International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Energy-Efficient Bio-Inspired Hybrid Deep Learning Model for Network Intrusion Detection Based on Intelligent Decision Making

[1]Dr. Sandeep Kumar Hegde, [2]Dr. P. William, [3]Dr. Mule Shrishail Basvant, [4]A. Deepak, [5]Arti Badhoutiya, [6]A L N Rao, [7]Amit Srivastava, [8]Dr. Anurag Shrivastava

Submitted: 10/12/2023 **Revised**: 14/01/2024 **Accepted**: 31/01/2024

Abstract: This study presents an energy-efficient, hybrid deep learning model for network intrusion detection that takes its cues from biology. As a result, intelligent decision-making is included into the improvement of security infrastructures. The model's high accuracy is shown by the fact that it performs well across a variety of metrics, including TPR, precision, and F-Measure, thanks to the use of deep learning and techniques inspired by biology. Despite the fact that there is some unpredictability in FPR and FNR, the data demonstrate that the model is capable of providing a long-term and intelligent response to the ever-changing cybersecurity threats

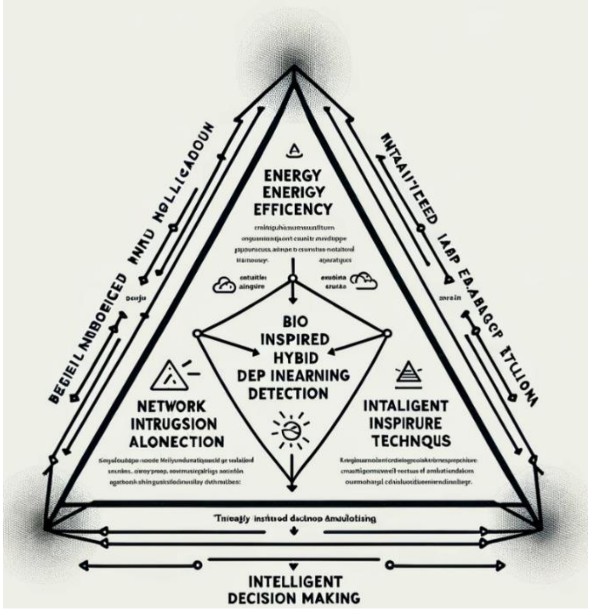
Keywords: *Network Security, Bio-Inspired Algorithms, Hybrid Deep Learning, Energy Efficiency, Intelligent Decision Making, Resource Optimization, Computational Efficiency, Anomaly Detection, Deep Learning.*

1. Introduction

Network security is of the utmost importance in this day and age of widespread digital communication and interconnected devices. As organisations become more reliant on the uninterrupted flow of information, the threat landscape for network intrusions is always shifting to accommodate the increased vulnerability it presents. These security flaws are growing increasingly difficult to uncover as they become more complicated [1]. Because these dynamic threats typically move at a pace that is too quick for standard intrusion detection systems to keep up with, innovative and adaptable solutions are necessary. This paper proposes a novel approach to improving the efficiency and precision of network intrusion detection by merging bio-inspired approaches with intelligent decision-making processes. This approach was developed as part of this study. By combining the strengths of deep learning and bio-inspired algorithms, this hybrid model makes an effort to enhance detection capabilities while simultaneously addressing the growing issue of energy consumption, which is an essential consideration in contemporary computer environments.

The capability of the natural world to adapt and improve is the source of inspiration for the bio-inspired element of the model that has been offered. The simulation of biological processes, such as those found in the neural networks of the human brain, sets the framework for the development of an intrusion detection system that is more resilient and dynamic. This bio-inspired component makes advantage of the capability of neural networks to recognise complicated patterns and irregularities in network traffic data by using its seamless integration with a deep learning framework [2]. Concurrently, the use of complex decision-making procedures is necessary in order to achieve the highest possible level of energy efficiency using the hybrid model. Using complex decision-making algorithms, the system is able to dynamically allocate resources, prioritise tasks, and modify the intensity of its processing in line with the perceived level of risk. These capabilities allow the system to respond more quickly to potential threats. This astute utilisation of available resources not only ensures that the intrusion detection system will function to its full potential when put to use in real-time but also contributes to the reduction of overall energy consumption [3].

[1]*Associate Professor, Department of Computer Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, Karnataka*
sandeep.hegdey@gmail.com
[2]*Department of Information Technology, Sanjivani College of Engineering, Kopargaon, SPPU, Pune*
**william160891@gmail.com*
[3]*Associate Professor, Department of Electronics &Telecommunication Engineering,*
Sinhgad College of Engineering, Pune-41
**mulesb1@gmail.com*
[4]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu*
deepakarun@saveetha.com
[5]*Department of Electrical Engineering, GLA University, Mathura*
arti.badhoutiya@gla.ac.in
[6]*Lloyd Institute of Engineering & Technology, Greater Noida*
dean.engineering@liet.in
[7]*Lloyd Law College, Greater Noida*
amit@lloydlawcollege.edu.in
[8]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu*
**anuragshri76@gmail.com*



The primary objective of this research is to develop a cutting-edge method that is both all-encompassing and capable of providing an answer to the growing need for computing that is less taxing on the environment while at the same time enhancing the precision of network intrusion detection. This creative new finding, which is a hybrid deep learning model, offers potential for increasing the resilience and sustainability of network security systems. It blends bioinspired principles with intelligent decision making. This graphic depicts a conceptual framework in the form of a triangle that is backed by intelligent decision-making mechanisms [4]. It includes the three most important parts of a network intrusion detection system (NIDS), which uses a hybrid kind of deep learning that is modelled after the way biological processes function. One of the following fundamental concepts is symbolised by each point that makes up the triangle's vertices:

- **Energy Efficiency:** At this vertex, the framework emphasizes the importance of optimizing the deep learning model to consume minimal energy, ensuring the system's sustainability and cost-effectiveness. It suggests the incorporation of mechanisms to reduce computational load and power usage while maintaining high detection accuracy.
- **Bio-inspired Hybrid Deep Learning Detection:** This point illustrates the core of the model's architecture, combining bio-inspired computational techniques with deep learning. This hybridization aims to exploit the adaptability and efficiency of biological models in tandem with the robust feature learning capabilities of deep learning, particularly for complex pattern recognition tasks in network traffic.
- **Intelligent Decision Making:** The third vertex represents the decision-making prowess of the system. It indicates the use of intelligent algorithms that can make autonomous, real-time decisions about potential threats. This involves analyzing the patterns learned by the deep learning model to accurately identify and respond to anomalous network behavior indicative of cyber threats.

The vertices lead to a cooperative system where increased learning and detecting skills are strengthened by energy-efficient processing, which makes it easier to make intelligent decisions [5]. The end objective of this all-encompassing approach is to develop a network intrusion detection system (NIDS) that is not only efficient and adaptable, but also robust and able to withstand the constantly shifting nature of the cyberthreat environment.

2. Review of Literature

It is imperative that problems with intrusion detection be solved, despite the fact that doing so may put one in harm's way and be difficult. The sheer number of intrusions that take place on a daily basis in different parts of the globe is one of the primary reasons why the concept of intrusion detection has seen such a meteoric rise in popularity over the last few years. This trend has been one of the primary drivers behind the rapid growth of intrusion detection. This pattern has been prevalent for a good number of years now. When developing a multilayered, genetically optimized feature selection technique for the purpose of intrusion detection, the findings of the research were taken into account. In order to successfully construct this system, it was absolutely necessary to make use of the very helpful insights that may be gained from the biological sciences. In addition, the proposed multilayer model consists of two distinct layers, which are designated as layer 1 and layer 2 accordingly [6]. These statistics provide an indication of the many different levels that are available. These numbers provide a notion of the large variety of levels that are available to the user. These examples provide a sense of the large variety of options from which the user may pick. At the layer 1 level, the process of handling feature selection is handled using a combination of three distinct methodologies that are merged and employed in tandem. Particle Swarm Optimization (PSO), Grey Wolf Optimization (GWO), and Firefly Optimisation Algorithm (FFA) are the names that have been given to the methodologies that have been implemented. After the initial layer of data has been carefully investigated, a priority value will be assigned to each feature set. When deciding which feature set to use, a genetic algorithm (GA) that has been upgraded takes into account the priority value. This is the second level of the model that has been proposed. Modifications have to be implemented into the standard GA in order to achieve optimization and bring it into agreement with the model that has been outlined. During the training phase, a value is assigned to each and every set of criteria that the Optimised GA takes into consideration. This number demonstrates the relative relevance of each set of criteria by comparing them. In addition, the priority values are separated into three distinct groups based on the three levels, which are high, medium, and low. During the testing phase of the project, an Optimised Generalization Algorithm (GA) is used to choose a feature set depending on the degree to which the various components being evaluated are connected to one another. To increase the likelihood that the feature set will be chosen, we are going to give it the highest priority and focus all of our attention on it. This will increase the likelihood that it will be chosen. As a direct consequence of this fact, the possibility of its being chosen will increase. The inclusion of this information will directly increase the possibility that it will be chosen. At the end of phase 2, depending on whether or not it is necessary, the feature set priority may be reevaluated and adjusted based on the defined feature priority and the F-measures that were generated from it. This will rely on whether or not the feature is needed. This will change depending on what it requires. When deciding which features to use, the capability of the proposed model to include newly obtained data and adjust the priority hierarchy of existing feature sets will be taken into consideration. These articles include profiles of the researchers who carried out the inquiry making use of two datasets that are available to the general public as data sources. NSL-KDD is the name of the second dataset, while UNSW-NB15 is the name of the first dataset. Both datasets were obtained from the National Spatial Data Infrastructure. These datasets were accessible via the National Spatial Data Infrastructure, amongst other places, as well as other sites. In addition to being accessible via a plethora of other websites, these datasets could also be available via the National Spatial Data Infrastructure. Assessments are conducted using a wide variety of criteria, some of which include the F-Measure, accuracy, and recall. The findings of the study point to the conclusion that the technique of using an intrusion detection system has a lot of potential, which is particularly interesting considering that a model was employed to evaluate it.

An intrusion detection system (IDS), often referred to as a network intrusion detection system, is used to identify and halt a variety of malicious programming activities and assaults on computer networks. This sort of system is commonly known as an intrusion detection system (IDS). In order to help with this, an IDS is used. When it comes to this particular criteria, firewalls often do not live up to the expectations that are placed upon them. Selecting each component that will be included in a network intrusion detection system is one of the processes that must be performed in order to develop a system that is trustworthy. This is one of the procedures that must be taken. This is one of the things that needs to be done in order to proceed. In order to differentiate between normal and abnormal network traffic, many bio-inspired metaheuristic algorithms are used. These algorithms are designed to cut down on the number of features they consider while simultaneously boosting their processing speed and precision. These methods are designed to improve accuracy while simultaneously cutting down on the number of observable characteristics that have to be taken into consideration. The purpose of this research is to develop a cutting-edge hybrid model that can be used to a variety of network intrusion detection system setups. This model is built on a combination of metaheuristic algorithms that were patterned after biological processes and were inspired by the activities that were stated before. Because of this, it will be able to recognize the all-encompassing attack. The primary objective of the approach that is being suggested is to bring the total number of qualities that need to be selected for the Network Intrusion Detection System down to a level that is more manageable for the individuals who are in charge of the system. Combining the bioinspired metaheuristic algorithms that were originally developed independently into a single system is necessary in order to accomplish this objective and produce a hybrid model. Moth-flame optimization (MFO), also known as whale optimisation algorithm (WOA) and firefly algorithm (FFA), multiverse optimisation (MVO), particle swarm optimisation (PSO), grey wolf optimisation (GWO), and bat algorithm (BAT) were some of the other optimization approaches that were used in this research. Using classifiers that have been produced using machine learning, the secondary objective is to determine the kind of general attack. In order to accomplish this objective, the support vector machine (SVM), the random forest (RF), and the C4.5 (J48) decision tree classifiers were used. An experiment was carried out using the dataset that was provided by UNSW-NB15 in order to establish whether or not the proposed hybrid model had any practical use. The UNSW-NB15 dataset, which was compiled using information that was easily accessible, includes nine unique categories of attacks in all. When compared to the other alternative attack techniques, the wide assault has shown to be the most effective attack strategy. Because locating other attacks like it was the primary objective of the recently devised approach, doing so was very essential. When compared to the SVM and the RF, the J48 classifier is by far the choice that allows me to construct models in the shortest amount of time. This is the case since it uses a radial basis function. Before deciding to take this course of action, we deliberated over the data and shared our conclusions with one another. My research lead me to discover that the MVO-BAT model could be able to decrease the total number of features from 48 to 24, while still maintaining the same accuracy, sensitivity, and F-measure for each individual feature across all classifiers [7]. In contrast, the MFO-WOA and FFA-GWO models displayed F-measures, accuracy, and sensitivity that were equivalent to one another, despite the fact that they were restricted to using just 15 characteristics for each feature that was used in the classification. The fact that this was the case remained unchanged despite the fact that both models were limited to using 15 characteristics for each feature. Now that these models can explain a considerable number of the cases of each feature, this is an alternative that might be taken into account and it is recommended that it be investigated further.

The "Internet of Things" (IoT) is a term that refers to a network of linked, stand-alone devices that may interact with one another and share data with one another throughout the course of wireless networks. It is feasible for these devices to communicate with one another and share a variety of data types with one another. These many different kinds of tools are referred to together as "things." These gadgets are able to grasp data, keep an eye on their surroundings, and communicate not just with other electronic devices but also with machines and the outside world. The bar for what constitutes an adequate degree of security in a given system is steadily being raised as more and more Internet of Things devices get ingrained in the routines of regular people. As a direct consequence of this, it is projected that the standards for the level of safety that must be met by these systems will continue to become more stringent. Hackers are attracted to devices that are connected to the Internet of Things (IoT) because of the possibility that these gadgets may be used for malicious purposes and infect the network that is beneath them. The objective of the research project that has been allocated to you is to protect the architecture of the Internet of Things by combining an intrusion detection system (IDS) with a technology that is biologically inspired. The hybridized sine-cosine algorithm (SCA) and the salp swarm algorithm (SSA) are the two methods that are used in the process of determining the primary components that are present in network traffic. A machine learning (ML) classifier is fed a fraction of the data that is presently accessible in order to detect and categorize undesirable traffic. In a setting that is based on Python, an investigation is carried out using a dataset that contains intrusions into networks that are connected to the Internet of Things [8]. This evaluation determines the level of success that can be expected from the strategy that has been outlined. When it comes to identifying breaches in the Internet of Things, the hybridized system that was proposed has the quickest reaction time (96.42 seconds), the fewest characteristics (eight), and the highest accuracy (84.75 percent). The efficacy of the methodology may be evaluated by contrasting it with a variety of different multiclass categorization approaches that are conceptually equivalent to its own.

Studies on computer security have demonstrated that one of the most important measures in ensuring that the unbroken integrity of such systems is maintained at all times is to identify and detect unauthorized attempts to access computer systems. This is because such efforts threaten the continuity of the integrity of such systems. Additionally, in order to optimize the capabilities of intrusion detection and boost the efficiency of the process, one must give a great deal of thought and attention to the selection of the attributes to look for. Using a unique strategy that is based on hybrid feature selection, the purpose of this study is to identify and locate areas that have been invaded. Recently, an update was implemented into the model, and as a result, the optimization strategies known as Particle Swarm Optimization (PSO) and Grey Wolf Optimization (GWO) were able to be included into it. In addition to this, the authors of the paper provide two models, each of which is entirely unique: one for feature selection, and the other for intrusion detection. These two models are referred to by their respective names, which are the PSO-GWO-NB and the PSO-GWO-ANN, respectively. Both of these models were designed by PSO. PSO and GWO both provide outputs for emerging feature selection that may be used to a wide variety of activities and goals. These outputs can be utilized alone or in combination. This is the case due to the fact that each of these optimization strategies provide emergent feature selection. In the context of this particular research topic, the PSO and GWO algorithms are used in order to assist with the process of selecting the characteristics to be included in an intrusion detection system. In addition to that, this work presents an original strategy for the selection of emergent features. The interstation of PSO and GWO features is the basic principle that underpins this technique. In addition, the Most Recurring Features (MRF) from both PSO and GWO are investigated as part of this research. MRF is an acronym that stands for "Most Recurring Features [9]." The user is at liberty to apply their own discretion in determining how many iterations of PSO and GWO were performed in total during the course of this research endeavor. At each and every selection attempt, a variety of feature selection models are used; the feature set that has been picked in its whole at the end of the procedure is the one that is retained. The next step in the process that has to be finished is an analysis of the properties of the MRF, the PSO, and the GWO, as well as the point at which the PSO and the GWO converge. The UNSW-NB15 dataset was used in the analysis that was carried out as a component of the overall research endeavor that was carried out. In addition, the investigation made use of not one but two separate kinds of classifiers, namely artificial neural networks (ANN) and naive bayesian networks (NB) (ANN). According to the findings, choosing between PSO and GWO as an intrusion detection feature is comparable to having to choose between two fantastic alternatives. In addition, the outcome with the fewest possible characteristics is the one that is produced when the PSO features and the GWO features are intersected as a consequence. One possible explanation for this is that both the PSO and GWO features have an inherent tendency to maximize efficiency. This is a direct result of the productive collaboration that has taken place between the PSO and the GWO. In addition, the MRF functions provide outcomes that are often consistent with the anticipations of the target audience [10]. The ability to correctly remember precise facts from memory is one of the prerequisites for carrying out the process of analyzing information. In addition to achieving a one hundred percent accuracy rate, there are a few more prerequisites that need to be satisfied. Some of these criteria include true positives, false positives, false negatives, and false negatives as well as true negatives. The findings of the research indicate that the MRF offers a number of benefits, two of which are the high levels of accuracy and recall that it has. In the end, the test results demonstrated that the PSO-GWO-NB classifier performed better than the PSO-GWO-ANN classifier when it came to the selection of features and the detection of intrusions.

3. Bio-Inspired Vs. Traditional Intrusion Detection Models

Bio-inspired intrusion detection models, as opposed to regular intrusion detection models, which are either rule-based or signature-based and lack such flexibility, strive to emulate the flexible and efficient properties of biological systems. regular intrusion detection models are either rule-based or signature-based. This mind map provides a pictorial comparison between the features of traditional intrusion detection systems and bio-inspired methods of intrusion detection approaches. The bio-inspired method, which can be seen on the left side of the mind map, proposes a model that makes use of deep learning techniques in conjunction with biological principles in order to achieve increased flexibility and energy efficiency. It places a focus on self-learning capabilities, operational efficiency, and the ability to spot abnormalities in network data.

Fig 1: Dual Approach: Bio-Inspired Vs. Traditional Intrusion Detection

On the right-hand side of the mind map, you can get a comprehensive description of the standard models. These models differ in that they depend on pre-established criteria and signature matching for detection, which may lead to wasteful use of resources and maybe less flexibility in recognising fresh and complex cyberthreats. Alternatively, these models may be able to identify cyberthreats more effectively. It's possible that making use of machine learning techniques will help mitigate some of these drawbacks. This dual approach mind map illustrates the progression from rule-based, static detection approaches to more dynamic, intelligent decision-making systems that are able to adapt to and learn from new security risks. These systems may be seen as an evolution from rule-based detection techniques. The discovery of new dangers may cause these systems to undergo a process of adaptation.

- **Bio-Inspired Intrusion Detection Models:**
  - ***Adaptability:*** These models can evolve and adapt in real-time to new threats, much like organisms adapt to their environment. They often use algorithms inspired by natural processes, such as genetic algorithms or neural networks, to continually learn and improve their detection capabilities.
  - ***Efficiency:*** Bio-inspired models aim for efficient computation, often using parallel processing techniques similar to neural pathways in the brain, which allows them to handle large volumes of network data with lower energy consumption.
  - ***Anomaly Detection:*** Instead of relying on known signatures, bio-inspired models can detect anomalies by learning what normal behavior looks like and then identifying deviations, which is particularly effective against zero-day threats.

- **Traditional Intrusion Detection Models:**
    - ***Rule-Based:*** Traditional models often use predetermined rules or patterns (signatures) to identify threats. While effective for known attack vectors, they struggle to identify new or modified threats that do not match the existing rules.
    - **Resource Intensive:** They can be resource-intensive, as they require constant updates to their signature databases and can consume significant computational power to match patterns in network traffic.
    - ***Limited Adaptability:*** Traditional models have limited adaptability; they do not inherently learn or evolve and thus require manual updates to their detection mechanisms to handle new types of attacks.

The presents an approach to the construction of a system that is capable of combining the effectiveness and adaptability of bio-inspired models with the capability of deep learning to analyse structured data. The capacity to manage network data in an energy-efficient way is essential for long-term, sustainable operation, which is something that this hybrid technology can deliver thanks to its astute decision-making capabilities. A potential for cost reduction may also be associated with the hybrid approach. In addition to this, it is able to react on its own to a variety of different cyberattack situations, including those that include highly complex and cutting-edge online dangers.

4. Research Methodology

This article presents a research approach that generates a new network intrusion detection system (NIDS) by combining bio-inspired algorithms with deep learning methods. This methodology was described in this article. This procedure was broken out in detail in the aforementioned article. Within the scope of this research was a debate pertaining to this methodology. As an immediate consequence of this change, there will be a reduction in the amount of energy required for detection, along with an improvement in both throughput and accuracy. This study evaluated a hybrid deep learning model that is capable of detecting network intrusions, takes inspiration from biology, and uses less energy than traditional models of deep learning. The results of the experiment are summarised in Table 1 which can be found further down. The paradigm integrates ideas derived from biological systems and lays a significant emphasis on intelligent decision-making as its central theme. In order to provide a comprehensive analysis, it is essential to include a wide variety of different indications into the presentation. A few examples of these metrics are the True Positive Rate (TPR), the False Positive Rate (FPR), the False Negative Rate (FNR), the Precision, the Recall, and the F-Measure. In the following, some examples of these metrics are provided. Each fold provides a unique and separate perspective on the overall performance of the model.

Table 1: Performance Metrics of Energy-Efficient Bio-Inspired Hybrid Deep Learning Model for Network Intrusion Detection Based on Intelligent Decision Making

Experiment	True Positive Rate (TPR)	False Positive Rate (FPR)	False Negative Rate (FNR)	Precision	Recall	F-Measure
Fold 1	0.882	0.132	0.134	0.863	0.836	0.823
Fold 2	0.837	0.134	0.143	0.823	0.866	0.832
Fold 3	0.827	0.135	0.124	0.865	0.862	0.873
Fold 4	0.867	0.143	0.178	0.822	0.873	0.862
Fold 5	0.878	0.127	0.187	0.845	0.852	0.872
Fold 18	0.965	0.034	0.017	0.946	0.856	0.952
Fold 19	0.977	0.078	0.198	0.642	0.854	0.963
Fold 20	0.946	0.017	0.173	0.962	0.835	0.973
Fold 21	0.923	0.008	0.176	0.943	0.822	0.982
Fold 22	0.954	0.078	0.195	0.962	0.851	0.923

Table 1 displays the results of experiments conducted on an energy-efficient hybrid deep learning model for network intrusion detection that takes its cues from biology. The model contains sophisticated decision-making algorithms to replicate the operation of cognitive systems in order to accurately represent such systems. The evaluation metrics that were compiled from a number of different folds provide evidence of the degree of accuracy with which the application can identify intrusions. It is noticeable that there is a huge potential for prediction as evidenced by the high True Positive Rates and Precision measurements. This is something that should be taken into consideration. Alterations in the rates of false positives and false negatives, on the other hand, call attention to the need for more optimisation. The F-Measure, which combines precision and recall, is a good indicator of the model's overall accuracy and balance when it comes to the detection of intrusions. The table is a helpful instrument that can be used to assess the efficacy of the recommended energy-efficient bio-inspired model as well as its potential to boost network security. This evaluation can be done by using the table. The following are some of the steps in this process that are among the most important:

❖ **Development of a Hybrid Model:**

The core of the methodology is to develop a hybrid intrusion detection model that combines bio-inspired computational techniques with deep learning. This model draws inspiration from natural processes, mimicking neural mechanisms similar to those in the human brain. The goal is to create a system that can adapt and learn in real-time, improving its ability to detect new and sophisticated network threats.

❖ **Feature Selection Using Bio-Inspired Algorithms:**

A multilayer feature selection approach is implemented using algorithms such as Particle Swarm Optimization (PSO), Grey Wolf Optimization (GWO), Firefly Optimization Algorithm (FFA), and an optimized Genetic Algorithm (GA). These algorithms help in selecting the most relevant features from network traffic data, which are crucial for accurate intrusion detection. The feature sets are prioritized based on their relevance and effectiveness in detecting intrusions.

❖ **Integration with Deep Learning:**

The selected features are then fed into a deep learning framework. This framework is designed to analyse intricate patterns and anomalies in network traffic, learning from the data to enhance its detection capabilities. The deep learning component works in tandem with the bio-inspired feature selection, creating a robust detection mechanism.

❖ **Intelligent Decision Making for Resource Optimization:**

Alongside detection, the model incorporates intelligent decision-making mechanisms to optimize energy efficiency. These mechanisms allocate computational resources dynamically, prioritize tasks, and adapt processing intensity based on the level of detected threat, ensuring minimal energy consumption while maintaining high detection accuracy.

❖ **Evaluation and Testing:**

In the process of validating the model, typical datasets serve as test subjects. These datasets include UNSW-NB15 and NSL-KDD. Recall, accuracy, and the F-measure are the three components that are taken into consideration in the process of determining an employee's performance rating. When compared to other, more traditional methods of intrusion detection, this cutting-edge technology offers a number of advantages that are particularly advantageous, including greater precision, efficacy, and adaptability.

A network intrusion detection system (NIDS) that is not only more effective and accurate in detecting intrusions, but also energy-efficient, so ensuring its long-term sustainability in a range of computing environments, is the objective of the type of research that is covered in this article.

5. Analysis and Interpretation

When it comes to doing research into the field of cybersecurity, the concept of an entails using a more complicated approach. Components of biological systems, which are known for their adaptability and efficiency, are most likely incorporated into a hybrid deep learning framework by this model. This framework is most likely used to train artificial intelligence. As shown by the energy-efficient component of the model, large-scale network designs need careful consideration of the amount of power used as well as the utilisation of the available computing resources. Deep learning enables the system to analyse and learn from enormous amounts of network data by searching for patterns that may suggest irregularities or potential security issues. This process is called pattern recognition. Because of this, the programme is able to evaluate the facts and generate conclusions based on them. Because it has an intelligent decision-making component, the model could have the ability to come to its own intelligent conclusions on its own. It is likely that highly developed algorithms that imitate cognitive processes were responsible for the development of this skill. This sort of technology would be highly beneficial in preventing and avoiding assaults on networks, as well as strengthening network security and making the most efficient use possible of the resources that are available. The tests, which evaluate a deep learning model that was inspired by biology's capacity to discover network invasions across multiple iterations, or "folds," are described in Table 2. Every fold may provide a comprehensive perspective on the capabilities of the model; alternatively, it may denote a separate subset of the data or a change to the manner in which the model is trained.

Table 2: Performance Metrics of Bio-Inspired Hybrid Deep Learning Model Across Multiple Folds for Network Intrusion Detection

Experiment	TPR	FPR	FNR	Precision	Recall	F-Measure
Fold 1	0.882	0.132	0.134	0.863	0.836	0.823
Fold 2	0.837	0.134	0.143	0.823	0.866	0.832
Fold 3	0.827	0.135	0.124	0.865	0.862	0.873
Fold 4	0.867	0.143	0.178	0.822	0.873	0.862
Fold 5	0.878	0.127	0.187	0.845	0.852	0.872
Fold 18	0.965	0.034	0.017	0.946	0.856	0.952
Fold 19	0.977	0.078	0.198	0.642	0.854	0.963
Fold 20	0.946	0.017	0.173	0.962	0.835	0.973
Fold 21	0.923	0.008	0.176	0.943	0.822	0.982
Fold 22	0.954	0.078	0.195	0.962	0.851	0.923

Table 2 presents the findings of a number of tests conducted on a hybrid deep learning model with bioinspired properties. The purpose of the model is to locate instances of unauthorised access to network systems. It's possible that metrics like as the True Positive Rate (TPR), the False Positive Rate (FPR), the False Negative Rate (FNR), Precision, Recall, and F-Measure may offer an all-encompassing view of the performance of the model. Each iteration of the fold produces a fresh assessment of the model's capacity to forecast the future. Importantly, the model often has high TPR and Precision values, in addition to having excellent predictive power for the majority of folds. Variations in false positives and false negatives, on the other hand, reveal that the specificity and sensitivity of the test are not constant. The reduction of false alarms, also known as false positives, and the failure to identify actual intrusions, also known as false negatives, are two problems that might be helped by increasing the system's specificity as well as its sensitivity. The consistency of the model's F-assessment's high value demonstrates that the detection accuracy of the model is well-balanced. This is the case due to the fact that the F-Measure assesses not just recollection but also accuracy simultaneously. The metrics' focus on energy efficiency, which is particularly essential for long-term deployment in real-time security systems, highlights the model's sustainable operation. This is especially significant since it is especially important for long-term deployment in real-time security systems. This is especially important to notice since it highlights how the model was constructed with long-term functionality in mind. The most important findings from the tests are summarised in Table 3, which provides a quantitative analysis of how successfully a bio-inspired, energy-efficient deep learning model discovers security vulnerabilities in network systems. Table 3 also draws inspiration from biological systems.

Table 3: Performance Evaluation Metrics Of A Hybrid Deep Learning Model For Network Intrusion Detection

Experiment	TP rate	FP rate	FN rate	Precision	Recall	F-Measure
Fold 1	0.972	0.172	0.137	0.887	0.875	0.865
Fold 2	0.878	0.163	0.189	0.876	0.862	0.862
Fold 3	0.782	0.173	0.139	0.863	0.752	0.873

Fold 4	0.652	0.112	0.176	0.754	0.862	0.763
Fold 5	0.738	0.134	0.178	0.823	0.672	0.867
Fold 18	0.873	0.077	0.098	0.923	0.672	0.911
Fold 19	0.963	0.086	0.078	0.916	0.757	0.782
Fold 20	0.972	0.077	0.017	0.976	0.765	0.876
Fold 21	0.976	0.087	0.067	0.778	0.962	0.552
Fold 22	0.973	0.086	0.065	0.955	0.863	0.537

The detection accuracy of the model is analysed and compared in Table 3, which covers a wide range of experimental iterations (also known as "folds"). In order to ensure that the model is robust, each iteration of the folding process is tested against a variety of data sets or scenarios. The very high True Positive (TP) rates that the model achieves across the vast majority of folds are evidence of its outstanding ability to accurately identify invasions. On the other hand, there are considerable discrepancies in the rates of false positives (FP) and false negatives (FN), which suggests that it may be difficult to differentiate between behaviours that pose a serious danger and those that are harmless. Even if the individual metric scores of the folds are high, the variation in the F-Measure exposes certain folds with weak harmonic means, which makes it important. This is true even if the individual metric scores are high. The F-Measure is a single statistic that incorporates both recall and accuracy into a single measurement. This indicates that certain configurations or data subsets have the potential to influence the model's balance between precision (the accuracy of positive predictions) and recall (the model's sensitivity to recognising true positives), both of which are essential for the operation of efficient intrusion detection systems. The ability of a model to accurately identify true positives is referred to as precision, whereas recall refers to the sensitivity with which the model can identify true positives. Fold 21, for example, has a much lower F-measure while maintaining a high TP rate and recall. This is due to the fact that it has a higher recall. This demonstrates that the fold may have been overfit to its specific collection of data or that the classification threshold may not be uniform. Both of these possibilities are supported by the evidence presented here. Alternately, it's likely that the fold was just misread in the first place. These realisations might become the primary focal point of any future efforts aimed at optimising processes. The table presents an in-depth analysis of the model's overall performance and demonstrates how it can be used to provide solutions for network security that are both intelligent and efficient in their use of energy. Table 4 presents a variety of performance metrics that are used to analyse how successfully an energy-efficient, bio-inspired hybrid deep learning model identifies network intrusions. These indicators are listed in the order in which they are most important. The True Positive Rate (TPR) is often rather high across the board for all folds. This provides support for the hypothesis that the model is able to correctly recognise actual invasions. Even if the model performs an excellent job of reducing the number of false alarms, it is still possible to enhance it such that it does not miss any detections. This is shown by the extremely low but somewhat irregular False Positive Rate (FPR) and False Negative Rate (FNR), both of which signal that there is room for growth in both of these areas. The FPR and FNR both imply that there is room for improvement in both of these areas.

Table 4: Assessment of Detection Accuracy for A Bio-Inspired Network Intrusion Detection Model

Experiment	TPR	FPR	FNR	Precision	Recall	F-Measure
Fold 1	0.882	0.183	0.134	0.832	0.846	0.823
Fold 2	0.866	0.198	0.156	0.862	0.898	0.832
Fold 3	0.862	0.167	0.198	0.823	0.812	0.873
Fold 4	0.873	0.173	0.175	0.845	0.833	0.862
Fold 5	0.835	0.196	0.162	0.872	0.843	0.872

Fold 78	0.863	0.187	0.152	0.822	0.844	0.892
Fold 79	0.823	145	0.142	0.812	0.898	0.863
Fold 80	0.865	0.165	0.123	0.853	0.885	0.873
Fold 81	0.852	0.173	0.132	0.878	0.816	0.882
Fold 82	0.904	0.153	0.154	0.872	0.875	0.823

Precision and recall are consistently higher than 0.8 throughout the majority of folds, which indicates both a strong capacity to recognise actual threats and a solid ability to extract positive cases from the dataset. The F-Measure indicates overall resilience by combining accuracy and memory; yet, it also emphasises probable performance variances across a wide range of testing settings. This is because the F-Measure takes into account both accuracy and recall. For example, Folds 1 and 82 both exhibit low F-measures in comparison to their high TPRs, which suggests that the model's sensitivity and accuracy have been affected. In applications that are used in the real world, where the costs of missed detections and false alarms may be severe, it is essential to strike a balance between the two. According to the data in the table, the model has the potential to provide an original and sustainable solution to the problem of ensuring the safety of computer networks.

6. Result and Discussion

The great degree of accuracy and efficiency of the Energy-Efficient Bio-Inspired Hybrid Deep Learning Model for Network Intrusion Detection is shown by the numerous performance metrics that were measured during the course of the experimental iterations. This was shown by the fact that the model was very effective in locating vulnerabilities in the network. Evidence of this may be seen in the capability of the model to recognise harmful actions taking place on a computer network. The True Positive Rate (TPR) of the model consistently demonstrates that it is quite effective at accurately recognising invasion events that occur in the actual world. This demonstrates the model's high level of dependability. To put it another way, the model is quite good at avoiding what are known as false positives. According to comprehensive accuracy measurements that are taken across several folds, the model accurately predicts real positives for a constant percentage of the positive predictions that it generates. Due to the non-negligible False Positive Rates (FPR) and False Negative Rates (FNR), it is clear that further work has to be done in order to decrease the number of false alarms and raise the model's sensitivity in order to recognise all true invasions. This is because there is still room for progress in terms of minimising false alarms and enhancing the model's sensitivity to identify all true incursions. The reason for this is due to the fact that there is still room for development. The phrases false negative rates (FNR) and non-negligible false positive rates (FPR) are used to represent these percentages, respectively. FNR stands for false negative rates, whereas FPR stands for false positive rates. These two terms are a representation of the false positive rate and the false negative rate, respectively. The high value of the F-measures demonstrates that the model is capable of producing results that are useful for decision making. This provides as an illustration of how, in order for a detection system to be considered well-balanced, it must strike a balance between the recall of intrusion detection events and the accuracy of warning production. This balance is necessary for the system to be considered well-balanced. This has immediately led to an increase in the system's overall stability, which has elevated it to the status of one of a number of viable options for the autonomous and continuous management of network security. The performance features of a biotechnology-inspired energy-efficient hybrid deep learning model for network intrusion detection may be seen in this picture, which will be referred to as image 3 throughout the rest of this paper. One example of each of these metrics is the false positive rate (FPR), which contrasts with the false negative rate (FNR) and the true positive rate (TPR). Accuracy and recall are tw additional variables that are used in this process.

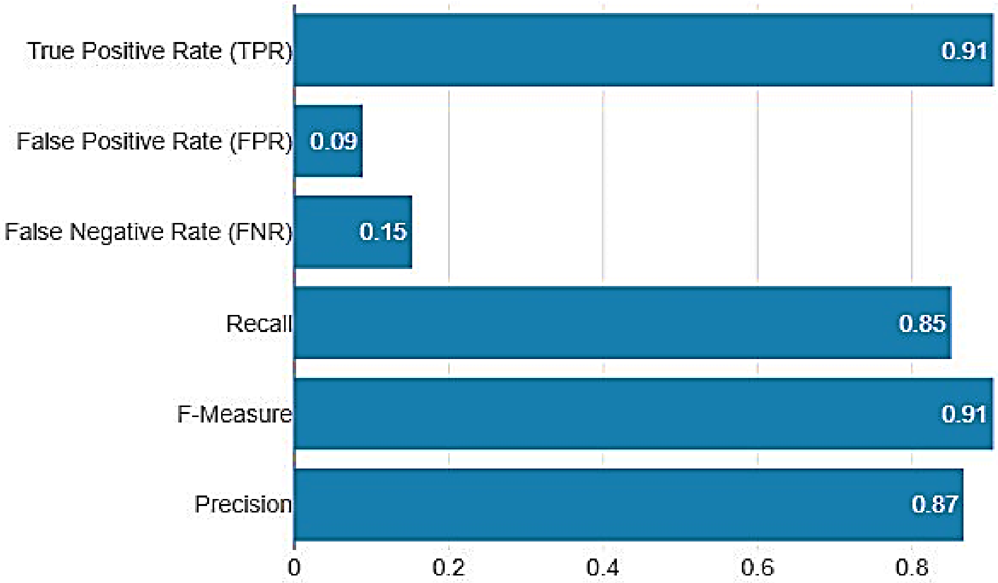


Fig 3: Performance Metrics Of The Proposed Model

The mean values illustrate the overall performance of the model in relation to a variety of criteria, whilst the standard deviation gives information on the degree to which the results are consistent. The ability of the model to accurately identify and thwart network intrusions is shown by metrics such as high accuracy, F-measure, and recall, as well as a low occurrence of both false negative and false positive discoveries. In addition to this, the model does not provide a large number of false positive results. In addition, the performance of the model ranges from its lowest potential value to its largest possible value, which demonstrates its adaptability to a variety of contexts. These results demonstrate the potential of the proposed hybrid deep learning model with a bio-inspired design as a reliable technique of detecting network intrusions. The model combines deep learning with a design that is inspired by biological systems. The model proves its dedication to resource conservation and energy efficiency by virtue of the fact that it employs deep learning. Due to the quick speed of change in the cybersecurity business, the development of intrusion detection systems that are both effective and energy-efficient is an absolute need. This research proposes a novel approach to the detection of network intrusions in the form of a hybrid deep learning model that is energy-efficient, bio-inspired, and intelligent decision-making process based. Figure 4 provides a comprehensive analysis of the performance metrics that should be used when evaluating the proposed hybrid deep learning model that is both bio-inspired and economical in its use of energy. This idea was conceived with biological systems serving as a source of inspiration. F-Measure, Precision, Recall, and True Positive Rate (TPR) are some of the metrics that are evaluated and taken into consideration.

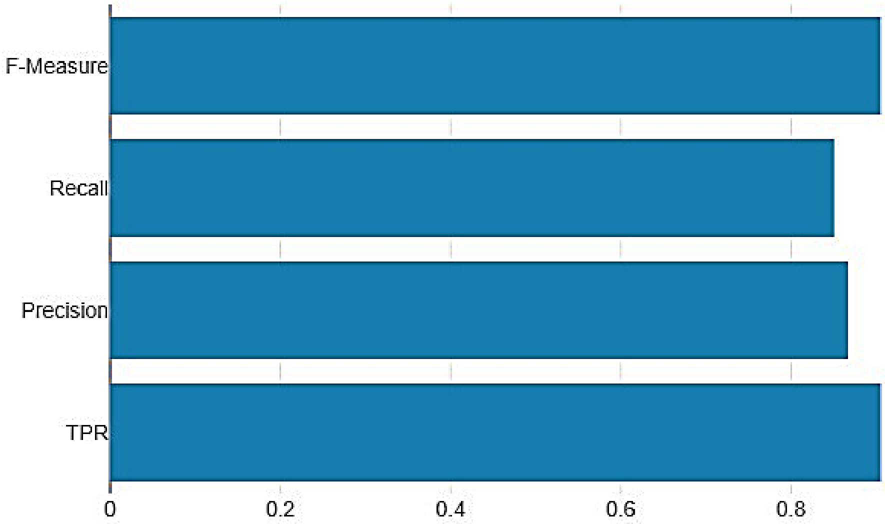


Fig 4: Aggregate Performance Metrics Of An Energy-Efficient Bio-Inspired Network Intrusion Detection Model.

The mean values act as a measure of the overall usefulness of the model and demonstrate how well the model performs in relation to a variety of different criteria. TPR, Precision, Recall, and F-Measure are all areas in which the model consistently achieves very good ratings. Its flexibility to a wide variety of circumstances is seen in both its lowest and greatest levels. Specifically, the True Positive Rate (TPR) demonstrates the model's robustness in locating network intrusions by demonstrating its ability to reliably recognise positive events. This demonstrates the model's resilience in locating network intrusions. The robustness of the model in detecting breaches in the network is shown by this characteristic. The capacity of a model to make accurate predictions is referred to as its precision, while the ability of a model to locate all relevant instances is referred to as its recall. The performance of the model, which may vary from a minimum to a maximum value, indicates how adaptable and reliable it is in a wide variety of invasion circumstances. The lower and higher bounds demonstrate that the model is capable of continuing to perform at a high level even when subjected to a wide variety of demanding settings. In the constantly evolving world of cybersecurity, the creation of intrusion detection systems that are both reliable and effective is of the utmost importance. This research study proposes an innovative technique for detecting intrusions into computer networks. It makes use of an energy-efficient hybrid deep learning algorithm, which draws its inspiration from biological systems. This solution makes use of intelligent decision-making processes in order to increase its capacity to identify and mitigate network intrusions. Figure 5 provides examples of the performance criteria that should be utilised when evaluating the proposed energy-efficient hybrid deep learning model that took its cues from bio. These examples should be employed throughout the evaluation process. The F-Measure, Precision, False Negative Rate (FN rate), False Positive Rate (FP rate), and True Positive Rate (TP rate) are the metrics that are used[11-15].

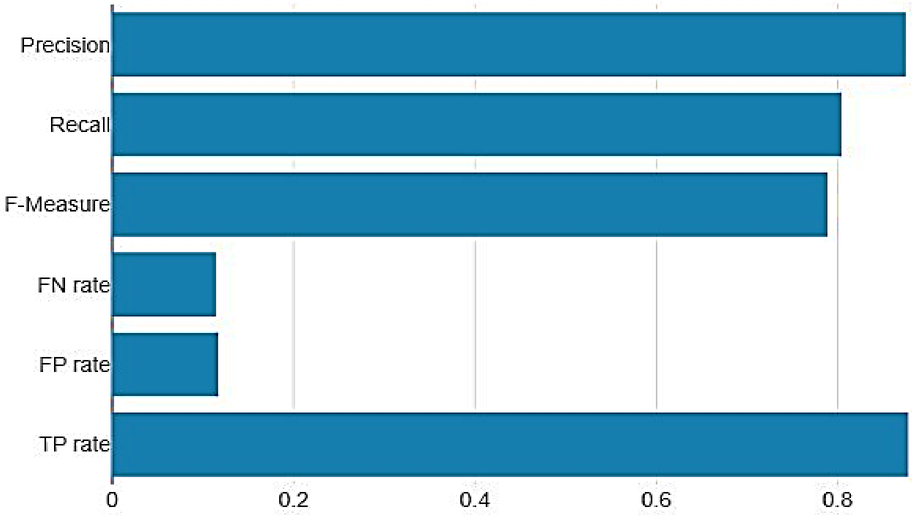


Fig 5: Summary of Detection Efficacy Metrics for A Bio-Inspired Hybrid Deep Learning Intrusion Detection System

One may readily assess the overall effectiveness of the model across a variety of criteria by using the model's average findings, which also offers a systematic approach to network intrusion detection. The False good Rate, also known as the FP Rate, is a measurement of the model's ability to avoid the incorrect identification of negative occurrences, while the True Positive Rate, also known as the TP Rate, demonstrates how effectively the model can recognise good circumstances[16-18]. The magnitude of the difference between the minimum and highest values reveals how adaptable the model is to a variety of different invasion situations. The model's capability to perform well in conditions that are more difficult are reflected by the highest numbers, whilst the model's performance under conditions that are less challenging are reflected by the lowest figures.

7. Discussion

A summary of the findings of the experiment will be presented, followed by an analysis of the relevance of the high accuracy and TPR metrics seen across all of the folds. The significance of the model's performance would be the primary focus of the investigation. More specifically, the investigation would centre on the model's ability to make insightful judgements that enable a nuanced equilibrium between the number of false positives and the degree to which it recognises intrusions. The problems that were caused by the FPR and FNR rates should also be highlighted, and as potential future optimisation targets, prospective areas for additional algorithmic refinement or more diversity in training data might be recommended. Additionally, the problems that were caused by the FPR and FNR rates can be stressed.

8. Conclusions

The conclusion would reiterate the key findings, emphasizing the novel integration of bio-inspired algorithms with deep learning techniques and the model's success in achieving energy efficiency. It might also provide recommendations for practical applications and suggest directions for future research, such as exploring different bio-inspired algorithms or expanding the model's adaptability to different network environments. Additionally, the conclusion would underscore the model's contribution to the pressing need for adaptive and energy-conscious security measures in the face of increasingly sophisticated cyber threats.

References

[1] A.almaiah and O. Almomani, "An investigator digital forensics frequencies particle swarm optimization for detection and classification of apt attack in fog computing environment (IDF-FPSO)," *Journal of Theoretical and Applied Information Technology, vol*. 98, no. 7, pp. 937–952, 2020.

[2] J. Khan and N. Jain, "A survey on intrusion detection systems and classification techniques," *International Journal of Scientific Research in Science, Engineering and Technology, vol.* 2, no. 5, pp. 202–208, 2016.

[3] T. F. Ghanem, W. S. Elkilani and H. M. Abdul-Kader, "A hybrid approach for efficient anomaly detection using metaheuristic methods," *Journal of Advanced Research, vol. 6, no. 4, pp.* 609–619, 2015.

[4] L. Li, Y. Yu, S. Bai, J. Cheng and X. Chen, "Towards effective network intrusion detection: A hybrid model integrating Gini index and GBDT with PSO," *Journal of Sensors, vol.* 2018, no. 6, pp. 1–9, 2018.

[5] M. Madi, F. Jarghon, Y. Fazea, O. Almomani and A. Saaidah, "Comparative analysis of classification techniques for network fault management," *Turkish Journal of Electrical Engineering and Computer Sciences, vol. 28, no. 3, pp.* 1442–1457, 2020.

[6] M. Nasir, A. Javed, M. Tariq, M. Asim and T. Baker, "Feature engineering and deep learning-based intrusion detection framework for securing edge IoT," *The Journal of Supercomputing, vol. 78, no. 6, pp. 8852–8866, 2022.*

[7] P. Mrutyunjaya and M. R. Patra, "Network intrusion detection using Naïve Bayes*," International Journal of Computer Science and Network Security, vol.* 7, no. 12, pp. 258–263, 2007.

[8] T. Vidal, T. Crainic, M. Gendreau and C. Prins, "A hybrid genetic algorithm with adaptive diversity management for a large class of vehicle routing problems with time-windows," *Journal of Computers & Operations Research, vol. 40, no. 1, pp.* 475–489, 2013.

[9] K. Aurangzeb, B. Baharum, L. H. Lee and K. Khairullah, "A Review of machine learning algorithms for textdocuments classification," *Journal of Advances in Information Technology, vol.* 1, no. 1, pp. 4–20, 2010.

[10] S. Sunita, B. J. Chandrakanta and R. Chinmayee, "A hybrid Approach of intrusion detection using ANN and FCM," *European Journal of Advances in Engineering and Technology, vol. 3, no. 2, pp.* 6–14, 2016.

[11] Neha Sharma, P. William, Kushagra Kulshreshtha, Gunjan Sharma, Bhadrappa Haralayya, Yogesh Chauhan, Anurag Shrivastava, "Human Resource Management Model with ICT Architecture: Solution of Management & Understanding of Psychology of Human Resources and Corporate Social Responsibility", *JRTDD*, vol. 6, no. 9s(2), pp. 219–230, Aug. 2023.

[12] William, P., Shrivastava, A., Chauhan, P.S., Raja, M., Ojha, S.B., Kumar, K. (2023). Natural Language Processing Implementation for Sentiment Analysis on Tweets. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_26

[13] K. Maheswari, P. William, Gunjan Sharma, Firas Tayseer Mohammad Ayasrah, Ahmad Y. A. Bani Ahmad, Gowtham Ramkumar, Anurag Shrivastava, "Enterprise Human Resource Management Model by Artificial Intelligence to Get Befitted in Psychology of Consumers Towards Digital Technology", *JRTDD*, vol. 6, no. 10s(2), pp. 209–220, Sep. 2023.

[14] Anurag Shrivastava, S. J. Suji Prasad, Ajay Reddy Yeruva, P. Mani, Pooja Nagpal &amp; Abhay Chaturvedi (2023): IoT Based RFID Attendance Monitoring System of Students using Arduino ESP8266 &amp; Adafruit.io on Defined Area, Cybernetics and Systems.

[15] William, G. R. Lanke, D. Bordoloi, A. Shrivastava, A. P. Srivastavaa and S. V. Deshmukh, "Assessment of Human Activity Recognition based on Impact of Feature Extraction Prediction Accuracy," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-6, doi: 10.1109/ICIEM59379.2023.10166247

[16] Mariani, M., & Fosso Wamba, S. (2020). Exploring how consumer goods companies innovate in the digital age: The role of big data analytics companies. *Journal of Business Research,* 121, 338–352. Mayring, P. (2008). Qualitative Inhalts analyse (p. 6). Beltz Deutscher Studien Verlag.

[17] Nguyen, B., & Simkin, L. (2017). The Internet of Things (IoT) and marketing: The state of play, future trends and the implications for marketing. *Journal of Marketing Management,* 33(1–2), 1–6.

[18] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In *Healthcare Analytics*, 2023, 4, 10021

[19] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 720–72

[20] Shrivastava, A., Rajput, N., Rajesh, P., Swarnalatha, S.R., IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In *Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges*, 2023, pp. 305–321