Labs created a system to collect raw TCP discard data for a LAN replicating a normal U.S. Air Force LAN over nine weeks. Even though constantly attacking it, they used the network as if it were a real Air Force base.

The unprocessed training information was about 4 TB of condensed binary TCP [23] discard data that showed how the network worked for seven weeks. There are already almost five million connection records based on this data. Similarly, there were almost two million connection records gleaned from the two weeks of test data. Data travels from one IP address to another using a predetermined protocol during a connection, which is defined as a series of TCP packets [24] with a beginning and an end at specified timings. Every one of your connections has been assigned a label: safe or attacked using one of the many possible methods. About 100 bytes go into making up each connection record.

$$v_{\text{rel}} = \begin{matrix} \left(v_x \cos\left(\theta_x\right) - v_y \cos\left(\theta_y\right)\right)\hat{\imath} \\ \left(v_x \sin\left(\theta_x\right) - v_y \sin\left(\theta_y\right)\right)\hat{\jmath} \end{matrix} \quad (1)$$

It is given that the exact number of relative velocity is

$$|v_{rel}| = \sqrt{v_x^2 + v_y^2 - 2v_x v_y \cos\left(\theta_x - \theta_y\right)} \quad (2)$$

R_y and R_x are the types of vehicles y and x, correspondingly, here, for instance. R x+R y is the extreme enclosed area in which two vehicles [25] may converse simultaneously. When V eh h x and V eh exchange messages, the maximum duration t max is specified as

$$t_{\max} = \frac{R_x + R_y}{|v_{rel}|} \quad (3)$$

Eq. (3) becomes true and the vehicles moves in the same way while they are going the opposite way due to the change in those angles, i.e., $\_x - y = \cos y = -1$.

$$|v_{\text{rel}}| = \sqrt{v_x^2 + v_y^2 + 2v_x v_y} \quad (4)$$

The extreme transmission time, t max, may be found by using Eq. (4). Given that the lowest value of the denominator in Eq. (2), at its lowest, t max. The automobiles moving in the opposite ways thus have the least amount of interaction time.

Lemma 2: The maximum amount of interaction time is accessible to automobiles moving in the same way.

Proof: The angle between Veh x and Veh y, that is, cos (0) =1 and x- y=0, is equivalent to the angle, when they are travelling in the same direction. The relative velocity value is determined by using equation (5) as follows:

$$|v_{\text{rel}}| = \sqrt{v_x^2 + v_y^2 - 2v_x v_y} \quad (5)$$

This is the absolute minimum. Because the denominator is the lowest when calculating t "max," the largest value is the t max. A total of four channels are available, with varying bandwidth rates between 1 Mbps and 11 Mbps. The infrastructure needed to employ a range of interfaces from these standards is installed in every vehicle. As a percentage of all links in use to the whole quantity of connections is known as the disruption's ratio. Transfer rate increases and context swapping delay decreases as the interference ratio rises. This is because more network resources are being used, which leads to higher network utilization.

3.2 Utilising Hybrid Particle Swarm Optimisation and Grey Wolf Optimisation for Data Offloading

The grey wolf optimizer (GWO) is a swarm intelligence system that takes cues from grey wolves' hunting techniques and pack structure. The name "grey wolf optimizer" also refers to this tool (GWO). The majority of a grey wolf's life is spent in a social group called a pack, which has a well-defined social dominance order. The wolf pack may be divided into four levels, or packs: alpha, beta, delta, and omega. Wolf packs have a hierarchy in which the alpha wolf is the pack's leader, the beta wolf is a subordinate who helps the alpha wolf, the delta wolf patrols the territory's edges and reports any threats to the alpha wolf, and the omega wolf is the scapegoat. Wolf packs have a dominant alpha and a group of followers known as betas. The alpha solution is the best possible match in the GWO method, while the delta and beta solutions are the second and third best possible matches. When all other possible solutions have been used up, we are left with the omega solutions. Grey wolf hunting performance may be broken down into these discrete phases according to the algorithm: (1) prey detection and encirclement (2) attacking prey and hunting (3) hunting and looking for prey (and areas around prey). The whole processing unit is shown in its entirety in Figure 2 on this page

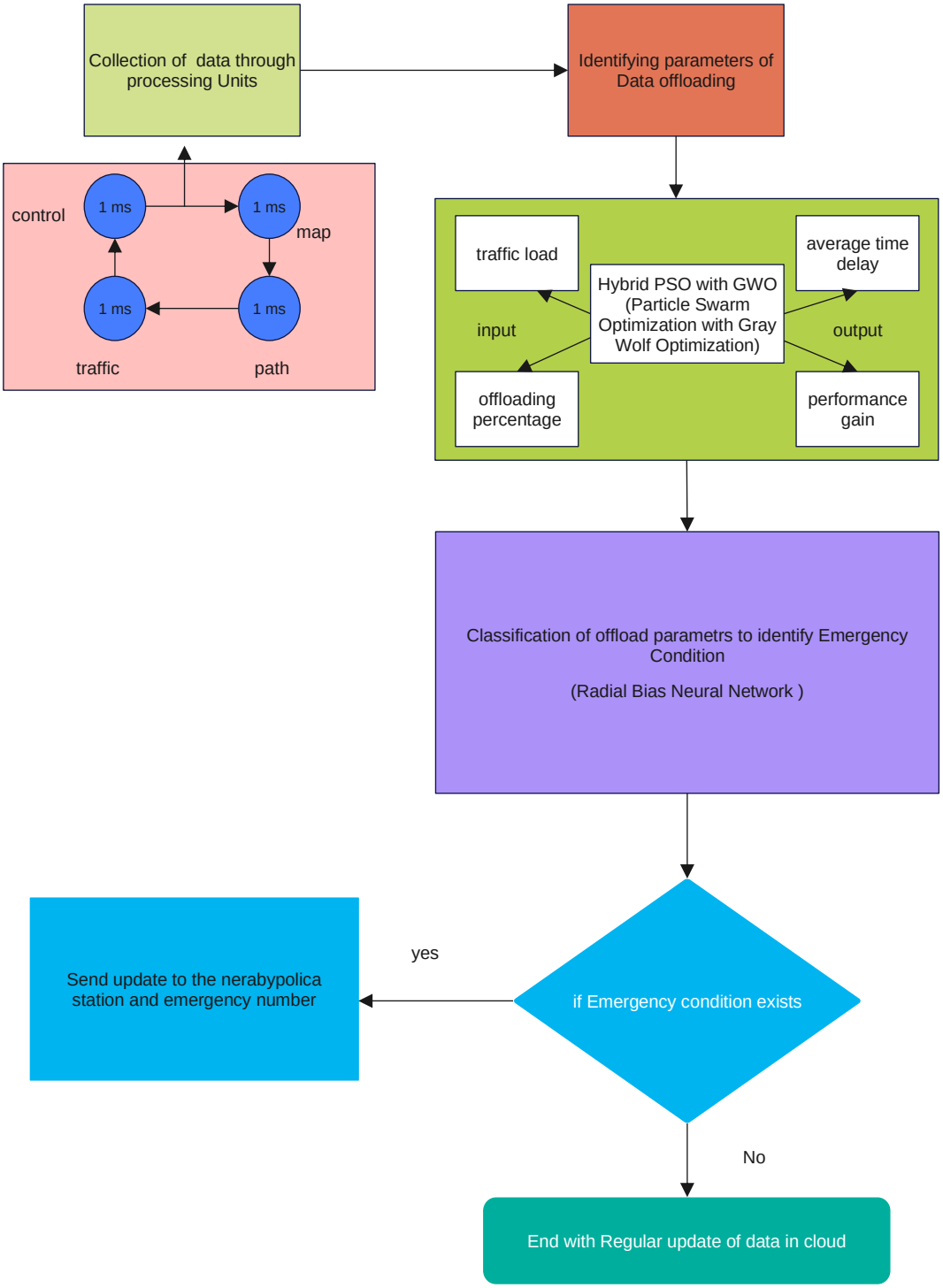

Figure 2: Complete Processing Unit of Planned Work

Kennedy and Eberhart established the foundation of the PSO algorithm in [32], which was inspired in large part by simulations of animal social interactions like fish schools and birds flocking. The PSO algorithm was developed by Eberhart and Kennedy to simulate the cooperative efforts of animals such as fish and birds. To maximize their chances of finding food, birds may either spread out or cluster in their hunt. The fact that one bird is able to detect the presence of food while the others are searching for it suggests that the bird is aware of its location and has

received the appropriate signal from the surroundings to find food. Because of the message they are delivering, birds will eventually congregate in large numbers at the location where there is food available, which is very helpful at any given moment as they migrate from site to site looking for food. The phenomena are referred to as the "swarming effect."

This method, which is inspired by animal behaviour, may be used to compute global optimization functions/problems, whereby each individual in the swarm or crowd is represented by a particle. In the PSO method, each pair in the crowd has its position across the worldwide search area updated using two mathematical calculations that determine its comparative position to the others. In this part, we offer the following mathematical equations:

$$\begin{aligned} v_i^{k+1} &= v_i^k + c_1 r_x\left(p_i^k - x_i^k\right) + c_2 r_y\left(g_{\text{best}} - x_i^k\right) \\ x_i^{k+1} &= x_i^k + v_i^{k+1} \end{aligned} \tag{6}$$

Our hybrid, a low-level coevolutionary mixed hybrid approach, combines the Grey Wolf Optimizer and Particle Swarm Optimisation algorithms. The hybrid is deemed low-level since we are merging the characteristics of both kinds into one. We avoid switch back and forth between the two forms, therefore it must be coevolving. That is to say, they are both active simultaneously. Therefore, it is considered mixed since two separate iterations contribute to the development of ultimate solutions to the issues at hand. We make improvements to both the exploitation and exploration abilities of Particle Swarm Optimisation at the same time to make each one stronger.

HPSOGWO's formulations of mathematical problems to revise the search space location of the first three agents in real-time (5). In its place of using standard measured formulae, we use the inertia steady to regulate the grey wolf's exploitation and exploration of the search area

$$\begin{aligned} \vec{d}_\alpha &= |\vec{c}_1 \cdot \vec{x}_\alpha - w * \vec{x}| \\ \vec{d}_\beta &= \left|\vec{c}_2 \cdot \vec{x}_\beta - w * \vec{x}\right| \\ \vec{d}_\delta &= |\vec{c}_3 \cdot \vec{x}_\delta - w * \vec{x}| \end{aligned} \tag{7}$$

Integration of the GWO and PSO variations is accomplished by the provision of the subsequent velocity and the revised equation:

$$\begin{aligned} v_i^{k+1} &= w * \left(v_i^k + c_1 r_1\left(x_1 - x_i^k\right) + c_2 r_2\left(x_2 - x_i^k\right) + c_3 r_3\left(x_3 - x_i^k\right)\right) \\ x_i^{k+1} &= x_i^k + v_i^{k+1}. \end{aligned} \tag{8}$$

Here is the pseudocode for the suggested work.

Algorithm1Pseudocodeof PSO-GWO algorithm

1. **Initialize** the inhabitants of whales *Xi* (i =1,2,…,*n)*
   Figuring out how fit to each search agent is.
   Initialize *A*, C,*l*, and p
   Using the fitness values as a guide, choose Xa, Xp,
   and Xs from the solutions
   While *(t*<maximum number of iterations)
   do
   for every search agent
   do
   Update *a*, *A*, C,*l*, and *p*
   if(,*p*<0.5)**then**
   if(IA I2:1)**then**
   Updatethepositionofthecurrentsearchagentbyusing(6)
   else
   Updatethepositionof*Xa, Xp, Xy*byusing(7)
   endif
   else
   Updatethepositionofthecurrentsearchagentbyusing(8)

endif

end for

CheckifanysearchagentgoesbeyondthesearchspaceandamenditCalculatethefitnessofeachsearchagent

Update*Xa, Xp, Xy*ifthereisabettersolutiont=t+l

end while

By using the hybrid optimization method, we may determine the superior job and, as a byproduct, get rid of superfluous information. It is possible that the proposed method's optimized findings would provide BS/AP with data that would allow it to more successfully assign resources, like as sub-carriers and power, to project unloading. The BS/AP will then respond to the person requesting services (end-user), who will use the information to decide which offloading mechanism to use. Here is a further explanation of what's going on: It is the job allocated to the MD that determines whether or not the tasks can be calculated close by, and whether or not they should be dumped to additional resource-intensive MEC servers. The MDs then reach out to their present BS for assistance in acquiring the necessary tools (home BS). Given the characteristics of the inquiry that was sent from the base station, the controller server, which also handles job scheduling and updates to the Resource Allocation Table (RAT), chooses the most suitable MEC server from among those available in the cooperative region. When the MDs have determined which MEC host is most suited to the task at hand, they forward the workload to that server.

The proposed Algorithm1 has certain challenging parts, one of which is determining the cost of a candidate explanation given the existing state of MDs. This is on top of the already challenging computations involved in updating the velocities of individual particles based on equation (20) and the current positions of MDs (21). We will go through the specifics of how Algorithm1 optimizes energy use and resource allocation in the two procedures below. The locations of the device, which are stored in a vector with k dimensions, must be initialized at the beginning of the function. Here, t is the longest potential time required for the startup operation to complete (time complexity maximum). Searchers need to iteratively discover the result space until they locate the optimum solution that is satisfied the optimization goal at hand. Since there are k dimensions to the issue and x i(k+1) candidates to choose from at each iteration, the difficulty of determining the cost of candidate solutions is t max'.

3.3 Classification of offload parameters

Learn how the suggested model is trained to recognize unsafe scenarios based on variables like speed, vehicle alignment, and annoying sounds. Improved performance is attained in the suggested model by the use of amplified feedforward layers

3.3.1 Radial Bias Neural Network (RBNN)

This research practises ada-boost boosted, a method based on very advanced learning machines, to make feed-forward layers work better. To improve the boosting technique's classification precision, the XG-boosting algorithm is used. When used to improve poor classifiers, the XGboost approach aggressively updates weights until models achieve optimal classification/prediction accuracy with minimal overhead in terms of memory and processing time. Next, we'll break down the suggested network's boosting techniques pseudo code.

Algorithm-2 Pseudo Code for Xg-Boost Algorithm

Inputs (i/p) Models Training Sets $\{x_i,y_i\}$where $x=\{x_1, x_2, x_3, x_{5.....}x_n\}$ where n=no of input samples and y_i €(1,-1) where $y_i$is the label associate with x

Initialize D(k)=n

For k=1,2,.3,…….K

Train the weak classifier using the distribution D_k

Determine the error function, ek, in relation to the D(k) function.

$e_k = P_r(h_k(x_k$ is not equal to $y_k)$ where $h_k$is the hypo proposed work function

Choose $\alpha_k=0.5 \{\ln(1- e_k) / e_k\}$ where α_k is the weight of the h_k,

Reinitialize the weight with D_{k+1}

Determine the error function and repeat the step 5
If an error is smaller than e_k
After that, result is computed by $H(x)= sign(\sum \alpha_k h_k)$
End
End

3.3.2 Feedforwarded Layers

The model is trained using Feedforward layers inspired by the work of Extreme Learning Machines. The auto-tuning characteristic and use of a single hidden layer characterize the neural network type known as a Radial Bias Neural Network (RBNN). ELM shows better performance, faster processing, and less computing overhead when associated to other learning models such as "Support vector machines (SVM), Bayesian Classifier (BC), K-Nearest Neighbour (KNN), and even Random Forest (RF)."

This type of neural network only makes use of one hidden layer, and the tuning of this layer is optional. ELM outperforms other learning algorithms like SVM and RF while also being faster and requiring less processing power. The ELM has used the kernel function to improve its accuracy and speed. Auto-tuning features of bias weights and non-zero activation functions are two advantages of the ELM architecture. In [29], [30], its inner workings as an ELM are described in detail. The ELM's input feature maps are indicated by the symbol Eq (9)

$$X = F(F, P) \quad (9)$$

Let X represent the combined space-time features from the CNN and GRU layers, F represent the CNN's spatial features, and P represent the GRU's aspects of time
The output ELM function is represented by Eq. (10)

$$Y(n) = X(n)\beta = X(n)X^T(\frac{1}{C}XX^T)^{-1}O \quad (10)$$

Equation (11) provides the entire training that is provided by ELM.

$$S = \alpha(\sum_{n=1}^{N}(Y(n), B(n), W(n)) \quad (11)$$

The input feature maps are marked by X(n), the time matrix is β, which is explained by the Moore–Penrose generalised inverse theorem and shown by X^T, C is a constant, and B and W are the network's bias factors and weights with an activation function.

3.4 Proposed Model

In Fig. 3, we see the overall design of the suggested framework. To improve performance, the framework that has been offered is a hybrid learning framework that involves a significant amount of integration between the ELM frameworks and the Boosted learning algorithm. The suggested classifier is extremely robust because of the boosted learning model, which demonstrates its superior performance. As a result, the suggested estimate framework uses boosting to train the ELM's weights, hence increasing the model's accuracy on the training data. The suggested model takes as its input the data that is kept on the cloud. Classification results from an ELM may be calculated using the method described in Eq (4)

$$S = \alpha(\sum_{n=1}^{N}(Y(n), B(n), W(n)) \quad (12)$$

To proceed, the determined S is contrasted with the cutoff, which is shown in Equation (5).

$$S(t) == S \quad (13)$$

The boosting method changes the bias weights every time step if S is not the same as S (t). This is shown mathematically by Eqn. (6)

$$S(k+1) = \alpha(\sum_{n=1}^{N}\big(Y(n+k), B(n+k), W(n+k)\big) \quad (14)$$

$$Where\ k = 1,2,3, \dots \dots N-1\ until\ S == S(t)$$

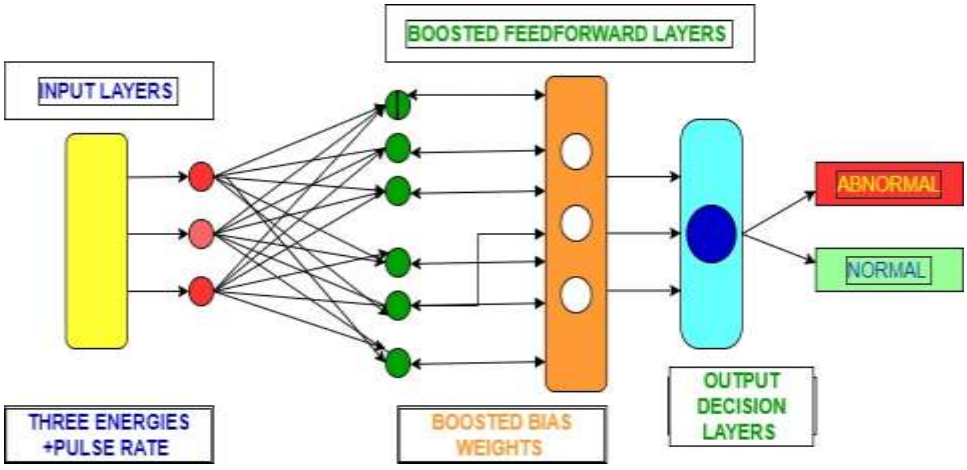

Figure 3: Network architecture of the suggested boosted model

4. Results and Analysis

This part looks at how well the suggested model works using the already-processed data that was gathered. Different activation functions are used on the model to get a better idea of the result. In Tab. 1, you can see the different performance measures that were used to find problems and rate the suggested model. One test and stopping method [31] is used to fix the overfitting problem of the network and make the issues with generalization better. This method can be used to stop training the suggested network when the evaluation presentation does not get better for N times in a row.

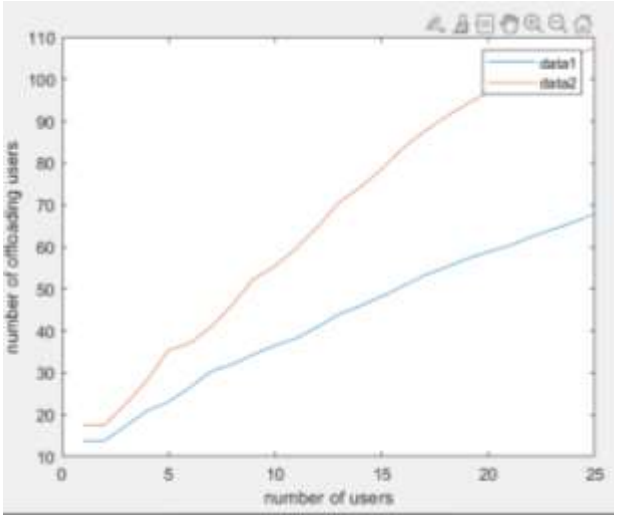

Figure 4: Number of Offloading users vs Number of users

The number of offloading users across various data sets is shown in Figure 4. Using the open-source Scikit-Learn Libraries, the whole model was constructed and run on a computer workstation equipped with an Intel I7 CPU, 16GB RAM, and a 3.5 gigahertz as the operational frequency. The performance measures' mathematical formulations are shown in Table 2.

Table 1: Instructional parameters that were used for the proposed model

Parameters	Specifications
Batch Size	20
No of Epochs	100
Testing data	30
Training data	70
Learning Rate	0.0001

Table 2: Formulas for the computation of performance metrics

Performance Metrics	Mathematical Expression
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$
Recall	$\frac{\text{TP}}{\text{T P+FN}}$ x100
Specificity	$\frac{TN}{TN + FP}$
Precision	$\frac{TN}{TP + FP}$
F1-Score	$2.\frac{Precison * Recall}{Precision + Recall}$

"FP for False Positive, FN for False Negative, TP for True Positive Values, and TN for True Negative Values"

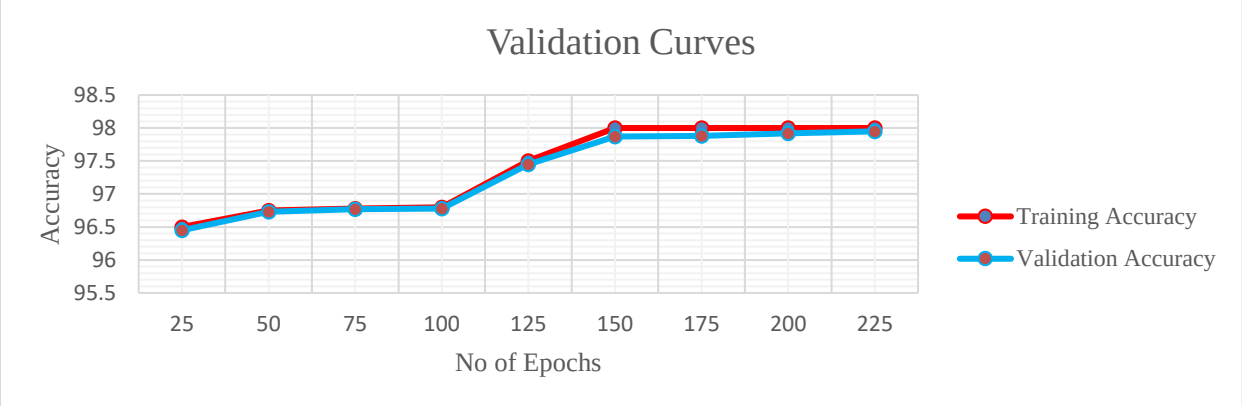

Figure 5: Validation performance for the proposed model in detecting normal condition

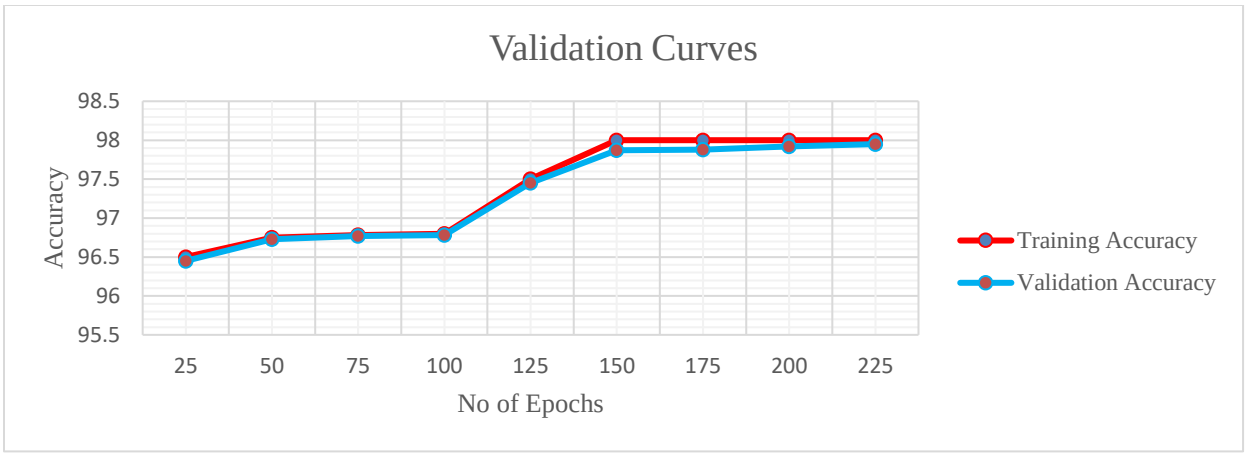

Figure 6: Authentication performance for the proposed model in detecting an abnormal condition

The validation performance of the suggested model in identifying human situations is shown in Figures 4 and 5. Based on the figures, it is evident that there is less than 0.001 error between the training and validation performance. The model's performance in terms of prediction and classification may be easily seen in a confusion matrix. The confusion matrix of the suggested model for determining the state of the body is shown in Figure 6.

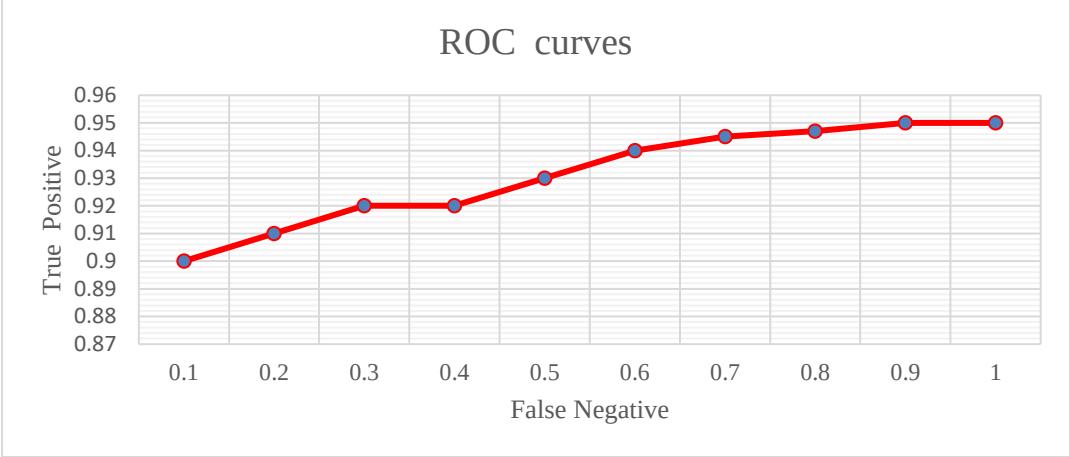

Figure 7: ROC performance for the Proposed Model optimization

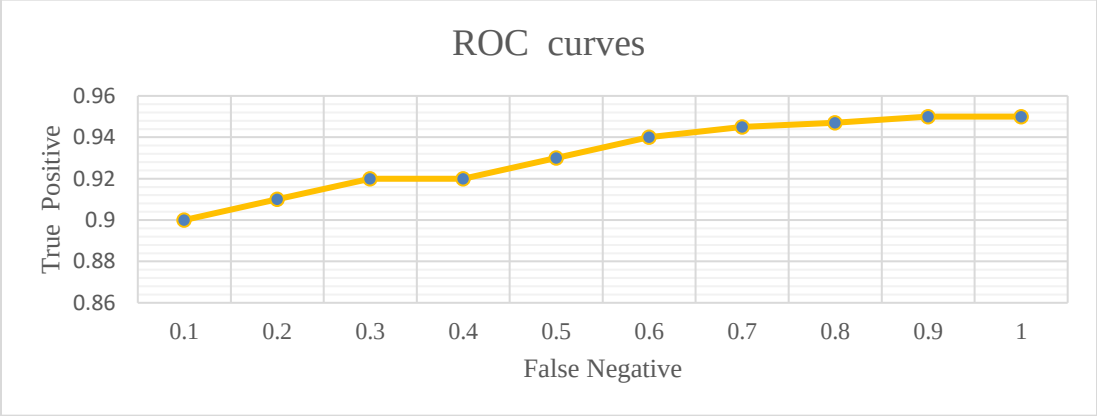

Figure 8: ROC performance for the Proposed Model in detecting the abnormal Conditions

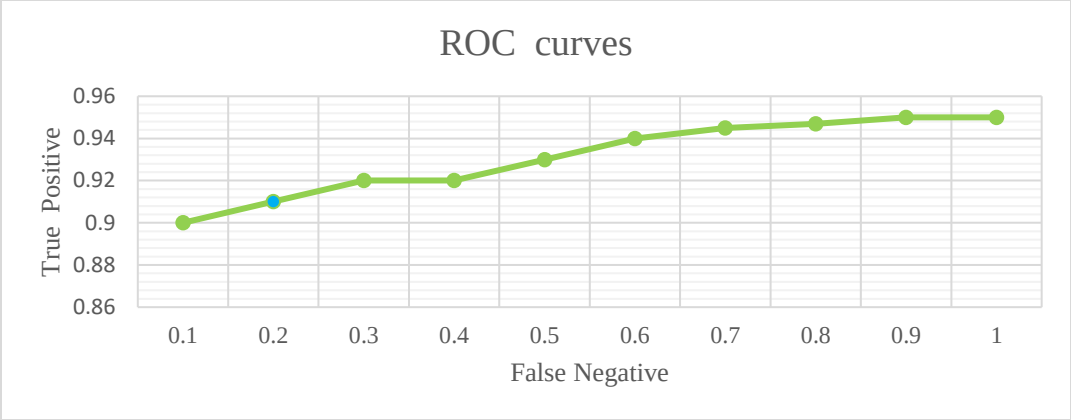

Figure 9: ROC performance for the Suggested Model in detecting the abnormal Condition

In identifying the three distinct body energies, Figures 7, 8, and 9 illustrate the suggested model's ROC performance. AUC (Area under Curve) of 0.975 and AUC of 0.96 in identifying the unusual situations are found to be maintained by the AUC for detecting the three energies.

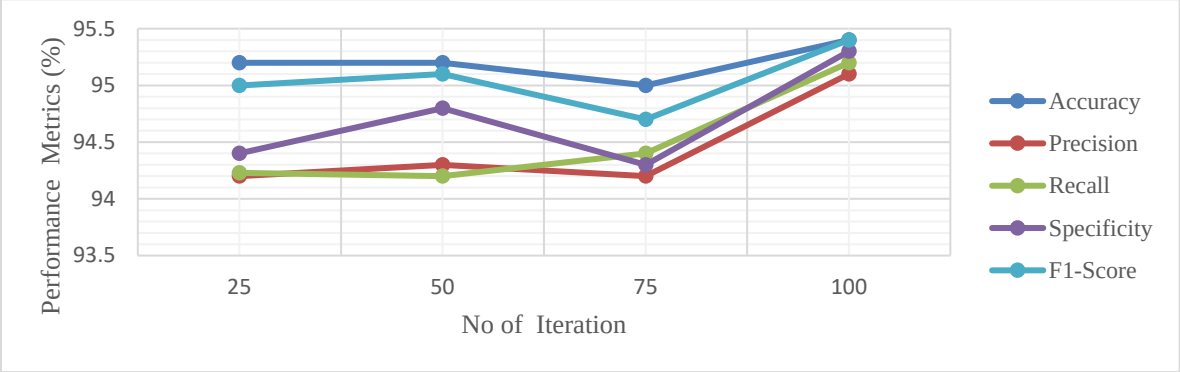

Figure 10: Performance Measurements with the Tanh Activation Function in the Suggested Model

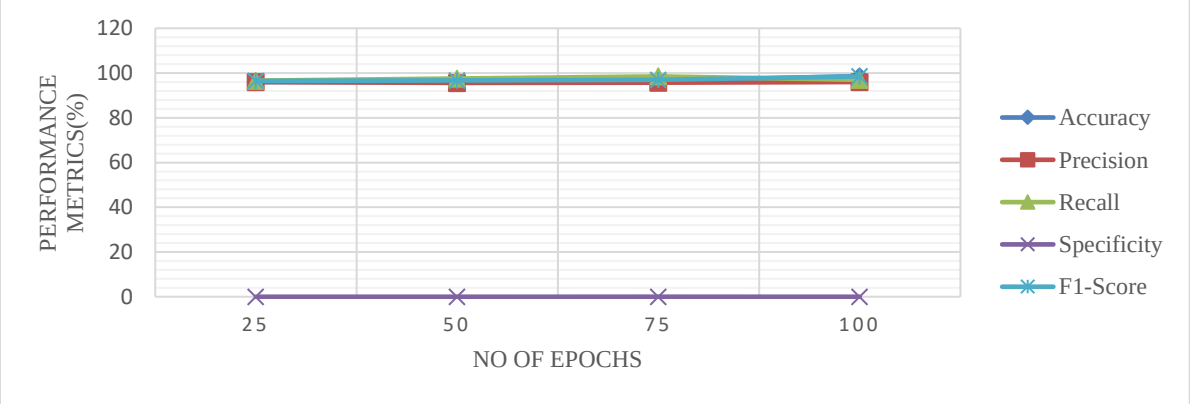

Figure 11: Efficiency Measures for the Proposed Model Employing the Relu Activation Function

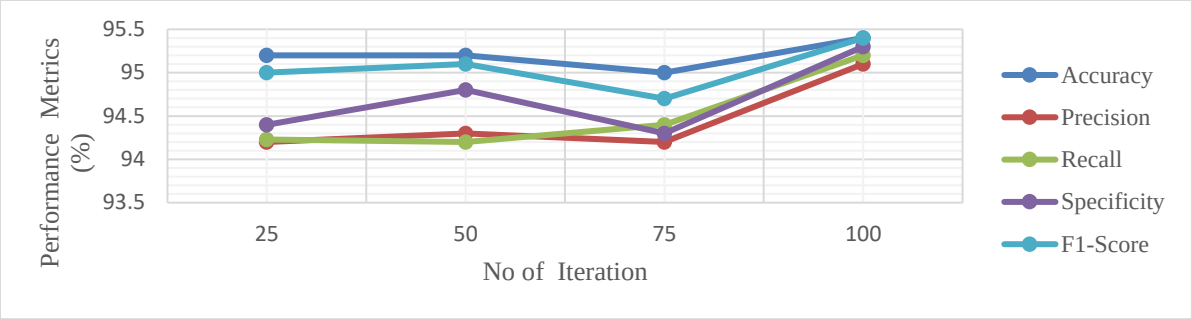

Figure 12: Evaluation of the Proposed Model's Effectiveness with the Sigmoidal Activation Function

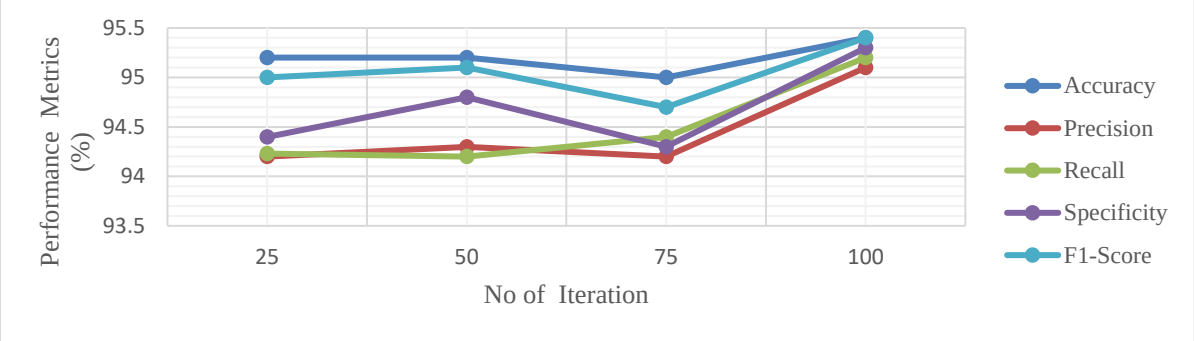

Figure 12: Analyses of the Proposed Model's Efficiency with the RBF Activation Function

Performance metrics are computed and various activation functions are used for model training in order to demonstrate the stability of the model. The suggested model's performance metrics with the various activation functions are shown in Figures 10, 11, 12, and 13. The performance of the suggested model has reached its maximum performance when ReLu is used as an activation function whereas other activation in the suggested model has produced a lesser performance compared to the other activation function.

Table 7: Examining the various algorithms' abilities to identify typical energies

Algorithms	Performance Metrics				
	Accuracy	Precision	Recall	Specificity	F1-Score
ANN	72.40	72.33	72.48	72.35	72.47
NB	68.20	67.90	68.20	67.30	67.90
ELM	89.10	88.56	88.40	88.70	88.20
RF	80.00	73.90	73.90	74.90	75.20
PROPOSED MODEL	95.10	95.20	95.00	95.10	95.12
KNN	82.00	81.20	81.00	80.20	80.30
BOOSTING ALGORITHM	78.40	77.20	79.40	78.30	78.20
SVM	88.20	87.92	86.93	87.50	88.20

Table 8: An analysis of the various algorithms' performance in identifying pitta disorder energies

Algorithms	Performance Metrics				
	Accuracy	Precision	Recall	Specificity	F1-Score
ANN	72.40	72.33	72.48	72.35	72.47
RF	80.00	73.90	73.90	74.90	75.20
KNN	82.00	81.20	81.00	80.20	80.30
PROPOSED MODEL	95.10	95.20	95.00	95.10	95.12
BOOSTING ALGORITHM	78.40	77.20	79.40	78.30	78.20
SVM	88.20	87.92	86.93	87.50	88.20
ELM	89.10	88.56	88.40	88.70	88.20
NB	68.20	67.90	68.20	67.30	67.90

Table 9: Examination of the various algorithms' abilities to identify emergency situations

Algorithms	Performance Metrics				
	Accuracy	Precision	Recall	Specificity	F1-Score
ANN	72.40	72.33	72.48	72.35	72.47
NB	68.20	67.90	68.20	67.30	67.90
PROPOSED MODEL	95.10	95.20	95.00	95.10	95.12
SVM	88.20	87.92	86.93	87.50	88.20
RF	80.00	73.90	73.90	74.90	75.20
KNN	82.00	81.20	81.00	80.20	80.30
BOOSTING ALGORITHM	78.40	77.20	79.40	78.30	78.20
ELM	89.10	88.56	88.40	88.70	88.20

Table 10: Examination of the various algorithms' abilities to identify emergency situations

Algorithms	Performance Metrics				
	Accuracy	Precision	Recall	Specificity	F1-Score
RF	80.00	73.90	73.90	74.90	75.20
ANN	72.40	72.33	72.48	72.35	72.47

KNN	82.00	81.20	81.00	80.20	80.30
NB	68.20	67.90	68.20	67.30	67.90
SVM	88.20	87.92	86.93	87.50	88.20
BOOSTING ALGORITHM	78.40	77.20	79.40	78.30	78.20
ELM	89.10	88.56	88.40	88.70	88.20
PROPOSED MODEL	95.10	95.20	95.00	95.10	95.12

Tables 7, 8, 9, and 10 present the comparative analysis of the distinct algorithms in classifying the disorders based on three energies and normal conditions, in all cases, the proposed model and ELM have produced good performances in classifying the different doshas and normal conditions, But the integration of Boosted algorithm with the ELM has produced the better results when compared with the ELM. Additionally, the suggested model has done better than the others and is the most suitable for the Ayurvedic diagnosis system.

5. Conclusion

In this research, we have designed IDS using different techniques; firstly we designed IDS to detect selective forwarding and sinkhole attacks using KMA with hash value and CBA with path matrix mechanisms. KMA scheme detects threats (selective forwarding and sinkhole attack) using the concept of shared keys among the nodes in the system. The message is furthered to the next node after verification of the data using a shared key basis. If the keys mismatch, then the data is dumped otherwise passed on to the next node. On the other side, using the CBA scheme, the entire network is distributed in a variety of clusters and the Cluster Head receives a message instead of the normal node. This process guides to rise in the entire performance of the network. Secondly, an ensemble intrusion detection model for IoT networks has been designed using SVM and DNN. The IDSs are used to detect the different kinds of assaults comprising DDoS and Replay attacks. Many intrusion detection mechanisms already have been presented by researchers but we need to consider multiple attacks that are capable of distinguishing unknown and known assaults. The research work also describes a set of classification algorithms to detect and prevent the network from intrusions and provides a better idea about the impact of classifiers on intrusion detection mechanisms. Here, SVM is used to find the suspicious path in the network whereas DNN is used for detection of the suspicious node list out of suspicious paths considered by the SVM in the network. In the third scenario, hybridization of the classification approach is used to detect multiclass attacks in the IoT network by utilizing the concept of PCA to extract the useful feature pattern of nodes in the network with LDA to reduce the high dimension feature into lower dimension space by considering only a set of important features. Then, the hybrid neural network with SVM as a classifier is used to enhance the rate of detection and lessen the FAR rate in the system.

Conflicts of Interest declaration

No conflict of interest is declared by the authors.

References

[1] Munqith Saleem, Hanan Burhan Saadon, Marwa S. Mahdi Hussin,Tamarah Alaa Diame, Raaid Alubady, Mohd K. Abd Ghani, Hatıra Günerhan, Application of Edge Computing-Based Information-Centric Networking in Smart Cities, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 2 , (2023) : 72-85 (Doi : https://doi.org/10.54216/JISIoT.080208)

[2] Mohammad Hammoudeh,Saeed M. Aljaberi, Modeling of Deep Learning based Intrusion Detection System in Internet of Things Environment, Journal of Cybersecurity and Information Management, Vol. 8 , No. 1 , (2021) : 17-25 (Doi : https://doi.org/10.54216/JCIM.080102)

[3] Basma M. Yousef,Germien G. Sedhom,Alshimaa H. Ismail, U-Shape Wideband Slot Antenna for 5G Mobile Phone Applications, International Journal of Wireless and Ad Hoc Communication, Vol. 5 , No. 2 , (2022) : 77-83 (Doi : https://doi.org/10.54216/IJWAC.050206)

[4] Y. Li et al., "Multiple mobile data offloading through delay tolerant networks", in Proc. of the 6th ACM workshop on Challenged networks (ACM CHANTS), 2011, pp. 43-48.
[5] Z. Li, C. Wang, S. Yang, C. Jiang and I. Stojmenovic, "Space-crossing: Community-based data forwarding in mobile social networks under the hybrid communication architecture", IEEE Trans. Wireless Commun., vol. 14, no. 9, pp. 4720-4727, Sep. 2015.
[6] D. Huang, P. Wang and D. Niyato, "A dynamic offloading algorithm for mobile computing", IEEE Trans. Wireless Commun., vol. 11, no. 6, pp. 1991-1995, Jun. 2012.
[7] L. Valerio, R. Bruno and A. Passarella, "Adaptive data offloading in opportunistic networks through an actor-critic learning method", in Proceedings of the 9th ACM MobiCom workshop on Challenged networks (ACM CHANTS), Sep. 2014, pp. 31-36..
[8] B. Han et al., "Mobile data offloading through opportunistic communications and social participation", IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 821-834, May 2012.
[9] M. Ghorbani, H. R. Rabiee, and A. Khodadadi, "Bayesian overlapping community detection in dynamic networks", arXiv preprint arXiv:1605.02288, 2016.
[10] S. Andreev, A. Pyattaev, K. Johnsson, O. Galinina and Y. Koucheryavy, "Cellular traffic offloading onto network-assisted device-to-device connections", IEEE Commun. Mag., vol. 52, no. 4, pp. 20-31, Apr. 2014. 106
[11] B. Han, P. Hui, V. Kumar, M. V. Marathe, G. Pei and A. Srinivasan, "Cellular Traffic Offloading through Opportunistic Communications: A Case Study", in Proc. of the 5th ACM workshop on Challenged networks (ACM CHANTS 2010), Sep. 2010, pp. 31-38.
[12] L. Valerio, R. Bruno and A. Passarella, "Cellular traffic offloading via opportunistic networking with reinforcement learning", Computer Communications, vol. 71, pp. 129-141, 2015.
[13] Ackerman, Eyal, Oren Ben-Zwi, and Guy Wolfovitz, "Combinatorial model and bounds for target set selection", Theoretical Computer Science, vol. 411, no. 44-46, pp. 4017-4022, 2010.
[14] W. Liu, W. Gong, W. Du and C. Zou, "Computation offloading strategy for multi user mobile data streaming applications", in 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 111-120.
[15] F. Rebecchi, M. D. de Amorim, V. Conan, A. Passarella, R. Bruno and M. Conti, "Data offloading techniques in cellular networks: A survey", IEEE Commun. Surveys Tuts., vol. 17, no. 2, pp. 580-603, 2nd Quart. 2015.
[16] G. Gao, M. Xiao, J. Wu, K. Han and L. Huang, "Deadline-sensitive mobile data offloading via opportunistic communications", in Proc. 13th Annu. IEEE Int. Conf. Sens. Commun. Netw. (SECON) , 2016, pp. 1-9.
[17] V. Srinivasan, M. Motani and W. T. Ooi, "Analysis and Implications of Student Contact Patterns Derived from Campus Schedules", in Proc. The 12th ACM International Conference on Mobile Computing and Networking (MOBICOM'06), 2006, pp. 86-97.
[18] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft and C. Diot, "Pocket Switched Networks and Human Mobility in Conf. Environments", in Proc. ACM Special Interest Group Data Comm. Workshop (SIGCOMM '05), 2005.
[19] N. Eagle, A. Pentland and D. Lazer, "Inferring social network structure using mobile phone data", Proc. Nat. Acad. Sci., vol. 106, no. 36, pp. 15274- 15278, Sep. 2007.
[20] J. Orimolade and N. Ventura, "Intelligent access network selection for data offloading in heterogeneous networks" in AFRICON 2015, 2015, pp. 1-5. 107
[21] J. Jiang, S. Zhang and B. Li, "Maximized cellular traffic offloading via device-to-device content sharing", IEEE J. Sel. Areas Commun., vol. 34, no. 1, pp. 82-91, Jan 2016.
[22] D. Kempe, J. M. Kleinberg and E. Tardos, "Maximizing the spread of influence through a social network", Theory of Computing, vol. 11, no. 4, Apr 2015.
[23] V. Gupta and M. K. Rohil, "Mobile data offloading: Benefits issues and technological solutions", in International Conference on Computer Science Engineering & Applications (ICCSEA), May 2012, pp. 73-80.
[24] K. Lee, J. Lee, Y. Yi, I. Rhee and S. Chong, "Mobile data offloading: How much can WiFi deliver ?", IEEE/ACM Trans. Netw., vol. 21, no. 2, pp. 536- 550, Apr. 2013.
[25] S. Hoteit et al., "Mobile data traffic offloading over passpoint hotspots", Comput. Netw., vol. 84, no. 19, pp. 76-93, Jun. 2015