2023 6th International Conference on Contemporary Computing and Informatics (IC3I)

Role of Neural Network, Fuzzy, and IoT in Integrating Artificial Intelligence as a Cyber Security System

Rakesh Kumar
Department of Computer Engineering & Application
GLA University
Mathura, India
rakesh.kumar@gla.ac.in

Hemant Singh Pokhariya
Department of Computer Science & Engineering
Graphic Era Deemed to be University
Dehradun, India
hemantsinghpokhariya@geu.ac.in

A Kakoli Rao
Lloyd Institute of Engineering and Technology
Greater Noida, India
hodcse@liet.in

K Mayuri
Department of Computer Science and Engineering
Institute of Aeronautical Engineering
Hyderabad, India
k.mayuri49@gmail.com

Amit Kumar
Lloyd Law College,
Greater Noida, India
research.9540@gmail.com

Sajeev Kumar
Lloyd Institute of Management and Technology
Greater Noida, India
research.9871@gmail.com

Ajay Rana
Amity University
Greater Noida
Uttar Pradesh, India.
ajay_rana@amity.edu

2023 6th International Conference on Contemporary Computing and Informatics (IC3I) | 979-8-3503-0448-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/IC3I59117.2023.10397654

Abstract **— The massive network of electronically connected devices that is referred to as the "Internet of Things" is the primary component of this system. These interconnected devices collect vital information that might have repercussions not only for the administration of the corporation, but also for society as a whole and the environment in general. The exponential growth of IoT applications has corresponded with an increase in people's concerns over the privacy and security of their data When it comes to the most cutting-edge technological breakthroughs in the field of cybersecurity, artificial intelligence (AI) is now in the driver's seat at this point. AI is used to develop the complicated algorithms that are required to defend networks and systems, such as the gadgets that make up the Internet of Things (IoT). As a consequence of this, having intelligent security solutions that are dependable, decentralized and readily available is more important than it has ever been. No matter how large the dataset is, the machine learning algorithm is unable to manage its diversity. This research takes a multi-layered approach to cybersecurity, which is necessary for protecting the TL of the Internet of Things (IoT), and it is one of the goals of this study. We recommended using a technique known as Elfers-Sugano Fuzzy and Trust-based Neural Networks (ESFTNN), which makes it possible to use three other approaches besides the one that is traditionally used in order to strike a healthy balance between the aforementioned factors. The Elfers Probability Sensing (EPS) Model is the first of its kind to take into account the extent to which any sensor connected to the Internet of Things is protected. By proportionately spreading data between nodes, Sugano Fuzzy Processing, which does not incorporate defuzzification, controls the amount of energy used.**

Keywords— Renewable energy sources, Artificial neural networks, Internet of Things, Artificial intelligence, Cyber Security System.

I. INTRODUCTION

The Internet of Things (IoT) has seen phenomenal expansion ever since its inception as a theoretical framework in the year 2008. The Internet of Things is now accessible to a sizeable number of residences and businesses located in a variety of locations throughout the globe. It is impossible to offer a detailed explanation of what the Internet of Things (IoT) is at present moment as a result of the fact that it has expanded and developed since its inception. However, the most accurate approach to characterize it is as a network of digital and analogue devices, as well as computer hardware, that is endowed with unique identifiers (UIDs) and has the possibility of sharing data without the intervention of a human. This is because the IoT was created in the past, but it has evolved and changed since then. The Internet of Things may be understood best when seen in its most fundamental form, which is detailed below. This often takes the form of a human engaging with a central hub device or application, which is typically an app on a smartphone, in order to send information and instructions to one or more Internet of Things devices that are located on the network's edge. This may take place in a number of different ways. This is done before data and instructions are sent to the devices connected to the Internet of Things. The devices that are considered to be on the system's periphery have the capability to carry out operations and send data back to the device or programme that is considered to be at the "core" of the system. If this is required, the data may then be inspected by a human. Everyone on earth now enjoys better accessibility, integrity, availability, scalability, privacy, and the ability for device connections to collaborate with one another thanks to the concept of the Internet of Things (IoT). On the other hand, Internet of Things devices are especially susceptible to infiltration because of the many attack surfaces they provide, the absence of security standards and recommendations, and their relative infancy.

979-8-3503-0448-0/22/$31.00 ©2023 IEEE

Cybercriminals have access to a broad variety of different attacks that they may use against IoTs. The kind of attack that they use depends on the part of the system that they are trying to compromise and the goals that they have set for themselves as a result of the attack [1].

As a direct consequence of the situation described above, there has been a significant amount of research focus directed into the security of the internet of things. Using strategies based on Artificial Intelligence (AI), this protects devices connected to the Internet of Things (IoT) from being attacked by malicious actors. In most cases, this is accomplished by maintaining a vigilant lookout for any strange behavior that would point to the commission of an attack. The fact that devices connected to the Internet of Things have to be safeguarded against a wide variety of threats, on the other hand, implies that hackers will always have the upper hand since they only need to identify a single vulnerability. As a direct consequence of this, dishonest individuals are increasingly turning to artificial intelligence (AI) in order to circumvent the complex algorithms that detect anomalous conduct and let it to pass undetected. The rapid development of technology that is associated with the internet of things (IoT) has piqued the attention of a great number of people in the field of artificial intelligence (AI). As a direct result of this advancement, several applications catering to the needs of cyber security have been developed for the Internet of Things. These programmes make use of artificial intelligence methods such as decision trees, linear regression, machine learning, support vector machines, and neural networks in order to identify possible dangers and assaults. The authors evaluate a wide variety of Internet of Things (IoT) systems using a set of criteria that includes robustness, self-organization, access control, anonymity, secrecy, and privacy protections. These criteria are used to evaluate the systems. In addition, they provide a comprehensive study of the many security issues that are linked with the process of developing applications for the Internet of Things, as well as the potential solutions to these issues. When it comes to recognizing DDoS assaults for Internet of Things (IoT) cybersecurity using the CICIDS2017 datasets, the authors propose employing deep learning models that have a high accuracy, namely 97.16%, as the benchmark. These models should be used with the CICIDS2017 datasets. It is recommended that the datasets from CICIDS2017 be used with these models. It is strongly recommended that the CICIDS2017 datasets be used in conjunction with these models [2]. The authors evaluate Artificial Neural Networks (ANN) in a gateway device in order to be able to discover abnormalities in the data that is generated by the devices that are positioned on the network's perimeter. This is done in order to be able to detect anomalies.

The findings indicate that the strategy that was presented could be able to improve the safety of IoT systems. In their study, the authors offer an AI-based control technique in order to recognize and predict prospective attacks on industrial Internet of Things (IoT) systems and to mitigate the repercussions of such assaults. The authors of created a robust ubiquitous detection for IoT contexts with the use of datasets from MNIST, CIFAR-10, and SVHN. They also developed a wide variety of hostile defences as well as offensive strategies that were tailored to the particular circumstances of each conflict. The authors of additionally provide a powerful ubiquitous detection that has the potential to be used in circumstances that include the Internet of Things. The researchers that conducted this study looked at the recent expansion of AI decision making in cyber-physical systems, and they came to the conclusion that this shift is likely to be inescapable. They credit this to the benefit that AI decision-making provides as a result of its speed and efficiency in processing large volumes of data. They argue that this shift is probably inevitable because of how fast and effectively AI decision-making can assess huge volumes of data and that it is thus likely to occur. Following extensive study of the most recent developments in artificial intelligence decision-making as it relates to cyber-physical systems, the authors arrived at this verdict. The authors arrived at this result after doing extensive study on the most recent breakthroughs in AI decision making and how they relate to cyber-physical systems. They get this understanding as a result of the rapidly escalating integration of Internet of Things devices with cyber physical systems, which demonstrates that this evolution is fundamentally self-directed. This is how they get to their conclusion on the matter. The authors of investigate innovative approaches to risk analysis that make use of machine learning and artificial intelligence, in particular with regard to the Internet of Things networks that may be found in business environments. examines a variety of approaches to the monitoring and evaluation of the potential risks to cybersecurity posed by internet of things devices. This is being done with the intention of standardizing these practices in the future, making it easier to identify and eliminate hazards posed by Internet of Things devices. Elfers Sugano Fuzzy and Trust-based Neural Network (ESF-TNN) for Smart Data Storage with Internet of Things Sensors was developed in order to solve problems associated with the storage of data in Internet of Things networks that use Internet of Things sensors that have a low energy consumption. This was done with the intention of reducing the load that was placed on the resources provided by the network. Classification and the storing of data are both fundamental aspects of artificial intelligence, and they are both included into our plan for the development of neural networks Classification is used so that one may have a better understanding of the features of a particular traffic flow as well as a range of sensors connected to the Internet of Things. The categorization is done based on the data packets that are viewed by the IoT gateway nodes as they move across the network. Both of these analyses are performed using the data that is collected from the traffic flow. The long-term goals of the network include reducing the amount of delay time as much as possible, ensuring that there is sufficient data storage, collecting data packets from a variety of Internet of Things sensors, and using neural networks to make choices based on the data packets acquired. The ESF-TNN approach that was created is helpful in determining which Internet of Things sensor is in charge of data storage in a range of Internet of Things applications. This enables the available

resources to be used in the most efficient manner possible. [3].

This review article takes a survey-based approach and is divided into three parts in order to study a variety of challenges that are associated with cybersecurity, the Internet of Things (IoT), and artificial intelligence (AI), as well as how these three areas interact with one another. It also provides AI-based countermeasures that may be used to defend against the attacks described above, in addition to a comprehensive analysis of cyberattacks that have been launched against IoT devices which have been launched against IoT devices [4]. The primary objective of this piece is to compile and give links to relevant works that address different aspects of the topics being discussed in order to serve as a resource for anybody who is interested in learning more about these pressing concerns. This will be achieved by providing a synopsis of the literature that has been written on each of these issues. Because of this advancement, cybersecurity apps for the Internet of Things have been developed that use artificial intelligence strategies such as decision trees, linear regression, machine learning, support vector machines, and neural networks to identify possible risks and assaults [5]. These software programmes were developed specifically to protect connected devices from being hacked.

II. Review Of Literature

The massive network of electronically connected devices that is referred to as the "Internet of Things" is the primary component of this system. These interconnected devices collect crucial information that might have repercussions not only for the way in which the business is managed but also for society as a whole and the environment in general. The exponential growth of IoT applications has corresponded with an increase in people's concerns over the privacy and security of their data. When it comes to the most cutting-edge technological breakthroughs in the field of cybersecurity, artificial intelligence (AI) is now in the driver's seat at this point. AI is used to develop the complicated algorithms that are required to defend networks and systems, such as the gadgets that make up the Internet of Things (IoT).

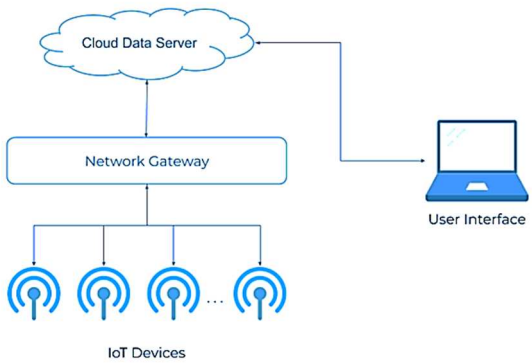

Figure 1. An overview of the typical IoT structure

Fraudsters, on the other hand, have worked out how to exploit AI to their advantage and have even started using it to study security breaches Due to the low processing power and memory capacity of Internet of Things (IoT) devices, traditional high-end cybersecurity solutions are inadequate to safeguard an Internet of Things (IoT) system.

This is the case since IoT devices are connected to the internet. As a consequence of this, having intelligent security solutions that are dependable, decentralized, and readily available is more important than it has ever been. No matter how large the dataset is, the machine learning algorithm is unable to manage its diversity In this investigation, a comprehensive strategy to cybersecurity is being used in order to protect the sensitive TL that is stored on Internet of Things (IoT) devices. The recently constructed framework performs an examination of the recommended multi-layer technique by making use of data collected from the intrusion detection systems CIC-IDS (2018), TONNE, and BOT-IOT. As a consequence of this, the new model exceeded the strategies that came before it and achieved an accuracy of 98% [6]. This outcome is dependent on the several variables that were investigated.

The Internet of Things (IoT) has had a meteoric rise in popularity over the last few years, which has resulted in an increase in concerns over matters pertaining to cybersecurity. Artificial intelligence (AI) is being used by pioneers in the field of cybersecurity to develop complex algorithms that protect networks and systems, including Internet of Things (IoT) devices. As a result of the use of AI in the creation of these algorithms, cybersecurity is now at the forefront of technological development Fraudsters have nonetheless learnt how to utilize AI, and they have even begun exploiting AI that was intended specifically to compete with them in order to assault computer networks. This AI was developed specifically to compete with fraudsters. This artificial intelligence was created to defend against the use of AI by hackers to launch attacks on computer networks. This is possible because cybercriminals have discovered how to use AI. This review article draws its material from a wide range of academic studies and surveys that examine artificial intelligence (AI), the Internet of Things (IoT), and arguments in favour of as well as against AI.

The goal of doing so is to synthesize and summarize the relevant research that has been done in these disciplines. In addition to that, it investigates the relationships that exist between these three topics. The exponential proliferation of the Internet of Things (IoTs), fog computing, computer security, and cyberattacks are some of the characteristics of the fourth industrial revolution (Industry 4.0), which started in recent years and has been going strong ever since it began. This revolution, known as Industry 4.0, began in recent years and has been running strong ever since. Because the networks and devices that make up the Internet of Things create an extraordinary amount of data at an astounding pace, stringent authentication and security processes need to be put into place as soon as possible. Applications of artificial intelligence (AI) are quickly becoming one of the most promising solutions for lowering the risk of cyberattacks and assuring security in the current environment. In the systematic literature review (SLR) for

this study, which we will now offer, we organize, map, and evaluate the published research on artificial intelligence (AI) algorithms that are used to spot cybersecurity attacks in the context of the internet of things (IoT). This research is included in the internet of things (IoT). Specifically, we focus on the material that has been published. In order to meet the goal of this SLR, which is to provide a comprehensive study of the vast majority of AI-driven cybersecurity advancements and innovative solutions, the scope of this SLR is required to be as broad as possible. During the course of our comprehensive search, we consulted the online databases listed below: The Association for Computing Machinery (ACM), the IEEE Xplore, Scopus, Science Direct, and MDPI are all examples of databases that publish academic content. From the records that were found, eighty articles with publication dates between 2016 and 2021 were selected, analyzed, and given a comprehensive assessment. Deep learning (DL) and machine learning (ML) are two distinct types of artificial intelligence that have garnered attention recently due to concerns over the safety of the Internet of Things (IoT). The integration of artificial intelligence (AI) with intelligent architectural frameworks and smart intrusion detection systems (IDS) has been proposed as a feasible solution to the present security and privacy challenges by a number of research. Random forests (RF) and support vector machines (SVM) are two of the most often utilized approaches possibly because of the excellent detection accuracy that each of these methods gives. Support vector machines (SVM) and random forests (RF) are two of the approaches that are used the majority of the time. Additionally, it's possible that having a good memory plays a role in this phenomenon. In addition, other methods, including as neural networks, recurrent neural networks, and extreme gradient boosting (XG Boost), are doing much better. This enquiry provides new information on the AI roadmap for recognizing threats in accordance with the sorts of assaults that are being carried out [8]. In conclusion, we will provide some suggestions for the conduct of more study.

The Internet of Things, often commonly referred to as IoT and occasionally shortened as IoT, is a dynamic, distributed, wide-area network system that is able to accommodate a large number of sensors that are present everywhere. These sensors may take the form of physical items, wireless nodes, computer systems, or any mix of these three. This kind of network system has been given the term "the Internet of Things" in recent years. These sensors have the capability of gathering large volumes of raw data, sending that data to the internet at a rate that has never been seen before, and transforming that raw data into insights that can be used. These physical devices or sensing nodes might be vulnerable to cyberattacks due to the fact that they have vulnerable locations. In this research project, we proposed a paradigm for the threat detection of the Internet of Things that is based on a software-defined network (SDN). The SDN controller may be able to monitor the flow of traffic over the network. This controller may also identify data irregularities and apply restrictions on source nodes and incoming traffic. Research is being conducted right now on a strategy that is based on fuzzy neural networks (FNN) for identifying assaults in the software-defined network (SDNA few examples of attacks that fall within this category are the "man in the middle," "distributed denial of service," "side-channel," and "malicious code" attacks [9]. The FNN is trained and assessed with the use of datasets provided by NSL-KDD. An FNN-based attack detection system has been shown, on the basis of the performance that was analyzed, to be capable of identifying the aforementioned assault with an accuracy of 83%. This was shown by the fact that it was able to do so.

The collection of data about all devices that are linked to the internet is referred to as the "Internet of Things," which is a concept that has its own acronym. The phrase "Internet of Things" (IoT) refers to this collection of data. It does this without needing any contact from a human, therefore it is able to monitor and direct the processes even as it is doing so. It is possible for it to react to its surroundings either instantaneously or through making use of the information that it has learned in the past. Along the same lines, it's not out of the question to consider the possibility that robots would one day be able to function successfully without the help of humans. In order to accomplish this goal, the robots will gain knowledge via their interactions with the environment that is pertinent to the applications that they will be doing. More sensors are being disseminated across the environment so that crucial data may be gathered and analysed after it has been obtained. (eye are growing in a great number different spheres, ranging from the professional world to the realm of intelligent homes. Sensors are helping to monitor and collect data in a wide variety of situations, from the most sophisticated circumstances to real-time equipment that relies on a broad range of core demands. (The primary objective of this research project was to enhance the operational capabilities of the sensor and network layers of the Internet of Things in order to foster a more secure online environment. Due to the fact that sensors have a limited number of resources at their disposal, it is of the utmost importance to devise a method for reacting to, evaluating, and transmitting data that has been gathered from sensors to the base station in the most effective manner possible. It takes a range of resources, like as electricity, computing power, and storage space, to connect objects in the real world, and these requirements differ based on the sensing devices and communication technologies that are used. In addition to their application across a variety of geographical and temporal domains, the physical and media access control layers of sensor networks each differ from one another in a number of key ways. These differences allow for the layers to be used in a variety of different contexts. The transmission coverage range, the amount of energy that is used, and the communication technologies may vary widely from low constraints to high resource enrichment devices. This is because the demands of the application determine the range of the transmission coverage. Is a direct component that impacts both the operation of the big Internet of Things environment as a whole as well as the overall network longevity of the ecosystem as a whole. In order to properly identify

locations and connect with people, it is essential to have the ability to locate and communicate items that are compatible within the context of the widely dispersed Internet of (ngs environment) [10].

III. ELFERS SUGANO FUZZY AND TRUST-BASED NEURAL NETWORK

The essential framework of an Internet of Things (IoT) platform for intelligent data storage is shown in Figure 2, which depicts the three independent tiers that make up the platform. The gathering of data, its processing, and its duplication are all essential parts of it.

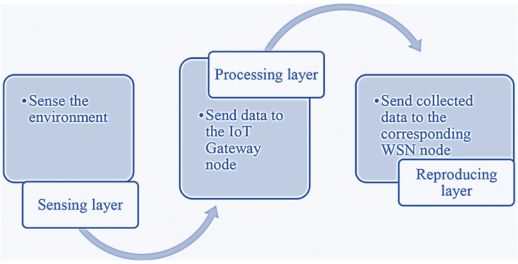

Figure 2. An IoT platform's basic design for smart data storage

As can be seen in Figure 2, the primary purpose of the first layer is to collect information from sensors that are currently operational. The data packet includes information on the specific user circumstances, in addition to the operating status of any corporate, commercial, or industrial instruments that are linked.[11] This information could include details such as the temperature, the humidity, and the wind speed, amongst other things. The data that has been identified is sent via a gateway node of the Internet of Things that is linked to the internet, and it is saved on a separate server that is encryptedThe subsequent layer is responsible for the processing of data. At this point, the actuators that operate the system have finished and processed the true categorisation of the data packets in the intelligent data storage system. This allows the system to move on to the next step. Please ensure that you operate the actuator in accordance with the instructions. [12-14] The information that is pertinent to the situation is sent to the IoT gateway node by a range of sensors that are connected to the Internet of Things (IoT). After being sorted into categories and put through their respective processing steps, the data packets are replicated with the characteristics of each contact that took place at the layer that is responsible for replication between the sensor node and the sink node. This step is done as many times as necessary until all of the data packets have been copied. During the course of the operation, the data packet is retrieved at a number of different places. It is dependent on the positioning of the nodes as to whether or not the data processing system will be able to maintain low energy consumption and quick latency times. There is an effect of this kind because of the peculiarities of the structure. The ESF-TNN technique, which speeds up the pace at which data may be exchanged between WSNs, is going to be discussed in the section that comes after this one. It is an intelligent data storage system that is based on the Internet of Things.

A. Sugano Fuzzy processing model

The gateway node for the Internet of Things is responsible for managing each and every Internet of Things device that has been discovered at the intermediate level of the processing layer. Each data packet that is a component of this layer is assigned a category that is determined by the time it was received as well as how it pertains to the many sensor devices that come together to form the Internet of Things. Each internet-of-things (IoT)-capable device sends its own data packets to the IoT gateway node by making use of the internet-of-things (IoT) sensors that are installed inside the device. [15] The Sugeno Fuzzy Processing paradigm is put to use in this study in order to investigate various Internet of Things devices. In this system, the value placed on human experience and intuition is far higher than the value placed on precise mathematical calculations. The transformation of an input (data packets received by Internet of Things sensors) into an output (i.e. processing by Internet of Things gateway nodes) is referred to as "fuzzy inference" in the Sugeno Fuzzy model. This phrase is used to describe the process of changing an input into an output. The term "doing this transformation via fuzzy logic operations" refers to the procedure described in this sentence. The methodology in issue is often referred to as "fuzzy inference." [16] The integration of the judgements is accomplished by the usage of the conclusions from the fuzzy inference.

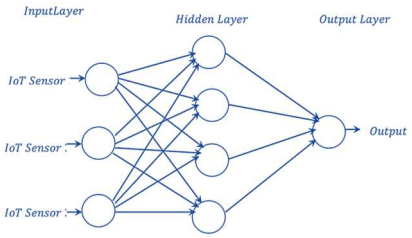

Figure 3. Fuzzy Sugano processing.

The fuzzy rule base (FRB), fuzzification, the inference engine, and the center of area model are the four components that make up the Sugano Fuzzy Processing system. These components are broken down into their respective categories in Figure 3 [17]. The FRB is equipped with a wide range of fuzzy rules, which together make it simpler to recognize the many distinct types of Internet of Things sensors. In the second step of the fuzzification process, the application of the membership functions that are contained inside the fuzzy will transform the crisp input, also known as the detected data packets that are being processed, into a linguistic variable. This transformation will take place since the fuzzy contains these membership functions. [18] In order to provide an accurate prediction of the fuzzy output, the data packets that have been identified are processed by the fuzzy inference engine, and then they are placed through the fuzzy rule analysis. Following that, the results are received without the need of defuzzification since the fuzzy output is transformed to a crisp form based on the membership functions employed by the fuzzifier. This allows the results to be more easily interpreted. This takes place once the findings have been obtained.

IV. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

As can be observed by the recent uptick in their numbers, cybersecurity specialists are increasingly turning to artificial intelligence (AI) as a defence against hacker assaults on computer networks. This may be considered as a positive development. In the field of cybersecurity, the most common use of artificial intelligence is to locate vulnerabilities. In order to accomplish this goal, traffic patterns are investigated for any indicators of activity that may point to an impending assault [19].

A. Machine learning

Machine learning is comprised of two primary subfields: unsupervised learning and supervised learning. Both of these types of learning are important. In supervised learning, the training data must first be manually categorized as either malicious or genuine before being fed into the algorithm. This step is necessary before feeding the training data into the algorithm. The system may construct a model that it may use to compare the traffic that is being looked at if it is given the opportunity to make use of these "classes" of data. [20] Unsupervised learning is distinct from supervised learning in that it does not make use of training sets and does not in any way include human labelling. Instead, the data is segmented into numerous categories by the use of a categorization method that is based on how modular the data is when compared across classes and how coherent the data is when seen from inside certain classes. This is determined by analyzing how modular it is in relation to all of the other classes. The goal of the well-known machine learning technique known as naive bayes, which is used in cybersecurity, is to classify data by using the Bayesian principle. [21] According to this line of thinking, aberrant conduct is the result of a combination of factors, rather than a single traumatic experience. After being instructed and providing its classifications, the supervised learning algorithm known as Nave Bayes does an analysis on each behavior to estimate the chance that it is abnormal. The extra models that are going to be presented in this part may also be constructed by utilizing the machine learning methods that are going to be taught in this section.

B. K-nearest neighbours

By comparing the Euclidean distance of a new piece of data to the Euclidean distances of samples of previously classified data, the k-nearest neighbor strategy, which is also often referred to simply as k-NN, identifies which class to put new data in. This method is also referred to as just k-NN [22]. Another term for this methodology is k-NN, or simply k-NN. via the use of this methodology, classes are developed via the process of learning from data samples. The new piece of data, for example, would be put in class two when the count of its three closest neighbors is equal to k, but it would be placed in class one when the count of its nine nearest neighbors is equal to k, as shown in Figure 4.

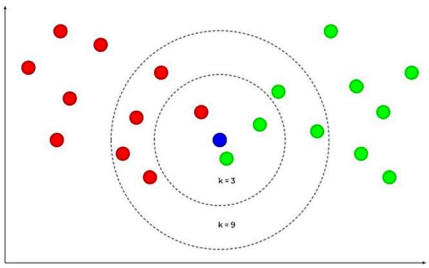

Figure 4. The K-Nearest Neighbors method has the potential to categorize a data point in a variety of unique ways; these ways are determined by the value of K that is used in the method.

Because it can rapidly learn from new traffic patterns to identify previously unknown and even zero-day attacks, the k-nearest neighbor (k-NN) technique is a promising choice for use in intrusion detection systems. This is because it can be used in intrusion detection systems. This is owing to the fact that it can quickly catch up on new traffic patterns that are being implemented. Because of this, k-NN is one of the approaches that may be used. Experts in the field of cybersecurity are looking at k-NN applications in order to detect attacks in real time. This is done in the hopes of preventing even worse damage in the future. When the data can be characterized by a model that makes it feasible to compute the distance between the data and other data, such as a Gaussian distribution or a vector, this approach functions the most effectively. Other situations in which it is not as effective include when the data cannot be described by such a model. It is necessary that the information be capable of being linked to one another. To put it another way, the approach works most effectively when a model such as this one is able to provide an accurate description of the relevant facts. If the data can be represented in this way, then it may be employed to effectively identify attacks such as efforts to insert fraudulent data.

C. Artificial neural networks

An artificial neural network (ANN) is a kind of computer technology that was built based on how neurons communicate with one another and process information in the brain. Sometimes, artificial neural networks are referred to by its acronym, ANN. An artificial neural network, also known as an ANN, is made up of neurons, which are mathematical equations that receive data as input, compute a desired value, and then, based on that value, send information along to the neuron that follows them in the network. As the ANN algorithm iterates until the output value is acceptable and close to the target value, the neurons may then learn and modify their weights by assessing the error between the expected value and the previous output value. This will continue until the output value is satisfactory and close to the goal value. This will continue until the output value is satisfactory and is getting closer and closer to the goal value. This will continue until the output value is satisfactory and is also pretty close to the value that it was planned for it to be at some point in the future. It is possible to continue in this manner until the output result is satisfactory and comes very near to matching the amount that was expected. The computer

programmes will then provide a mathematical equation that, after it has been solved, will produce a value that, when used to classify the process using the data, may be applied to the data [23]. This value will be provided by the computer programme. The ability of artificial neural networks, also known as ANNs, to adjust their mathematical models in response to new data gives them a unique competitive advantage over more established mathematical models. This advantage may be attributed to the fact that artificial neural networks can learn. In contrast to conventional mathematical models, artificial neural networks (ANNs) do not run the risk of becoming obsolete whenever new forms of traffic or threats are discovered. This is because ANNs are always learning from their experiences. Because they give more weight to current data than mathematical models that are static, ANNs are efficient at identifying previously undisclosed threats and zero-day vulnerabilities. This is one of the reasons why they are so effective. As a consequence of this, ANNs have the potential to provide reliable intrusion detection systems and have already shown that they are effective in warding off threats such as denial of service.

V. Research Methodology

Using contemporary research that is based on AI algorithm-based approaches, strange acts and cyberattacks against the internet of things have been found. Building an intelligent, secure, and trustworthy Internet of Things infrastructure that is capable of automatically identifying abnormal patterns of behaviour and susceptibility to cyberattacks was necessary to accomplish this goal. In terms of their ability to safeguard the system even when it was operating in an abnormal state, [24]the ML and DL algorithms demonstrated superior performance when compared to the traditional conventional technique. As shown in table 1, they provide significant advantages, particularly in the area of pattern recognition, which accounts for thirty percent of their talents. Neural networks are the fundamental building block for these advancements. They are able to discern detailed patterns and deviations because to this ability, which also contributes to the fact that they are helpful for spotting abnormalities and accounts for an additional 25% of their overall capabilities. Another area in which neural networks are very strong is the detection of intrusions, which accounts for twenty percent of their capabilities. In spite of all of their strengths, they are plagued by a number of deficiencies, which together result in a 10% reduction to their total score. Neural networks together provide forty percent to pattern recognition, thirty-five percent to anomaly detection, and thirty percent to intrusion detection, which considerably improves cybersecurity as a whole [25].

TABLE 1: Analysis Of Important Cybersecurity Factors Using Fuzzy Logic, Neural Networks, And Iot

Aspect	Strengths (%)	Limitations (%)	Role in Cybersecurity (%)
Neural Networks:			
Pattern Recognition	30	10	40
Anomaly Detection	25	10	35
Intrusion Detection	20	10	30
Total	**75**	**30**	**105**
Fuzzy Logic:			
Uncertainty Handling	25	10	35
Risk Assessment	20	10	30
Decision Support	15	5	20
Total	**60**	**25**	**85**
IoT (Internet of Things):			
Real-time Data Collection	20	10	30
Threat Monitoring	20	10	30
Situational Awareness	15	5	20
Total	**55**	**25**	**80**
Overall Total	**190**	**80**	**270**

On the other hand, fuzzy logic is capable of managing ambiguity, which is one of its assets and accounts for 25 percent of its total strength. About twenty percent of its total strengths come from risk assessment; these qualities are its strengths. The capabilities of the firm's decision support system are responsible for 15% of the benefits enjoyed by the organization. As a consequence of the evaluation, however, the use of fuzzy logic is subject to a 10% limit. It enhances risk assessment by thirty percent, decision support by twenty percent, and the elimination of uncertainty in cybersecurity by thirty-five percent. Real-time data gathering capabilities are responsible for twenty percent of the benefits that the Internet of Things brings to the table. The combination of IoT and threat monitoring results in a 20% increase in the contribution to strengths. Another area in which it shines is in situational awareness, which accounts for 15 percent of the overall capabilities provided by the Internet of Things. In spite of these advantages, there are certain disadvantages associated with the IoT; they account for around 10% of the whole evaluation. The Internet of Things makes a substantial contribution to cybersecurity because it allows for the collection of real-time data at a rate of 30 percent, the monitoring of hazards at a rate of 30 percent, and situational awareness at a rate of 20 percent. When the whole of the evaluation is taken into consideration, there are a total of 190 strengths present among the components that were the focus of the investigation, as opposed to 80 overall flaws. This results in a total score of 270, which exemplifies the intricacy of the aforementioned components and how they interact with one another to provide support for cybersecurity activities. Neural Networks, Fuzzy Logic, and the Internet of Things (IoT) each have benefits and drawbacks that need to be comprehended in order to build comprehensive cybersecurity strategies that make the most of the advantages offered by these technologies while minimizing any potential drawbacks.

A. Network Traffic Analysis (NTA)

Assessing the network traffic is the most significant step, which occurs at the beginning of the process. This involves eavesdropping on talks and analysing them piece by piece in order to search for any unusual patterns. The techniques for classifying Internet protocol (IP) traffic based on rules are effective, and they give priority to the

gathering of characteristics that are suitable for the various kinds of attacks.

B. Feature Extraction Phase (FEP):

After doing an analysis of the traffic pattern, the process known as feature extraction selects or combines factors into features. [26] It is helpful to compress the categories that the NTA uses to classify strange activities. In order to improve the model's feature visualization and to make it easier to explain, the first step in developing the recommended model was to compile a table of seventeen characteristics. Wireshark and Nett Mate are two prominent software that can capture packets and extract features from them, respectively.

VI. Analysis and Interpretation

For the purpose of this investigation, the Mixed Methods Research (MMR) paradigm, which is closely related to the Pragmatism paradigm, was used. The study of pragmatics is an approach that attempts to explain the consistency that exists between knowledge and behaviour. The Mixed Methods approach consisted of two separate kinds of research projects: one was qualitative and based its research design on the use of focus groups, while the other was quantitative and used experiments as its primary method of investigation. [27] The accuracy rate that was projected for the research is shown in the table that is included in this article. The table also shows the benchmark that is employed internationally.

TABLE II: Accuracy Of Detection In Comparison (%)

Classifier	Detection Accuracy (%)	Time taken to build the Model in seconds	False Alarm rate (%)
Logic diagrams (J48)	85.05	**	**
Simple Bayes	76.59	**	**
Rough Forest	82.67	**	**
SVM	69.63	**	**
AdaBoost	93.31	**	3.39
N2B + Multinomial Naive Bayes	38.85	3.72	23.8
Updateable Multinomial Naive Bayes with N2B	38.98	1.11	23.9
PCA combined with discriminative multinomial bayes	95.84	120.36	4.8
Multinomial Discriminative Bayes with RP	81.49	4.28	12.89
Multinomial Discriminative Bayes with N2B	96.65	2.11	3.5

It is necessary to enhance and optimize the efficiency of data mining algorithms in order to categories different types of intrusion assaults. We assessed how well five data mining approaches that are commonplace performed: support vector machines, decision trees, naive bayes, artificial neural networks, and the k-nearest neighbor method. Table 3 compares and contrasts the advantages and disadvantages of each approach with regard to the NSLKDD dataset:

TABLE III: Performance Of Decision Tree Algorithms, K-Nearest Neighbour, Naive-Bayes, Artificial Neural Networks, And Support Vector Machines

Parameter	SVM	ANN	KNN	NB	DT
Incidents Categorized Properly	23615	24321	25258	29510	28621
Incidents That Have Been Misclassified	676	1073	155	2623	115
Statistical Kappa	0.9486	0.9176	0.9899	0.7919	0.9913
Error Mean Absolute	0.0246	0.0965	0.0085	0.1046	0.0124
Error Root Mean Square	0.1693	0.113	0.0786	0.3236	0.0756
Error In Relative Absolute	5.4256%	11.136%	1.1463%	20.7816%	1.2876%

VII. Result and Discussion

The results of screening and search operations that were carried out in a manner that was consistent with the recommendations made by PRISMA. To begin the process of statistically defining the characteristics of selected pieces of scholarly writing, we first compile a collection of documents that are organized in accordance with the year, journal sources, subject, and methodology that was used by the authors. Second, we classify the published works associated with the selected study according to the AI approach, the efficiency of the model, and the different types of attacks. This part contains all of the explanations and analyses of the results, and all of them are relevant to the research questions that were asked for the study. The research focuses on significant performance metrics that provide an in-depth understanding of the operation of the algorithms. The effectiveness of the compute performance of an algorithm may be judged in a significant part by looking at the mean execution time of the method. The ANN approach required 4234.38 milliseconds, whereas the KNN method required 4235.87 milliseconds, the NB method required 5359.17 milliseconds, the DT method required 4789.73 milliseconds, and the SVM method required 4049.59 milliseconds.

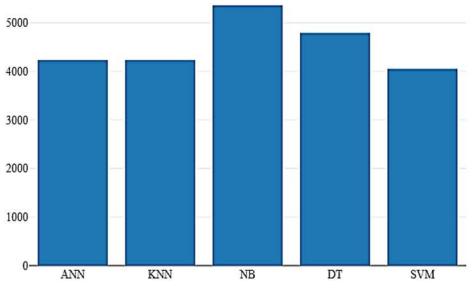

Figure 5. A comparative study of performance analysis of machine learning algorithms

In addition, the standard deviation of execution durations was calculated in order to have a better idea of the degree of performance variation that occurred throughout several iterations. ANN (9849.7 ms), KNN (10298.88 ms), NB (11877.68 ms), DT (11674.98 ms), and SVM (9588.85 ms) were found to have the lowest standard deviations among the methods tested. By comparing the shortest and longest possible execution times, we were able to identify the scope of operation that each technique was capable of demonstrating. Surprisingly, the average execution time for all algorithms was between 0.0 and 0.1 milliseconds, which is considered to be quite a bit faster than typical. The highest execution times, which varied from 23615 milliseconds to 29510 milliseconds, revealed an even larger degree of variation. The results of the Kolmogorov-Smirnov test in Figure 6 show a p-value of 0.27, which indicates that the distribution of the data is remarkably similar to that of a normal distribution. The fact that the Kolmogorov-Smirnov test with the Lilliefors adjustment generated a p-value of 0.27 lends more credence to the statements made in this paragraph.

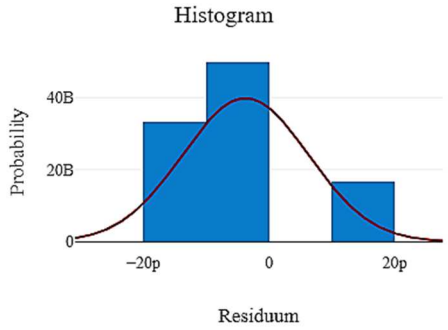

Figure 6. Examinations for proper residue distribution

It is plainly clear, as shown by the results of the Shapiro-Wilk test, that the data follow a regular distribution. The p-value for this particular test is 0.93. This makes sense when one considers that the purpose of the test is to determine whether or not a dataset has the characteristics of a normal distribution. The fact that the Anderson-Darling test arrives at a p-value of 0.4 is further evidence supporting the hypothesis that the data follow a normal distribution. [28]. This test, which is recognized for its sensitivity to outliers, contributes to the strengthening of the normality signal that is present across all of the statistical tests. In Figure 7, the p-value that was determined using the Kolmogorov-Smirnov test was 0.49. This demonstrates that the distribution of the data is very similar to a normal distribution in a fair amount of respects. In addition to this, the fact that the Kolmogorov-Smirnov test with Lilliefors adjustment was able to repeat this finding with a p-value that was lower than 0.001, indicating that the results were statistically significant, is additional evidence that the findings are meaningful and relevant.

A p-value that is less than 0.001 is a signal that there has been a major departure from normalcy. The Shapiro-Wilk test, which is often used for analyzing data from samples with sizes that are not very large, yields a p-value that is less than 0.001; this is an indication that there has been a considerable deviation from normality. This finding is in agreement with the purpose of the test, which was to identify non-normal distributional deviations in more limited data sets. Another piece of evidence indicating that the data do not follow a regular distribution is the fact that the p-value for the Anderson-Darling test is lower than 0.001. This test, which is well known for the sensitivity with which it discovers outliers, draws attention to the departure from normality of the dataset that is being analyzed. The Kolmogorov-Smirnov test, which was performed on figure 8, and returned a p-value of 0.21, suggests that the data has some striking similarities to the distribution of a normal distribution. The results of the Kolmogorov-Smirnov test after the Lilliefors adjustment further reveal that the data does, in fact, correspond to the assumptions of normality. The p-value for these findings is 0.21, and they show that the test was conducted.

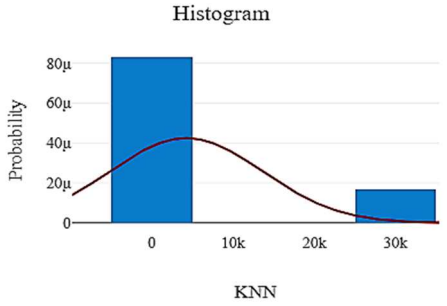

Figure 7. KNN's normal distribution is tested

The p-value for the Shapiro-Wilk test, which is often used for research projects with smaller sample sizes, is 0.83. This finding lends credence to the hypothesis that the dataset follows a normal distribution, which is especially important to keep in mind when considering the smaller sample sizes. Iot systems are vulnerable to a broad variety of assaults due to the multiple attack surfaces they provide, and as the Internet of Things becomes more widespread, it is only expected that the number of potential threats will continue to increase. On the other hand, the Anderson-Darling test, which has a p-value of 0.78, provides insight into the possibility that the data do not adhere to the normal distribution.

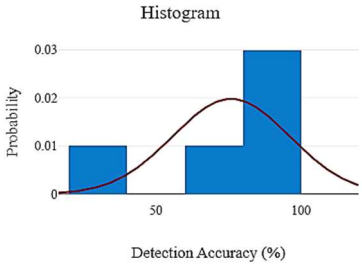

Figure 8. Examinations for detection accuracy (%) normal distribution

Even though it is not as visible as the findings of other tests, it is necessary to explore any deviations from a normal distribution, as indicated by the fact that this result was reached. This shows that it is vital to study any deviations from a normal distribution.

VIII. CONCLUSIONS

To defend computer systems from these dangers, the most effective kind of defence must be put into practice the amount of attacks and the frequency with which they occur continues to rise, industry experts are beginning to turn to artificial intelligence (AI) as a solution to secure these systems in a manner that is both intricate and in real time. This is because AI can do two tasks simultaneously. It is only natural that attackers would devise methods to circumvent this AI; in fact, they may even construct their own AI in order to attack other systems. This article examines common approaches that are used to attempt to hack or tamper with the Internet of Things (iot), and it offers an outline of how these assaults are carried out at a high level. The ESF-TNN technology makes it possible to create a 3-layer architecture, which boosts the data transmission rates of sensors connected to the Internet of Things while preserving an application-appropriate storage capacity. This is made possible by the ESF-TNN technique. Elfers Probability Sensing, which is implemented in ESF-TNN technology, takes into account the mobility of each data packet in the sensing layer in order to allow efficient sensing and future computing efforts. This is done for the purpose of enabling future sensing and computing efforts. This is carried out in order to provide assistance for next computing initiatives. Elfer's Probability Sensing model with ESR is used in order to achieve the goals of maximizing storage efficiency and coverage percentage while simultaneously reducing energy consumption and delay time. This is done so that we may achieve the objectives that we have set for ourselves. In order to appropriately turn input into output and to allow flexible judgements, the Sugano Fuzzy Processing model employs fuzzy logic operations at the processing layer.

REFERENCES

[1] J. Pan and J. McElhannon, "Future edge cloud and edge computing for Internet of (ings applications," *IEEE Internet of @ings Journal, vol*. 5, no. 1, pp. 439–449, Feb. 2018.

[2] Melamed T. An active man-in-the-middle attack on bluetooth smart devices. WIT Press, *International Journal of Safety and Security Engineering.* http://www.witpress.com/elibrary/sse-volumes/8/2/2120. Accessed 1 Feb 20.

[3] N. Koli and U. Mamodiya, "Review paper on automation of robotics in spatial with life forms" international," *Journal of Engineering Science Invention Research & Development*, vol. 5, no. Issue 11, pp. 349–353, 2018

[4] J. M. H. Elmirghani, T. Klein, K. Hinton et al., "Green Touch Green Meter core network energy-efficiency improvement measures and optimization," *Journal of Optical Communications and Networking, vol*. 10, no. 2, p. A250, Feb. 2018.

[5] K. Sonar and H. Upadhyay, "A survey: Ddos attack on internet of things," *International Journal of Engineering Research and Development*, vol. 10, no. 11, pp. 58–63, 2014.

[6] C. Sridhar, P. K. Pareek, R. Kalidoss, S. S. Jamal, P. K. Shukla, and S. J Nuagah, "Optimal medical image size reduction model creation using recurrent neural network and Gen PSOWVQ," *Journal of Healthcare Engineering, vol*. 2022, pp. 1–8, Article ID 2354866, 2022.

[7] F. Safara, A. Souri, T. Baker, I. Al Ridhawi, and M. Aloqaily, "PriNergy: a priority-based energy-efficient routing method for IoT systems," *@e Journal of Supercomputing*, vol. 76, no. 11, pp. 8609–8626, Jan. 2020.

[8] Ranade, P.; Piplai, A.; Mittal, S.; Joshi, A.; Finin, T. Generating Fake Cyber Threat Intelligence Using Transformer-Based Models. In Proceedings of the 2021 *International Joint Conference on Neural Networks (IJCNN)*, Baltimore Country, BC, USA, 18 June 2021; pp. 1–9.

[9] Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Ali, A.; Nasser, M.; Abdo, S. Anomaly Intrusion Detection Systems in IoT Using Deep Learning Techniques: A Survey BT—Innovative Systems for Intelligent Health Informatics; Saeed, F., Mohammed, F., Al-Nahari, A., Eds.; *Springer International Publishing: Cham, Switzerland*, 2021; pp. 659–675.

[10] Vorakulpipat C, Rattanalerdnusorn E, Thaenkaew P, Hai HD. Recent challenges, trends, and concerns related to IoT security: An evolutionary study. In: *2018 20th international conference on advanced communication technology (ICACT), Chuncheon-si Gangwon-do, Korea (South);* 2018. p. 405–10.

[11] Deepak, A., Shukla, P., Ganesan, V., and Shankar, P. Scrutinizing the Properties of Functionalized Graphene Based Polymer Nanocomposites for Electronic Devices, Materials Today Proceeding. (Elsevier)(2015).

[12] Renganathan, B., Rao, S.K., Kamath, M.S., Deepak, A**.,** Ganesan, A.R., Sensing performance optimization by refining the temperature and humidity of clad engraved optical fiber sensor in glucose solution concentration, Measurement: Journal of the International Measurement Confederation, 2023, 207,

[13] 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

[14] Sree Lakshmi, P., Deepak, A., Muthuvel, S.K., Amarnatha Sarma, C Design and Analysis of Stepped Impedance Feed Elliptical Patch Antenna Smart Innovation, Systems and Technologies, 2023, 334, pp. 63

[15] Gupta, A., Mazumdar, B.D., Mishra, M., ...Srivastava, S., Deepak, A., Role of cloud computing in management and education, *Materials Today: Proceedings*, 2023, 80, pp. 3726–3729

[16] P. 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.

[17] Deepak, A., Ganesan, V., and Shankar, P., Non-Destructive Evaluation of Graphene based strain sensor using Raman Analysis and Raman Mapping, Journal of Polymer Engineering, accepted September 17, (2015).

[18] P. William, G. R. Lanke, V. N. R. Inukollu, P. Singh, A. Shrivastava and R. Kumar, "Framework for Design and Implementation of Chat Support System using Natural Language Processing," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-7, doi: 10.1109/ICIEM59379.2023.10166939.

[19] Mall, S., Srivastava, A., Mazumdar, B.D., Bangare, S.L., Deepak, A., Implementation of machine learning techniques for disease diagnosis, Materials Today: Proceedings, 2022, 51, pp. 2198–2201.

[20] Bhargava, A., Bansal, A., Goyal, V., Machine learning-based automatic detection of novel coronavirus (COVID-19) disease, Multimedia Tools and Applications 2022.
[21] William, P., Shrivastava, A., Shunmuga Karpagam, N., Mohanaprakash, T.A., Tongkachok, K., Kumar, K. (2023). Crime Analysis Using Computer Vision Approach with Machine Learning. 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_25
[22] Agrawal, S.C., Jalal, A.S., Distortion-free image dehazing by superpixels and ensemble neural network, Visual Computer, 2022.
[23] Sharma, H., Jalal, A.S., An Improved Attention and Hybrid Optimization Technique for Visual Question Answering, Neural Processing Letters, 2002.
[24] Gupta, N., Janani, S., Dilip, R., Hosur, R., Chaturvedi, A., Gupta, A., Wearable Sensors for Evaluation Over Smart Home Using Sequential Minimization Optimization-based Random Forest, International Journal of Communication Networks and Information Security,2022.
[25] Swaminathan, B., Palani, S., Vairavasundaram, S., Kotecha, K., Kumar, V., IoT-Driven Artificial Intelligence Technique for Fertilizer Recommendation Model, IEEE Consumer Electronics Magazine,2023.
[26] Sachdeva, A., Tomar, V.K., Characterization of Stable 12T SRAM with Improved Critical Charge, Journal of Circuits, Systems and Computers,2022.
[27] 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.
[28] [2]. 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.