JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

THE PRETEND ARTIFICIAL INTELLIGENCE PODIUM FOR CLOUD DEFENCE

Dr.Pramoud Kumar[1] , Dr. D. Stalin David[2], Jai Rajesh P[3], Dr. Chinmaya Dash[4], Dr. Prakash Chandra Behera[5], Abhinav Singhal[6]

[1]Assistant Professor, Department of Computer Science and Engineering,Ganga Institute of technology and Management, Kablana Jhajjar Haryana-124104

[2]Associate Professor, Department of Information Technology,Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College,Avadi, Chennai-600062

[3]Assistant Professor, Department of Mechatronics,Bharat Institute of Higher Education and Research, Chennai-600073

[4]Assistant Professor, Department of Computer Science, St.Claret College, Bangalore

[5]Assistant Professor, Department of Sciences, St.Claret College, Bangalore

[6]Assistant professor, School of Sciences, Christ University, Delhi NCR, Ghaziabad -201003, Uttar Pradesh, India

pramod.gill1@gmail.com[1], stalindavid@veltechmultitech.org[2], jairajesh2008@gmail.com[3], Chinmaya@claretcollege.edu.in[4], prakash@claretcollege.edu.in[5], ism.abhinav@gmail.com[6]

Abstract:

Cloud security safeguards data against loss, fraud, and removal. In Cloud, several models and platforms secure important data and information. AI techniques have progressed substantially in recent decades, and their applications range from face identification to computer vision. AI-based technologies will increase cyber defence and assist opponents refine cyber attacks. Malicious persons are aware of the new opportunities and will likely abuse them. It combines AI with security experts' skills in vulnerability management and defence. Cyber AI automates cyber defence detection, reaction, and investigation. Cyber AI changes our ability to secure data networks and digital surroundings. Cloud security uses AI to authenticate saved data from several businesses. Market professionals use AI to enhance digital data processing. AI and Cloud computing are great for transforming technology. AI's tough challenges and machine learning thrive on enormous volumes of data, which is scalable on the cloud.

Keywords: Cloud Security, Artificial Intelligence, Cyber Security, Machine Learning

12.1 Introduction

These are some Cloud data storage systems. Many corporations and organisations use this place to safeguard their data, however it might be hacked. Cyber AI is suggested for Cloud security. Intrusion, illegal users, vulnerable protocols or functions, data theft, inaccessibility, remote information sharing, suspicious members, cyber assault, and DoS assaults are cloud difficulties. AI is when computers can execute human-like functions. It involves artificial intelligence, where computers learn without human input. Machine Learning is a subset of DL that obtains information using algorithms, Artificial Neural Networks, and data analyses.

Submitted: 21/10/2022 **Accepted**: 24/11/2022

Cyber AI analyses knowledge and behaviour, like the immune system. Uncertainty requires millions of forecasts for developing facts. Cyber AI Researcher sorts, monitors, and updates employee security violations. This will ensure Cloud security.

Cloud computing is a cloud database system that provides a variety of services. Basic programming may be used to create a system. They may be a Cloud-based interface or software-related network. Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service may be characterised as cloud computing platforms (PaaS). Earlier cloud storage had unique components. Service on demand is an important component of cloud services that allows customers to request the quantity of services they need. According to consumer need, SaaS, PaaS, and IaaS deliver applications, platforms, and infrastructure. In all facilities, customers' business facts and rules are supplied. Protect sensitive information and industry norms, and improve service. SaaS, PaaS, and IaaS need security. Despite fraudulent users, access authorisation, connection or route, data, and data processing, facility security is limited. Cloud Computing is also adaptable, allowing firms to scale up or down demand-based services to save money. Cloud Computing services are not securely tied to the consumer; instead, they are computed based on their usage while contributing to the cloud provider and are paid based on their use. Cloud computing's pay-per-use model has cut the cost of fixed-service apps and services. These characteristics have changed how sectors use cloud-based solutions. Personal cloud solutions such as OpenStack and VMWare adapt to particular user requests. Public cloud solutions such as AWS, Google cloud services, and Microsoft Azure.Since public cloud services are utilised, the public cloud framework is low- and mid-level. The cloud's shared and mid-design stimulate knowledge interchange, which increases the danger of sharing data and resources. Many worldwide firms and industries are hesitant to employ cloud environments since business-sensitive data isn't transmitted or compromised.This viewpoint highlights the complexity and significance of Cloud Security and the need for specialised and novel techniques to support cloud security. Many cloud-based data authentication protocols and recommendations released in recent decades have promoted cloud protection. Multiple access control mechanisms and advanced identity recognition, mitigation, and monitoring technologies have enhanced cloud safety policies.

12.2. Issues occur in the cloud security

94% of organisations worry about cloud security. Misconfiguration (68%) is the biggest security risk for public clouds, followed by unauthorised access (58%), unknown interfaces (52%), and data theft. Cloud security threats and concerns. Every company uses distributed computing to varying degrees. With this move to the Cloud, the company must ensure that its cloud security strategy can resist the main threats.

12.2.1 Unauthorized access

In contrast to an association's on-premises framework, their cloud-based arrangements are outside the organization edge and straightforwardly reachable via the public Internet. While this is a resource for the openness of this framework to representatives and customers, it

likewise makes it easier for an aggressor to enhance unapproved admission to an association's Cloud-based assets. Inappropriately built security or negotiated qualifications might enable an attacker to increase direct access, potentially without an association's knowledge.

12.2.2 Hijacking of account

Many people overuse private terms and use weak passwords. This vulnerability fosters phishing attacks and data breaches since a stolen key may be used on several records. Record hijacking is a growing cloud security risk as businesses rely increasingly on cloud-based infrastructure and apps. An attacker with a worker's credentials may access sensitive information or be beneficial, and a client's credentials give them complete internet access. In the Cloud, companies often can't anticipate and respond to these risks as effectively as on-premises.

12.2.3 External Sharing of data

The Cloud is meant to make information sharing easy. Numerous mists provide the option to welcome an associate by email specifically or share a connection that enables everyone with the URL to get to the shared asset. While this easy information exchange is a resource, it may also be a huge cloud security risk. The utilisation of connection based sharing a famous alternative because it is more simple than indisputably welcoming each suggested teammate-makes it hard to regulate access to the shared asset. The mutual relationship might be communicated to another individual, interpreted as a cybercriminal component, providing unauthorised entrance to the standardsupport. Furthermore, link based sharing makes it tough to renounce admission to a single benefit of the shared connection

12.2.4 Cyberattack

Cybercriminals choose their targets based on their predicted profits. Cloud-based framework is easily accessible from the public Internet, is often insecure, and holds sensitive data. The Cloud is used by many companies, hence a successful attack may likely be repeated with great success. Cyberattacks often target cloud-based associations.

12.2.5 Denial of Service Attack

The Cloud helps many organisations collaborate. They store business-critical data and operate internal and client-facing apps on the Cloud. This means a viable DoS attack on cloud framework will likely impact many enterprises. DoS attacks when the attacker demands a fee to terminate the attack pose a risk to cloud-based assets.

12.3.Cyber Artificial Intelligence Analysis

Before AI analysis, investigation of can sort begins with data assortment. The following are the different information sources from where information is gathered and afterwards examined.

12.3.1 Customerinformation

Customer information will be collecting and examining client access and exercises from AD, Proxy, VPN, and applications

12.3.2 Submissioninformation

Submission information includes the Collection and examination of calls, information trade, and orders and the Web Application Firewall information for introducing the specialists on the application.

12.3.3 Resultant data

Resultant data, analyzing the inner endpoints, for example, records, measures, memory, library, associations, and a lot more by introducing specialists

12.3.4 Web data

Web data comprises Network Forensics and Analytics products Collecting and dissecting the bundles, net streams, Domain Name System, and Intrusion Prevention System information by introducing the organization apparatus.

12.4. The impact of AI on Cybersecurity

AI may need two definitions. It aims to comprehend intelligence and construct intelligent robots utilising knowledge, reasoning, and awareness. Intelligent devices are human-made. AI can read, analyse, determine, and solve issues. Artificial Intelligence provides solutions to tackle ambiguous situations. Using big data, researchers may build an AI framework for decision making and real-time analysis. AI has led to computerised robots, facial recognition, language structure, and intelligent agents.

Computers and the Cloud change people's lives and jobs. It's created cybersecurity difficulties. Data growth first eliminates assessment. Second, rising risks cause shallow ecosystems and fast-resilient threats. Dangers alter distribution, replication, and avoidance techniques, making them unpredictable. Avoiding vulnerabilities is expensive. Programming requires time, resources, and energy.

Recruiting and training specialists is difficult and costly. Danger fluctuates constantly. AI-based cybersecurity solutions are needed.

12.4.1. The Positive Uses of AI

AI is utilised to improve cybersecurity defences. AI will examine large amounts of data with accuracy, precision, and importance, thanks to its optimization and data processing technologies. An AI framework should identify prior risks to detect relevant dangers in context, even if their tendencies change. AI's strengths in criminal defence include:

Traditional intelligence relies on experience; AI improves assault adaptability. It relies heavily on confirmed hackers and threats, leaving blind spots in forecasting odd activity. By intelligent technology, traditional defence flaws are explored. Rich intranet behaviour can be

recorded, therefore any large deviation in user authentication might signal an existential danger. If the computer can accurately recognise comparable models in context, the actions will be more genuine. With more information and situations, the computer can better comprehend and recognise aberrant, faster, and more precise behaviours. This is critical as cyberattacks improve and attackers employ new strategies.

AI can manage information and increase security by building intelligent protection solutions to recognise and respond to threats. Regular safety alerts might be overwhelming for security groups. Dynamically identifying and reacting to assaults reduces the involvement of information security specialists and helps detect threats more effectively than previous ways. Network security experts will have problems monitoring and identifying threat factors. Every day, a lot of safe data is created and delivered online. AI will monitor and identify questionable behaviour. This helps cybersecurity experts adapt to new situations and eliminates time-consuming people-searching.

Over time, an AI defence framework may adapt to respond quicker to assaults, based on user activities and system functioning. Over time, the AI safety system learns everyday activities and behaviour and provides a backdrop. Any standard deviations may be used to detect intrusions. AI algorithms increase cybersecurity protection controls.

Cognitive computing, machine learning, expert systems, automated immune systems, data analysis, problem-solving, causal, Deep Learning, and Machine Learning are used to counter assaults. Deep Learning and Machine Learning have garnered the best success in fighting cyber-attacks.

12.4.2. Drawbacks and Limitations of Using AI

Data sets: Designing an Artificial Intelligence framework requires a large number of input samples. It can require a significant period and several money to collect and analyze the sample data.

Resource specifications: An enormous number of resources, especially storage, information, and computational power, are needed to construct and retain the primary system. Besides, the professional personnel required to incorporate this technology entail considerable costs.

Fake notifications: For customers, repeated fake notifications are a concern, affecting the enterprise by possibly frustrating any required reaction and consequently reducing performance. The perfect procedure is an exchange between reducing fake notifications and retaining the level of protection.

AI-based device attacks: Hackers can use different intrusion methods that involve AI systems, such as aggressive inputs, data manipulation, and software theft. The illegal use of AI is one significant factor to be taken into consideration. This framework can also be used as a method to increase risks. Cybercriminals, for instance, can exploit the ML techniques to produce a malicious system model that is difficult to detect. Moreover, AI will be able to personalize the

malware system further and increase the intrusion scale, allowing the threat more possible to be successful.

12.5. AI Methodology for Cybersecurity

12.5.1. Learning Methods

AI is an information technology field that aims to create a modern form of an intelligent algorithm that reacts like human intelligence. Systems need to train to attain that objective. To be more specific, using the ML techniques, we have to educate the machine. Typically, learning methods help to increase efficiency by understanding and practising from knowledge in achieving a mission. At present, there are three main categories of learning methods used to educate devices:

Supervised Learning: Supervised Learning involves learning with a broad and recognizable collection of already labelled data. As a selection process or correlation process, these learning methods are also used.

Unsupervised learning: Unsupervised learning methods use unidentifiable data sets, as compared to supervised learning. These methods are also used for data clustering, dimensionality reduction, or depth estimation.

Reinforcement learning: It is a kind of learning method focused on encouragement or penalties to determine the right acts. For circumstances where data is minimal or not provided, reinforcement learning is effective.

12.5.2. Machine Learning Models

Machine learning is a category of Artificial Intelligence that seeks to motivate processes without having specifically configured by using knowledge to understand and develop. ML has broad links to computational approaches that facilitate knowledge extraction, pattern discovery, and information forming assumptions to be processed. The ML model has various forms, and they can typically be grouped into three key areas: supervised learning, unsupervised learning, and reinforcement learning. In the informationsecurity domain, the standard ML algorithms are Support Vector Machines, Decision Trees, Bayesian classification, Association Rule Mining, etc.,

12.5.3. Deep Learning Models

Deep learning (DL) is anML discipline, and it requires knowledge to educate machines how only people are trained to do stuff at that period. Its purpose resides in the human mind and brain cells' functioning methods to interpret signals. The essence of deep learning is that their efficiency improves as we build more comprehensive NN and educate them with the data as necessary. Its excellent output in complex data is the main significant benefit of DL over traditional ML. DL approaches can include supervised learning, unsupervised learning, and reinforcement learning, equivalent to Ml algorithms. DL's advantage is the advantage of unsupervised learning to pick functions randomly. In the cybersecurity domain, the standard

DL algorithms widely used are: Convolutional Neural Network, Graph Neural network, Recurrent NeuralNetworks, Deep Belief Networks, Stacked RNN, etc

12.5.4. Bio-Inspired Computation Models

Bio-inspired computing is a subfield of AI that's become important in recent decades. It's a combination of academic models and strategies that follow bio-inspired behaviours and qualities to solve challenging intellectual and field challenges. Bio-inspired cybersecurity uses the following approaches: AI, GA, Ant Colony, etc.

12.6. AI-Techniques for Preserving Against Cyberspace Attacks

Researchers have offered several techniques that have employed AI approaches to detect or classify ransomware, identify system breaches, spoof and malicious assaults, address Advanced Cyber Threat (ACT), and acknowledge domain established by algorithms developed by domain Generation algorithm (DGAs) (DGAs). There are four primary strategies employed against cyberspace assaults as Malicious Identification, Intrusion Detection System, SPAM and Phishing Identification and other procedures, which weaken the disputing of ACT and the Identification of DGA. The key AI approaches for cybersecurity are presented in Figure 12.1.

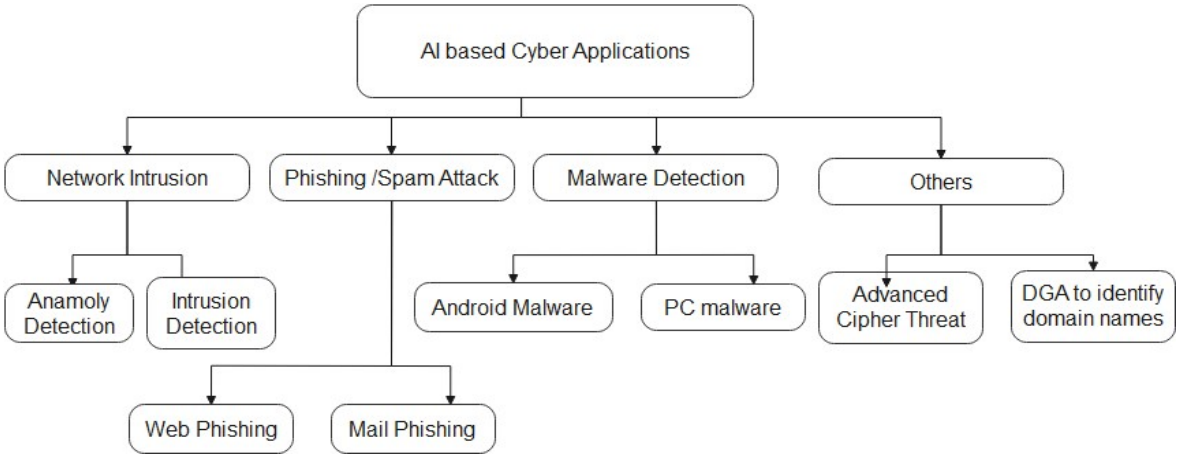

Figure 12.1:AI techniques for cyber applications

12.6.1. Identification of Malware

Malware is a popular term for harmful software such as bugs, zombies, computer viruses, hackers, and adenoviruses. It's also a typical cyber-attack strategy. Malware's impact on digital society is huge, hence AI has been used to prevent and lessen it. Recent improvements in malware detection and prevention leverage knowledge. In [9], the author presented Machine Learning to construct a digital platform for hardware-assisted malware detection. Simulations employed logistic regression, an SVM, and an RFC on the RIPE comparison set. With a false predictive rate of less than 5%, the system has a 99.9% accuracy. [10] suggested an approach for recognising and locating malicious code using knowledge discovery and ML. This article

analyses stamp-based and outlier-based identifying characteristics. The recommended methodology outperformed similar strategies, according to research. Another system[11] employed OpCode, KNN, and SVM to classify malware using ML. The OpCode was represented as a graph in Euclidean space, and each variable was identified as malware or neutral by one classification model or an aggregate. The results showed that the recommended strategy reduces bogus notifications and increases discovery. [12] built a deep learning system for malware detection. In this work, they deployed multilayer Restricted Boltzmann machines to detect malware (RBMs). The author stated that clustered deep learning frameworks may boost malware detection outcomes. Recent malware testing has emphasised online and android malware. ML with DL was a major advance. [13] proposed a CNN to categorise malware. Malware is identified using a program's raw OpCode. [14] employed an SVM and permission data to discriminate between good and hazardous applications. [15] presented rotating forest, an ML algorithm for malware discovery. [16] employed an ANN and API process calls to discover Application malware. Currenttraining [17] established a dual strategy ba sed on a Deep Auto Encoder (DAE) and a convolutional neural network to enhance large-scale Software virus detection (CNN). Bio-inspired ways for identifying malware also interested scientists. These techniques were used to improve features and classifiers. In [18], particle swarm optimization (PSO) was applied; in [19], the genetic algorithm (NN) improved malware detection.

12.6.2. Detection of Intrusion

An intrusion detection system (IDS) protects against possible or imminent threats. AI-based techniques are appropriate for building IDS and other approaches since they are versatile, efficient, and rapid. Many scientists are researching clever IDS processes. Optimizing functionality and strengthening the categorization model helped reduce bogus news. Here are some key results.

An IDS framework [20] used SVM and deep learning with updated k-means. Using KDD'99 Cup datasets, their model had 95.75 percent accuracy and 1.87 percent bogus notifications. [21] suggested a sampling-based Least Square SVM architecture for IDS. The recommended technique was tested for reliability and efficacy using KDD'99 Cup datasets. [22] suggested an uncertainty-based semi-supervised IDS learning approach. Using unidentified instances and supervised learning, they improved the classifier's accuracy. On the KDD'99 Cup dataset, the algorithm outperformed other approaches.

12.6.3. Phishing and SPAM Identification

Cybercriminals use phishing to steal personal or financial information. Phishing is a scary cyberthreat. Several complex strategies have been developed to address these problems. In[23], authors presented a phishing identification system using neural networks and reinforcement learning. Their model was 98.6% accurate and 1.8% incorrect. In[24], the authors devised an anti-phishing solution using 19 ML features to distinguish phishing websites from authentic ones. Their strategy yielded a 99.39% true positive rate. Monte Carlo equation and risk reduction theory categorise phishing websites using a neural network. Their model attained a

97.71% identification rate and a 1.7% bogus identification rate. A recent research built a real-time anti-phishing system with natural language capability. The authors say their technique achieved 97.98% accuracy. Another research used Hyperlink and Markup to detect phishing web pages by combining LightGBM, XGBoost, and GBDT. Their approach reached 98.60% accuracy. Spam is unwelcome e-mail. Spam emails cause security issues and incorrect information. To combat cyber-threats, researchers have created sophisticated spam filter algorithms.

12.7. Issues of Artificial Intelligence platform for Cloud Security

- . Several AI solutions rely on intelligent assistants to improve cybersecurity data processing. In cloud computing and open stack frameworks, IT is threatened by a lack of privacy expertise, which threatens solid algorithms and machine learning applications. Information and design technologies encounter special dependability concerns.Inadequate security expertise is a recognised fact. 52% of companies reported a cybersecurity skills gap in 2018. Emerging technologies, alerts, and data continue to rise, increasing security teams' obligation to understand and defend them. In 2017, newflaws quadrupled from 2016. Exhausted security researchers will embrace AI. Security teams will be well-prepared with quantifiable information and focus on mitigating critical security risks by dedicating the initial step of analysis and description to 'bots' totally or partly, improving threat identification and restoration.

  Warnings

- identifying key problems
- Give priority to threats;
- Track actions and methods with Security Threats.
- Identifying suspicious activity.

12.7.1.Challenges and Solutions of Data Security

The next obstacle for businesses, beyond the AI excitement, is to consider what the security best practices are for each latest AI system. It brings with attack surfaces (and security flaws) that attackers can use to recover data, as with any emerging technologies:

A. **Platform:** many businesses use Cloud services, Azure, but this does not eliminate the requirement to monitor and implement best practices for cloud security configuration implementation, even though we respect our cloud services.
B. **Virtual Cloud:** keeping track of all properties, such as databases, networks, memory, storage, is essential for infrastructure and services.
C. **Security of applications, APIs and staffing levels:** often the most noticeable and open aspect that fundamental web assaults can abuse. They can also be available publicly!

D. **Protection of messages:**The communication system must adopt standards of privacy and honesty.
E. **Capacity:** With network access, privacy, honesty and accessibility, the stored data must be secured.
F. **Data security during implementation:** a more complicated topic than the others, with significant development in asymmetric cryptography.

An Encryption helps with D and E. People using a cloud service may save authorization codes' authority and employ Cryptographic Algorithms. Both cloud services provide authentication so users may protect themselves while adhering to standards. New research on homomorphism encryption are expected to play a major role in cloud data services for attack material F by allowing powerful data analytics in encrypted data without compromising authentication.

Unlike traditional systems, anybody with a business credit card may use the newest cloud services. Financing and spending evaluations are one approach to regain track of Virtual Cloud (B). On-demand payment helps detect new needs and manage resources more effectively, even though identification is frequently halted by the invoice deadline. Intermittent or continual property monitoring is a safer Cloud practise[24-45]. This makes inconsistencies and expenses more visible. Automatic demand estimates (and payment) from APIs make this control possible.

Start with Substance A's Configuration Benchmarks. Amazon Web Services and Microsoft Azure both have one. Monitors cover "standards" organizationally and automatically. Cloud Protection Association-drafted measures will be included.

12.8. Cloud security

Cloud security includes all software technologies, organisational methods, and efforts to improve cloud network resilience. Cloud protection ensures data privacy and Cloud structure. This depends on needs, cloud service, and cloud protection techniques. As a businessperson and service provider, adopt cloud protection techniques to safeguard data.

Key cloud security objectives include:

Protect your records, including property rights, in the Cloud (IP); • Preserve employee and customer confidentiality and private identifying data; • Adhere to regulatory procedures; • Validate cloud network access devices and users.Company-specific cloud privacy may be customised. Verifying users and controlling dangerous traffic will fulfil these demands.

12.9. Strategies for Cyber Security Efficiency Metrics
12.9.1Insufficient Elimination of Data

The Collection of information about occasions not valid for the recognition period is taken as excess data. In this way, data is collected to extend the presentation. As shown in Figure 12.2, the data is directed to the programming advancement section after removing insufficient information to classify digital breaches. Finally, using perception components, the results are predicted.

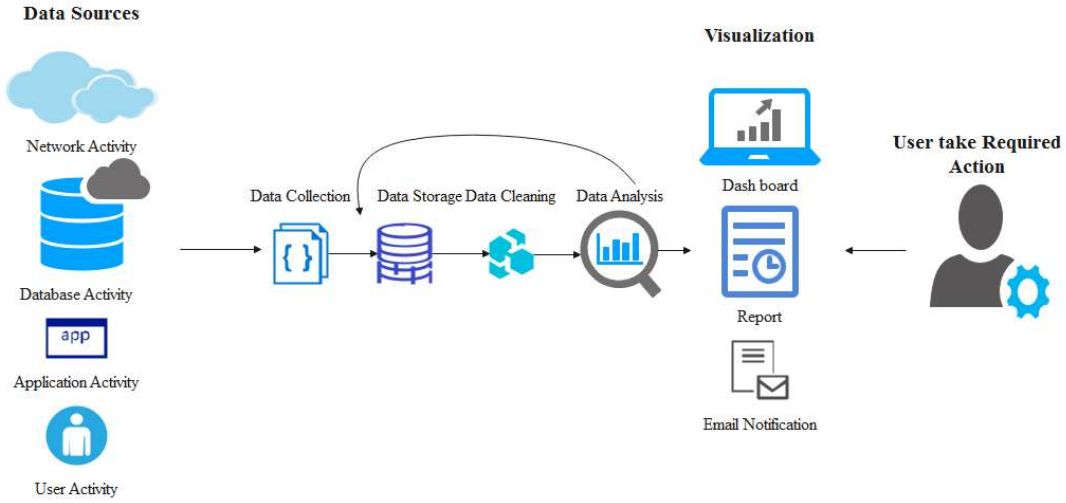

Figure 12.2: Insufficient Elimination of Data

12.9.2 Feature Extraction and Selection

Feature extraction and selection is shown in Figure 12.3. The component extraction and highlight choice cycles permit equal handling capacities to speed up the determination and extraction measure. At that point, the removed element dataset is sent onto the information examination module that plays out an alternate activity to breaks down the reduction in the size of thedataset to distinguish digital breaches.

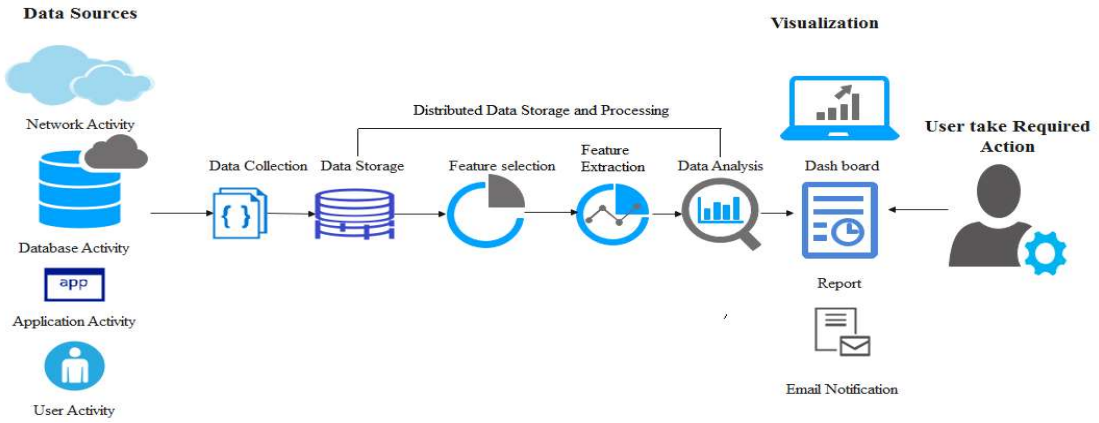

Figure 12.3: Feature Extraction and Selection

Preventive measures are recommended in situations of an attack that can be interpreted by the client using the interpretation section. A business or customer may find a way to minimize or thwart the attack's effects if these attack warnings go under notifications.

12.9.3 Data Cut-off

The information cut-off section imposes the cut-off by ignoring security events after an organization's or cycle's limit. Any security event that comes after maximum doesn't contribute to the attack discovery measure; thus, analysing these events adds weight to information handling resources without a measurable increase. Figure 12.4 shows how the information storage material may store security event data after cutoff. Information investigation reads stored data to discover digital attacks. The results of the assessment are presented to the customer in a report, allowing them to act upon each red flag.

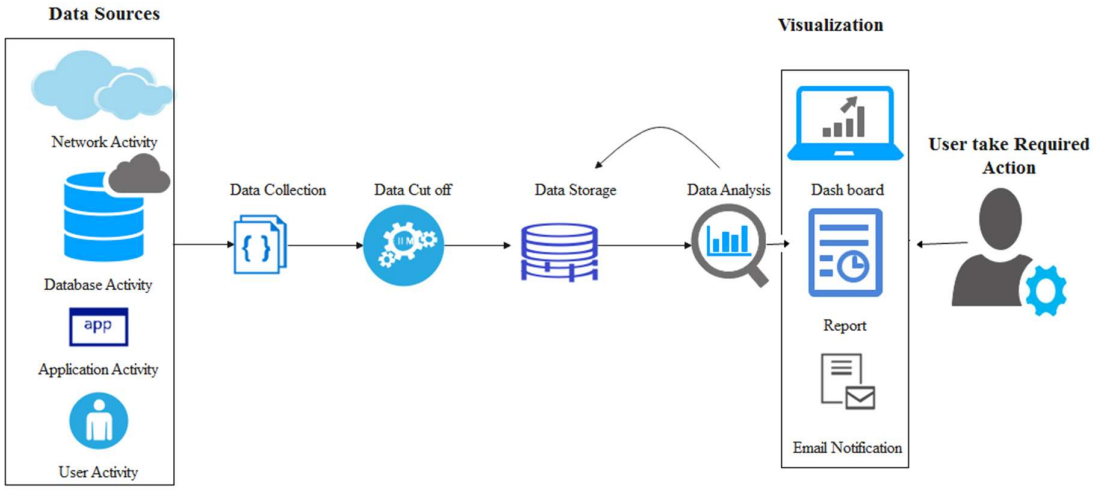

Figure 12.4: Data Cut Off

12.9.4 Parallel Processing

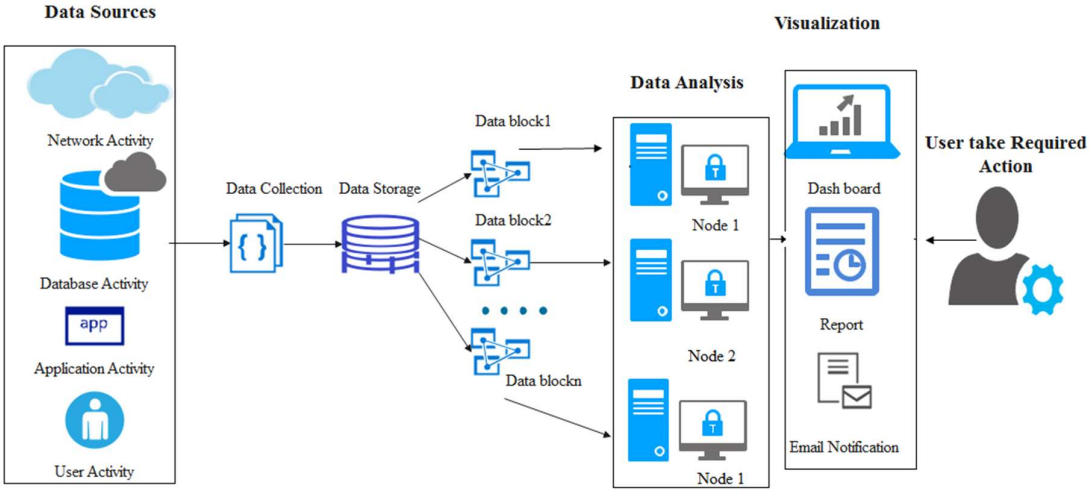

Figure 12.5: Parallel Processing

The information authority substance collects security event data from numerous sources according on the security investigation and project needs (Figure 12.5). Information gathered is sent to a data storage material. Hadoop File System, HBase, and Relational Database may store data. Put-away information should be in data blocks for equitable treatment. After splitting, information is imported in the information examination segment via many hubs functioning in equal based on Spark or Hadoop rules. Perception gives the customer the exam result.

12.9.5 Training Models used for Cyber AI

The information collection substance collects security event data for a security investigation framework's preparation cycle. Preparation information might be gathered from sources inside the project. After gathering preparation information, the information readiness segment sets up model preparation information using several channels. From then on, the chosen ML computation is used to construct an attack identification approach. The processing time needed to develop a design varies.

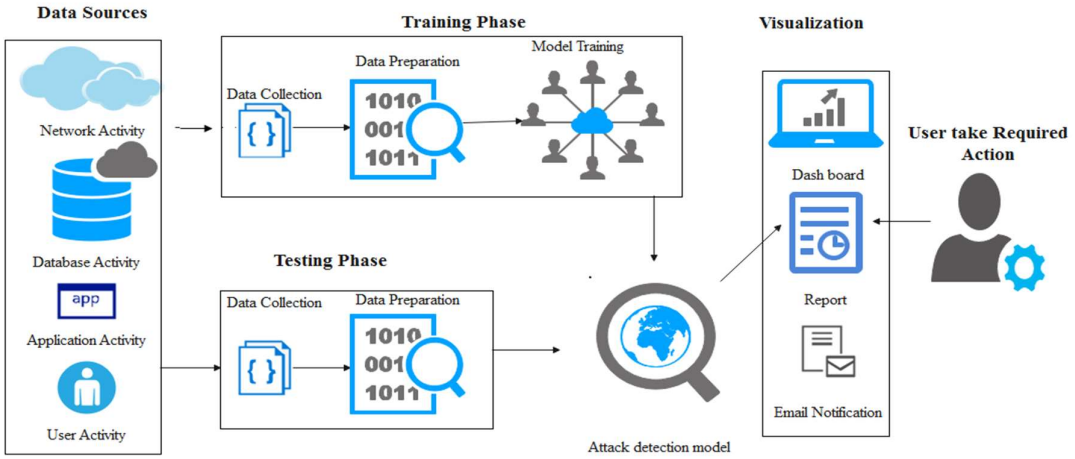

Figure 12.6:Training Models used for Cyber AI

After the model in Figure 12.6 is developed, it is required to explore how digital threats may be recognised by the model. Information is gathered using an activity for model research. Via the information arrangement system, the data to be tried is separated and brought into the attack position system, which is used to analyse the data to identify the attacks based on the criteria identified via the planning phase. The duration is employed by an attack identification model to determine whether a given flow of information associated with an attack (i.e., option time) depends on the quantified measurement. The outcome of the data analysis is presented to the consumer through a perception variable.

12.9.6 Accuracy in Security Models

12.9.6.1 Alert Correlation

The information aggregation section then collects security opportunity details from diverse assets and sends them to the per-processor section for pre-handling. The ready review module swallows pre-treated data to spot assaults. Figure 12.7 shows that it Alert analysis unit presents data in an outdated way, depending on inconsistency or abuse-based analysis. The readiness validation unit utilises multiple techniques to determine whether an alert is dishonestly safe. False positive warnings are disregarded.

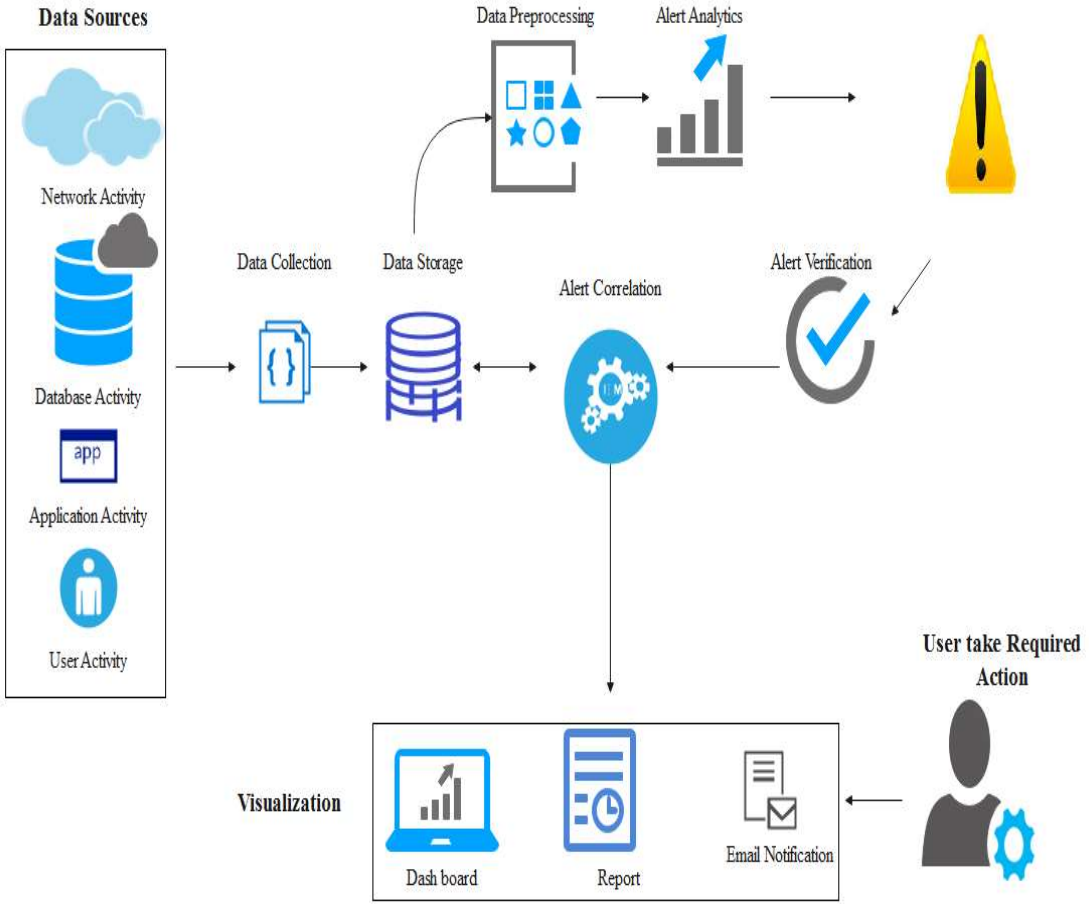

Figure 12.7: Alert Correlation

The well-orchestrated warnings are forwarded to the ready connection module for inquiry. From then, the alerts are linked (intelligently connected) using different tactics and computations, such as rule-based, situation-based, ephemeral, and quantifiable. Alert connects to data stockpiling to gather logical warning data. Representation publishes interaction implications. Neither a robot nor a security chairman examines the risk and responds automatically.

12.9.6.2 Signature Based Anomaly Detection

In Figure 12.8, the information collection portion acquires security-relevant assets. The information accumulating module then stores the acquired data. Next, mark-based recognition

investigates the information to find attack instances. This component of the study uses pre-planned criteria from states that recognise assaults. A representation module creates an alert if a match is found.

If the mark-based identification section doesn't identify any assaults, the information is forwarded to the peculiarity-based location part to locate obscure attacks. A peculiarity is anomalous information or behaviour. This indicates a framework error. The peculiarity-based identification module uses AI to identify departures from normal behaviour. The representation module creates an alert when an irregularity is detected. The oddity is categorised as an assault example or rule and uploaded to the standards database. The rules database is constantly updated to help the mark-based location segment identify attacks.

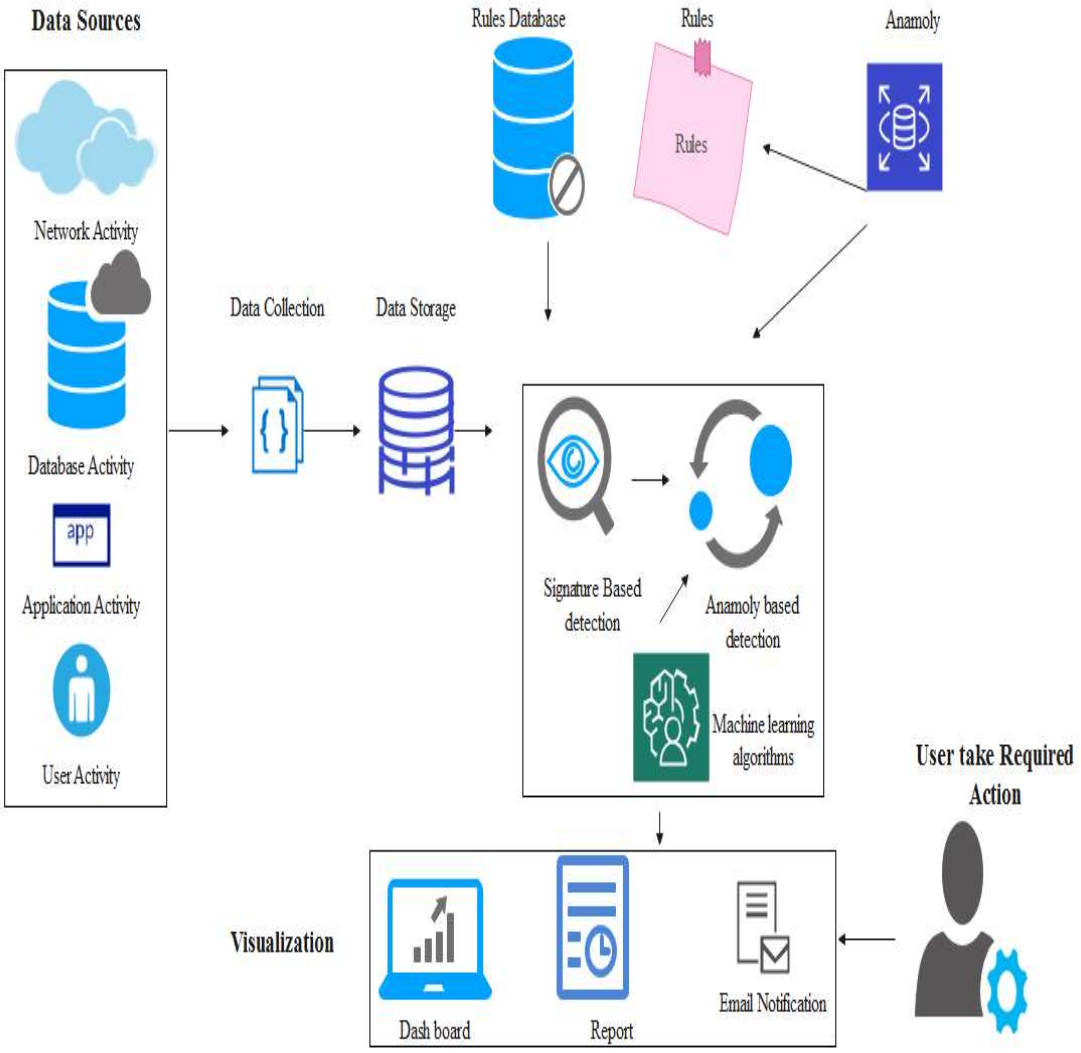

Figure 12.8: Signature-Based Anomaly Detection

12.9.6.3 Attack Detection Algorithm

The section collects security event data to develop the scientific security framework for spotting digital attacks. Preparation information may be acquired from numerous sources inside a project. After the information collection cycle identifies preparation information, the information planning unit prepares the model by inferring channels and highlight extraction techniques.

Figure 12.9 shows how ready planning data prepares the module for attack detection. When ready, the unit may check whether the system can distinguish digital assaults. A company's data approves the technique. Sample data is available for attack identification. The assault position model evaluates ready test data based on planning-phase criteria. Test knowledge instances are either malicious or valid. The perception unit shows a client the investigation's results. In malevolent or assault models, a client may close ports or cut off damaged firm sections to minimise additional harm.

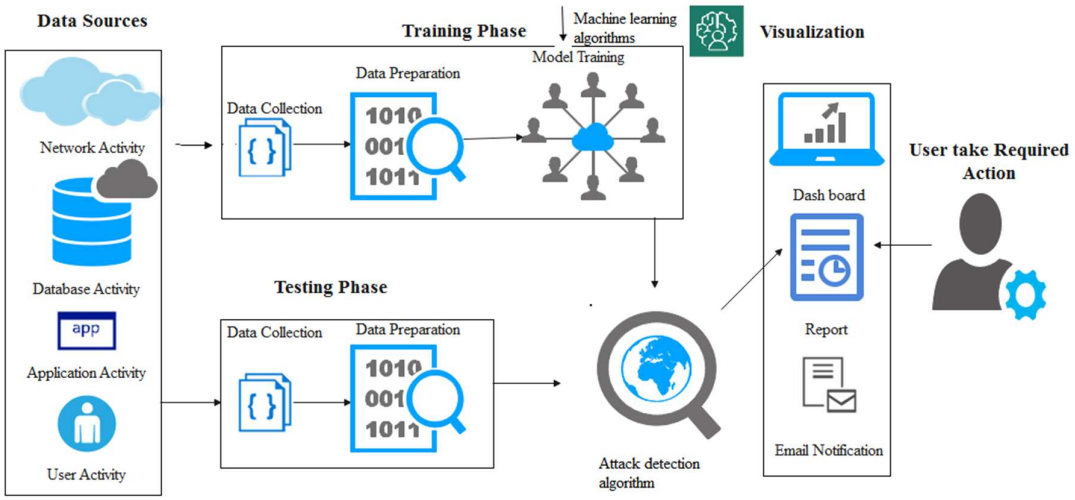

Figure 12.9:Attack Detection Algorithm

12.10. GPU based CNN-MSVM cloud security system

The CNN-MSVM GPU-based cloud protection framework aims to establish a dependable and powerful cloud security based on machine learning by evaluating data patterns and recognising deviations and abnormalities. ML-based cloud protection helps reliably and clearly detect irregularities. To categorise assaults, the dataset's transfer rate, contact time, and other factors are investigated. By calculating TP, TN, FP, and FN across UNSW-NB15 and ISOT Botnet datasets, fraudulent risks are reduced. Figure 12.10 shows the whole eco-system.

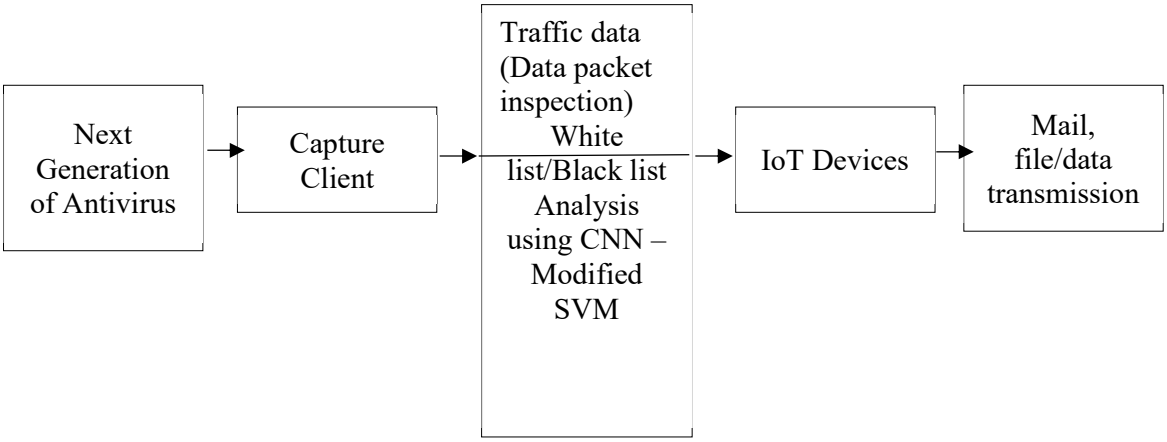

Figure 12.10: CNN-Modified SVM Cloud Security System

Figure 12.11 shows the topology of an ML-based cloud security system. This approach benefits from Machine Learning Classification Models and Artificial Intelligence at multiple layers of the cloud network (AI). Based on the diagram, in addition to traditional antivirus software, operating system firewalls, etc., the suggested method uses Artificial Intelligence techniques of the next decade to collect and analyse customer feedback even at the entry-level to ensure no unusual data reaches the cloud-based framework. Protection must be offered at three stages: the point of entry where the customer request is accepted, the network interface privacy, the cloud framework, and the end state where the system user model resides. Each data stream is encoded/decoded when preprocessed, retrieved, and evaluated using ML algorithms to discover and alert anomalous packets. These packets are sent to the cloud layer, allowing just the right ones through.

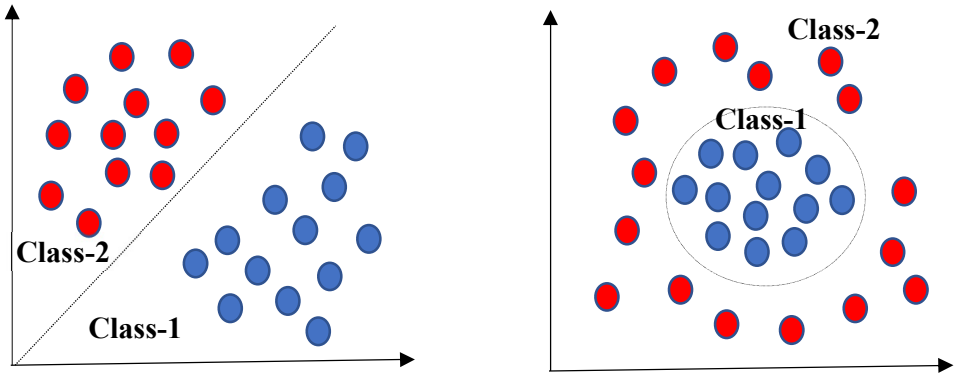

Figure 12.11: Support Vector Machine

12.10.1 Modified Support Vector Machine

Different categories found in the datasets can be identified by the Modified SVM Classification model. The SVM grouping is shown in Figure 12.11 and 12.12, while Figure12.11 displays the classification model of the Modified SVM. The SVM classification

model, based on the feature space, qualifies two or more groups. Each feature space in Modified SVM allows the data as group 1, group 2, group 3, etc., into several groups.

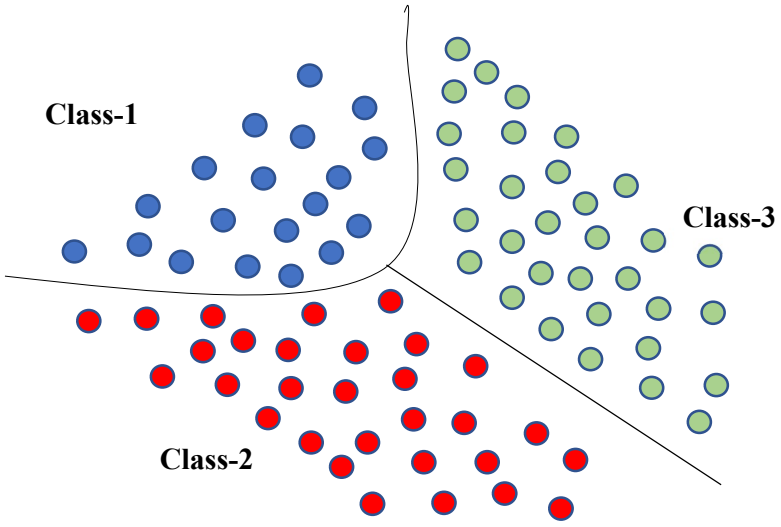

Figure 12.12: Modified Support Vector Machine

12.10.2. GPU based CNN architecture

The GPU based CNN framework involves the use of ML system-based categorization to identify any unusual activity in the cloud framework based on analysis of data. In this case, the GPU based CNN framework is used for anomaly categorization. The cloud source data is feed to the CNN system. This involves introducing many shared information levels as a convolutional layer, and at each convolution point, the knowledge is converted into many types. The GPU-CNN output consists of various feature variables that act as the entry to the classification model of the Modified SVM. The ultimately linked layer in the GPU-CNN typically identifies the final variable data where its length is two or three and eventually decides the unusual groups.

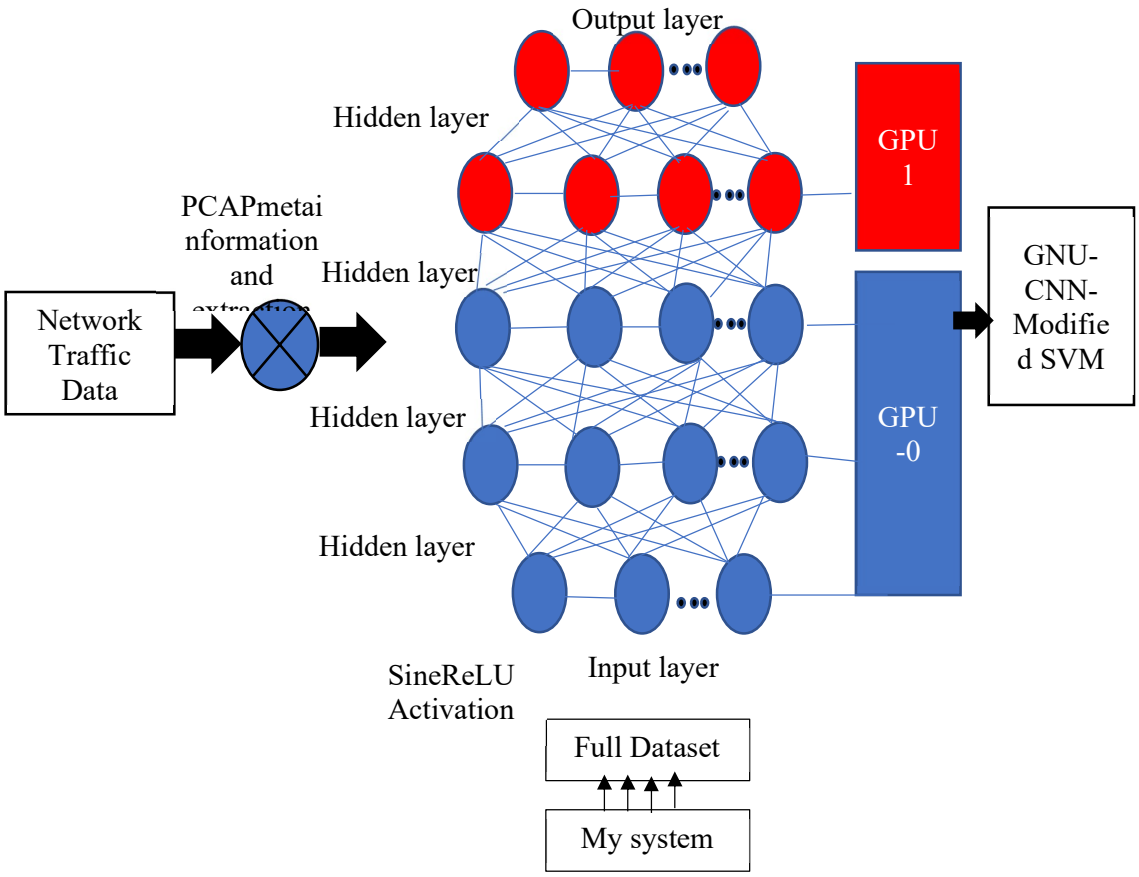

Figure 12.13: GPU-CNN-Modified SVM Functionality

Five categories define irregularity: source node, destination node, connection accuracy, time duration, and notification pattern. Increased performance vector. To detect aberrant groupings, GPU-output CNN's variable is modified using SVM. GPU-secret CNN's results are accurate. Modified SVM labels the GPU-CNN output variable to categorise the same data category. This Modified SVM classifier organises cloud network operations based on data. The collected characteristics classify real-time cloud framework operations as normal or abnormal. Figure 12.13 shows GPU-CNN. Hidden layers might range from 1 to 10. 5-layers is optimal. SineReLU triggers all hidden levels. All matrices and consolidating tales are important, and 250 measures. GPU-CNN reduces data size from the matrix to the variables. The real variable is the function introduced to the Modified SVM to determine regularity.

12.10.3.Data Traffic analysis for GPU based CNN network

Figure 12.14 shows a test model of the data structure and empirical setup. GPU-based convolution neural network contains one hidden layer, one activation function, and accumulated layer contortions. Entry, output, and interface fields are removed due to design. All raw data is fed into hidden layers and processed into convnet arrays. Convent and pooling

levels know entire outcome characteristics. All convnet accumulation levels are dubbed hidden layers because they collect and recover secret source data after approximation.

Source IP, Source port, Destination IP, Destination Port, Protocol, Flow Bytes, Flow duration, Flow IAT mean, Flow Packets, Flow IAT Max, Flow IAT Std, Flow IAT min, Fwd IAT Mean, Fwd IAT Std, Fwd IAT Max, Fwd IAT Min, Bwd IAT Mean, Bwd IAT Std, Bwd IAT Max, Bwd IAT Min, Active Std, Active Mean, Active Max, Active Min, Idle Mean, Idle Std, Idle Max, Idle Min, Active Std, Active Mean, Active Max, Active Min, Idle Mean, Idle Std, Idle Max, Idle Min, Label, 10.0.2.15, 53912, 216.58.208.46, 80, 6, 434, 0, 4597.7011494252, 435, 0, 435, 435,0, 0, 0,0, 0, 0, 0, 0, 0, 0, 0, NON-TOR

Figure 12.14: Sample data

Modified SVM activates output. Modified SVM employs "Normal" and "Abnormal" to identify performance. Keras and TensorFlow are used to train the CNN model in GPU-CNN and Modified SVM. Cross-entropy is used to assess loss to enhance GPU-CNN. Multiple repetitions teach the advised strategy. Figure 12.13 shows the CNN-ModifiedSVM GPU-based model specification to boost the efficiency of identifying anomalies and regular data with minimal failure for longer epochs. Figure 12.15 compares the performance of GPU-based CNN-Modified SVM to Linear Regression, Support Vector Machine, Naive Bayes Classification, and Random Forest classification. Accuracy, remembering, and F-score evaluate categorising ability effectiveness. GPU-CNN-Modified SVM can identify TOR-10class.

Identifying NONTOR-10 is also required and assessed. According to private results, GPU-CNN-Modified SVM reduces NON-TOR Function Point occurrences. Figure 12.16 shows contrast's impact.

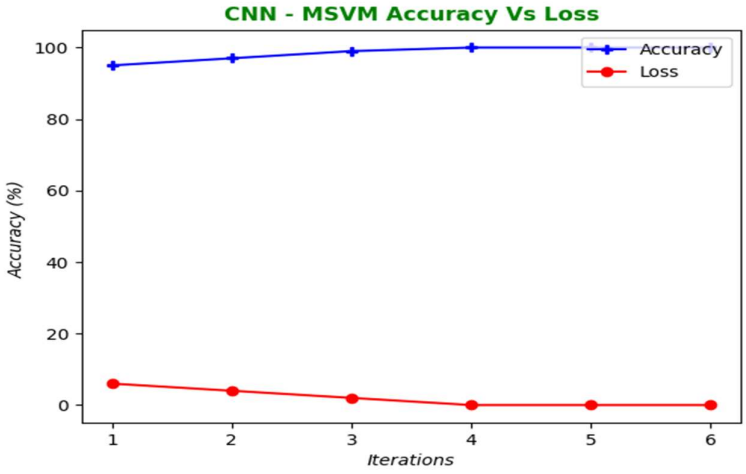

Figure 12.15: CNN-Modified SVM Accuracy Vs Loss

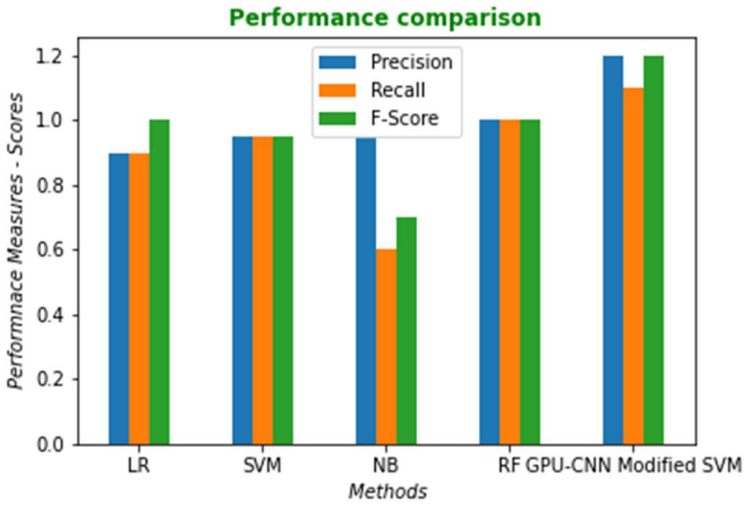

Figure 12.16: Performance Comparison

12.10.4. Benefits of AI and machine learning for cloud security

AI and ML may not be magic AI and ML aren't magic bullets, but they can improve Cloud security. 95% of firms use the cloud for at least some of their operations, according to Gartner. Despite increased cloud adoption, many IT practitioners still view the Cloud as a security vulnerability in their company, and 50% of firms anticipate to increase cloud protection costs in the coming year, according to a Cybersecurity Experts report. Some firms are using AI and ML to increase cloud security and minimise hacking risk. AI can complete problems and learn autonomously, much like humans. Machine learning uses an algorithm to enhance AI outcomes. The more statistical approaches it assesses, the more it integrates and self-adjusts abnormalities, making its findings more important.Cybersecurity technologies generate more data than any human team can review. ML uses this data to discover attack flaws. The more it learns, the more variations it recognises and observes, which it uses to identify pattern variances. Shifts may include cyber concerns. Machine learning notes when and where employees connect into their systems, what they habitually access, and other traffic and user behaviour trends. Signing in early in the morning is a variation on these concepts. Possible assaults may be highlighted and repelled faster.By using a more information-driven technique, man-made brainpower may uncover and proactively warn on inadequacies and weaknesses being mistreated now or that may be abused later. This works by evaluating information arriving via protected endpoints, identifying existing threats and predicting future dangers. This more prophetic strategy captures all endpoint movement data, not just the 'bad' action, and improves it from numerous sources to assist address the fundamental derivers of a projected attack, rather than just minimising its affects. It may assist shorten the cycle between detection and remediation by giving security teams greater information.When AI and AI technologies analyse system data and find anomalies, they may alert a human or terminate a

client's account. By taking these steps, events are often recognised and stopped within hours, preventing the spread of potentially dangerous code and a data leak. This cycle of examining and linking geoscience data gives companies more time to react to security threats.Alarms regarding prospective hazards or irregularities are common in many security levels, but mechanical developments may eliminate most of the noise to focus on the important things. When AI handles mundane tasks and first-level security checks, security teams may focus on more basic or complicated threats. This is important given network protection limitations. 51% of firms report a difficult shortage of network security skills. By assigning bots the main level of investigation, security specialists may focus on more difficult attacks. This doesn't imply these developments can replace human specialists, since digital attacks often originate from both humans and robots and need responses from both. It helps examiners arrange their work.

Conclusion

New cybersecurity concerns have arisen due to IT advancements. Cyber-attacks are becoming more mathematically sophisticated, efficient, and adaptable. This chapter discusses AI-based cybersecurity. AI is used to detect threats, scan vulnerabilities, filter spam, and identify malware. AI implementation in cybersecurity focuses on IDS, anomaly detection and classification, spoofing, and email attachments. In these locations, DL deployment is a growing trend. ML/DL and bio-inspired techniques also piqued researchers' attention. Such changes provide favourable results and encourage more research. AI's role in solving cybersecurity difficulties is still being investigated, however AI-based defences have several glaring drawbacks. Intelligent software malware is one threat to AI. Further research is needed to find solutions to these difficulties. For cloud protection.

GPU-based CNN-Modified SVM is employed. All input data is sent into the GPU-based CNN model's hidden layers. This effort aims to improve cloud protection learning methods. It also implements scientific work utilising GPU-based CNN and Modified SVM. Experimental findings and output assessment show that enlarged supervised ML approaches are useful in real-time cloud services. Experiments on multiple datasets validate GPU-based CNN-Modified SVM's performance.

References:

1. David, D. S., Arun, S., Sivaprakash, S., Raja, P. V., Sharma, D. K. et al. (2022). Enhanced Detection of Glaucoma on Ensemble Convolutional Neural Network for Clinical Informatics. CMC-Computers, Materials & Continua, 70(2), 2563–2579.
2. David, D. S., Anam, M., Kaliappan, C., Arun, S., Sharma, D. K. et al. (2022). Cloud Security Service for Identifying Unauthorized User Behaviour. CMC-Computers, Materials & Continua, 70(2), 2581–2600.
3. Jayachandran, A., and D. Stalin David. "Textures and Intensity Histogram Based Retinal Image Classification System Using Hybrid Colour Structure Descriptor."

Biomedical and Pharmacology Journal, vol. 11, no. 1, 2018, p. 577+. Accessed 12 Feb. 2021.

4. D. Stalin David, 2019, “Parasagittal Meningiomia Brain Tumor Classification System based on MRI Images and Multi Phase level set Formulation”, Biomedical and Pharmacology Journal, Vol.12, issue 2, pp.939-946.
5. Thendral R., David D.S. (2022) An Enhanced Computer Vision Algorithm for Apple Fruit Yield Estimation in an Orchard. In: Raje R.R., Hussain F., Kannan R.J. (eds) Artificial Intelligence and Technologies. Lecture Notes in Electrical Engineering, vol 806. Springer, Singapore. https://doi.org/10.1007/978-981-16-6448-9_27
6. D. S. David and A. Jeyachandran, "A comprehensive survey of security mechanisms in healthcare applications," 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-6, doi: 10.1109/CESYS.2016.7889823.
7. Stalin David, D., Jayachandran, A. A new expert system based on hybrid colour and structure descriptor and machine learning algorithms for early glaucoma diagnosis. Multimed Tools Appl 79, 5213–5224 (2020). https://doi.org/10.1007/s11042-018-6265-1.
8. D Stalin David, A Jayachandran, 2018,Robust Classification of Brain Tumor in MRI Images using Salient Structure Descriptor and RBF Kernel-SVM, TAGA Journal of Graphic Technology, Volume 14, Issue 64, pp.718-737.
9. D Stalin David, 2016, Robust Middleware based Framework for the Classification of Cardiac Arrhythmia Diseases by Analyzing Big Data, International Journal on Recent Researches In Science, Engineering & Technology, 2018, Volume 4, Issue 9, pp.118-127.
10. M. Rajdhev, D. Stalin David, "Internet of Things for Health Care", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 800-805, March-April 2017.
11. P. Prasanth, D. Stalin David, "Defensing Online Key detection using Tick Points", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 758-765, March-April 2017.
12. Sudalaimani, D. Stalin David, "Efficient Multicast Delivery for Data Redundancy Minimization over Wireless Data Centres", International Journal of Scientific Research

in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 751-757, March-April 2017.

13. R. Abish, D. Stalin David, "Detecting Packet Drop Attacks in Wireless Sensor Networks using Bloom Filter", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 730-735, March-April 2017.

14. Vignesh, D. Stalin David, "Novel based Intelligent Parking System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 724-729, March-April 2017.

15. D Stalin David, 2020, 'Diagnosis of Alzheimer's Disease Using Principal Component Analysis and Support Vector Machine, International Journal of Pharmaceutical Research, Volume 12, Issue 2, PP.713-724.

16. Jaswanth K S, Dr. D. Stalin David, "A Novel Based 3d Facial Expression Detection Using Recurrent Neural Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 48-53, March-April 2020.

17. D Stalin David, 2020, 'An Intellectual Individual Performance Abnormality Discovery System in Civic Surroundings' International Journal of Innovative Technology and Exploring Engineering, Volume 9, Issue 5, PP.2196-2206.

18. D Stalin David, 2020, 'Machine learning for the prelude diagnosis of dementia', International Journal of Pharmaceutical Research, Volume 13, Issue 3, PP.2329-2335.

19. David, D.S. and Y. Justin, 2020.A Comprehensive Review on Partition of the Blood Vessel and Optic Disc in RetinalImages.Artech J. Eff. Res. Eng. Technol., 1: 110-117.

20. D. Stalin David and A.A. Jose, 2020. Retinal image classification system for diagnosis of diabetic retinopathy using SDCMethods.Artech J. Eff. Res. Eng. Technol., 1: 87-93.

21. D. Stalin David and T. Joseph George, 2020. Identity-based Sybil attack detection and localization.ArtechJ. Eff. Res. Eng. Technol., 1: 94-98.

22. David, D.S. and L. Arun, 2020.Classification of brain tumor type and grade using MRI texture and shape in a machine learning scheme.Artech J. Eff. Res. Eng. Technol., 1: 57-63.

23. David, D.S., 2020. Retinal image classification system for diagnosis of diabetic retinopathy using morphological edgedetection and feature extraction techniques.Artech J. Eff. Res.Eng. Technol., 1: 28-33.

24. David, D.S., 2020. A novel specialist system based on hybrid colour and structure descriptor and machine learningalgorithms for early diabetic retinopathy diagnosis.Artech J. Eff. Res. Eng. Technol., 1: 50-56.

25. David, D.S. and M. Samraj, 2020.A comprehensive survey of emotion recognition system in facial expression.Artech J. Eff. Res. Eng. Technol., 1: 76-81.

26. David, D.S. and L. Arun, 2020. Multi-view 3D face renovation with deep recurrent neural networks. ArtechJ. Eff. Res. Eng. Technol., 1: 64-68.

27. David, D.S. and S. Namboodiri, 2020.Improvement of framework for the grouping of CA diseases by investigating bigdata.Artech J. Eng. Appl. Technol., 1: 7-14.

28. Stalin David D , Saravanan M, 2020, 'Multi-perspective DOS Attack Detection Framework for Reliable Data Transmission in Wireless Sensor Networks based on Trust', International Journal of Future Generation Communication and Networking , Volume 13, Issue 4, PP.1522–1539.

29. J. K. S and D. S. David, "A Novel Based 3D Facial Expression Detection Using Recurrent Neural Network," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp. 1-6, doi: 10.1109/ICSCAN49426.2020.9262287.

30. Stalin David D, Saravanan M, "Enhanced Glaucoma Detection Using Ensemble based CNN and Spatially Based Ellipse Fitting Curve Model", Solid State Technology, Volume 63, Issue 6, PP.3581-3598.

31. Stalin David D, Saravanan M, Jayachandran A, "Deep Convolutional Neural Network based Early Diagnosis of multi class brain tumour classification", Solid State Technology, Volume 63, Issue 6, PP.3599-3623.

32. D. Jayakumar; Dr.U. Palani; D. Raghuraman; Dr.D. StalinDavid; D. Saravanan; R. Parthiban; S. Usharani. "CERTAIN INVESTIGATION ON MONITORING THE LOAD OF SHORT DISTANCE ORIENTEERING SPORTS ON CAMPUS BASED ON EMBEDDED SYSTEM ACCELERATION SENSOR". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2477-2494.

33. R. Parthiban; S. Usharani; D. Saravanan; D. Jayakumar; Dr.U. Palani; Dr.D. StalinDavid; D. Raghuraman. "PROGNOSIS OF CHRONIC KIDNEY DISEASE (CKD) USING HYBRID FILTER WRAPPER EMBEDDED FEATURE SELECTION METHOD". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2511-2530.

34. Dr.U. Palani; D. Raghuraman; Dr.D. StalinDavid; R. Parthiban; S. Usharani; D. Jayakumar; D. Saravanan. "AN ENERGY-EFFICIENT TRUST BASED SECURE DATA SCHEME IN WIRELESS SENSOR NETWORKS". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2495-2510.

35. Dr. D. Stalin David; R. Parthiban; D. Jayakumar; S. Usharani; D. RaghuRaman; D. Saravanan; Dr.U. Palani."MEDICAL WIRELESS SENSOR NETWORK COVERAGE AND CLINICAL APPLICATION OF MRI LIVER DISEASE DIAGNOSIS". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2559-2571.

36. D.Raghu Raman; D. Saravanan; R. Parthiban; Dr.U.Palani; Dr.D.Stalin David; S. Usharani; D. Jayakumar."A STUDY ON APPLICATION OF VARIOUS ARTIFICIAL INTELLIGENCE TECHNIQUES ON INTERNET OF THINGS". European Journal of Molecular & Clinical Medicine, 7, 9, 2021, 2531-2557.

37. D.Saravanan; Dr.D.Stalin David; S.Usharani;D.Raghuraman; D.Jayakumar; Dr.U.Palani; R.Parthiban. “AN ENERGYEFFICIENT TRAFFIC-LESS CHANNEL SCHEDULING BASED DATA TRANSMISSION INWIRELESS NETWORKS”. European Journal of Molecular & Clinical Medicine, 2020, Volume 7, Issue 11, Pages 5704-5722.

38. S. Usharani; D.Jayakumar; Dr.U.Palani; D.Raghuraman; R.Parthiban; D.Saravanan; Dr.D.Stalin David. “INDUSTRIALIZED SERVICE INNOVATIONPLATFORM BASED ON 5G NETWORK AND MACHINELEARNING”.European Journal of Molecular & Clinical Medicine, 2020, Volume 7, Issue 11, Pages 5684-5703.

39. P Gopala Krishna, D StalinDavid, “AN EFFECTIVE PARKINSON'S DISEASE PREDICTION USING LOGISTIC DECISION REGRESSION AND MACHINE LEARNING WITH BIG DATA”, Turkish Journal of Physiotherapy and Rehabilitation; 32(3), Pages 778-786.

40. Jaswanth K S, Dr. D. Stalin David, "A Novel Based 3d Facial Expression Detection Using Recurrent Neural Network", International Journal of Scientific Research in

Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 48-53, March-April 2020.

41. T. Babu, H. Roopa, Arvind Kumar Shukla, D. Stalin David, S. Jayadatta, A.S. Rajesh, Internet of things-based automation design and organizational innovation of manufacturing enterprises,MaterialsToday:Proceedings,2021,ISSN:2214-7853, https://doi.org/10.1016/j.matpr.2021.10.459.

42. M. Chandragowda, C. Gnanavel, D. Saravanan, D. Stalin David, R. Parthiban, A.S. Rajesh,
43. Consequence of silanee combination representative on the mechanical possessions of sugarcane bagasse and polypropylene amalgams,Materials Today: Proceedings,2021, ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.10.455.

44. T.V.V. Pavan Kumar, Shafqat Nabi Mughal, Radhika Gautamkumar Deshmukh, S. Gopa Kumar, Yogendra Kumar, D. Stalin David,A highly consistent and proficient class of multiport dc-dc converter based sustainable energy sources,Materials Today: Proceedings, 2021,ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.10.458.

45. David, D.S. Enhanced glaucoma detection using ensemble based CNN and spatially based ellipse fitting curve model. *J Ambient Intell Human Comput* (2021). https://doi.org/10.1007/s12652-021-03467-4.