

INTRUSION DETECTION SYSTEM

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

By

Abhinav Anand (Reg. No - 40110010)

Altaf Reza (Reg. No – 40110071)



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade “A+” by NAAC
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI - 600119**

NOVEMBER - 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with —All grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **Abhinav Anand (40110010)** and **Altaf Reza (40110071)** who carried out the Project Phase-1 entitled “**INTRUSION DETECTION SYSTEM**” under my supervision from June 2023 to November 2023.

Internal Guide

Dr. A. C. Shanta Sheela M.E., Ph.D.

Head of the Department

Dr. L. LAKSHMANAN, M.E., Ph.D.

Submitted for Viva voce Examination held on_____

Internal Examiner

External Examiner

DECLARATION

I, **Abhinav Anand (Reg.No- 40110010), Altaf Reza (Reg.No-40110071)** hereby declare that the Project Phase-1 Report entitled **“INTRUSION DETECTION SYSTEM”** done by me under the guidance of **Dr. A. C. Shanta Sheela M.E., Ph.D.** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**.

DATE:

PLACE: Chennai

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph. D, Dean**, School of Computing **Dr. L. Lakshmanan M.E., Ph.D.**, Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my phase-1 project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Intrusion detection is a new, retrofit approach for providing a sense of security in existing computers and data networks, while allowing them to operate in their current “open” mode. The goal of intrusion detection is to identify, preferably in real time, unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators. The intrusion detection problem is becoming a challenging task due to the proliferation of heterogeneous computer networks since the increased connectivity of computer systems gives greater access to outsiders and makes it easier for intruders to avoid identification. Intrusion detection systems (IDSs) are based on the beliefs that an intruder’s behaviour will be noticeably different from that of a legitimate user and that many unauthorized actions are detectable.

Chapter No	TITLE	Page No.
	ABSTRACT	i
	LIST OF FIGURES	iii
1	INTRODUCTION	1
2	LITERATURE SURVEY 2.1 Inferences from Literature Survey	3
	2.2 Open problems in Existing System	7
3	REQUIREMENTS ANALYSIS	8
	3.1 Feasibility Studies/Risk Analysis of the Project	8
	3.2 Software Requirements Specification Document	8
4	DESCRIPTION OF PROPOSED SYSTEM	11
	4.1 Selected Methodology or process model	12
	4.2 Architecture / Overall Design of Proposed System	13
	4.3 Description of Software for Implementation and Testing plan of the Proposed Model/System	14
	REFERENCES	16

LIST OF FIGURES

4.2	System Architecture for proposed system	13
-----	---	----

CHAPTER 1

INTRODUCTION

In Today's world, several organisations store their data in several ways. These organisation's only requirement is to protect their private and official data from the internal intruders and external intruders. It may also possible that some authorised user may leak the data of the organisation for any purpose. In real-time, it is challenging to recognise the attacker because duplicate IP address and attack packets can be created. Techniques used before like firewall, and IDS was not able to detect the real-time attackers which occurred in the absence of the admin without his knowledge. A computer network is the combination of a set of hardware and software.

Information transfer between peer entities (including computers connected by a network). This service must ensure correct operation of the system hardware and firmware, and it should protect against unauthorized modification of data and labels. Denial-of-service is a threat, and assurance against denial-of-service is an important security service. A denial-of-service condition is said to exist whenever the system throughput falls below a pre-established threshold, or when access to a (remote) entity is unavailable. While such attacks are not completely preventable, it is often desirable to reduce the probability of such attacks below some threshold.

Anomaly detection model identifies new attacks by analysing the anomalous behaviour from normal behaviour and achieves high detection rates (DR) for new attacks, but produces many false positives (FP). Anomaly based IDS generate rules by observing collected audit data that is the records of activities generated by the operating system. Currently adaptive intrusion detection aims to solve the problems of analyzing the huge volumes of audit data and realizing performance optimization of detection rules. Detecting intrusions using data mining algorithms such as decision tree (DT), naïve Bayesian (NB), neural network (NN), support vector machine (SVM) k-nearest neighbours (KNN), and genetic algorithm have been widely used in the last decades.

1.1 Intrusions Detection can be classified into two main categories.

They are as follow:

Host Based Intrusion Detection: HIDSs evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files.

Network Based Intrusion Detection: NIDSs evaluate information captured from network communications, analyzing the stream of packets which travel across the network.

1.2 Problem statement:

An Intrusion Detection System (IDS) is a crucial component of network security that aims to identify and respond to unauthorized access or malicious activities within a computer network. The primary problem statement for an IDS is to detect and prevent intrusions by monitoring network traffic or system activities, generating alerts, and taking appropriate actions when potential threats or attacks are detected. The specific challenges and objectives for an IDS can vary depending on the environment and the organization's security requirements.

1.3 Problem Justification

To distinguish the activities of the network traffic that the intrusion and normal is very difficult and needed much time. An analyst must review all the data that large and wide to find the sequence of intrusion on the network connection. Therefore, it needs a way that can detect network intrusion to reflect the current network traffics. To enhance the network intrusion detection system with the use of Machine Learning algorithm by obtaining the optimal policy with the maximum reward.

CHAPTER 2

LITERATURE SURVEY

The concept of intrusion detection began with Anderson's seminal paper he introduced a threat classification model that develops a security monitoring surveillance system based on detecting anomalies in user behaviour.

Over the last five years, the problem of intrusion detection has been the subject of extensive research and development efforts by both cybersecurity experts and technology companies. Numerous solutions have emerged, each with its unique approach to tackle the challenge. These solutions range from analyzing diverse patterns of potential threats to scrutinizing intricate details of system health and network traffic. Researchers and industry leaders have explored a myriad of techniques, from signature-based and anomaly-based detection methods to the incorporation of machine learning and deep learning algorithms, all in a concerted effort to enhance the efficacy of intrusion detection systems. In this rapidly evolving field, the quest for more robust and adaptive solutions continues as the threat landscape evolves, requiring novel strategies to safeguard information and infrastructure from emerging cyber threats.

Binary classification is a common approach adopted by most intrusion detection systems, categorizing network traffic into two primary classes: "Normal" and "Attack." This binary classification simplifies the problem and enables the utilization of diverse algorithms to accurately classify data. Among the classification algorithms explored are Cluster Center K-Nearest Neighbors (K-NN), Naive Bayes, C 4.5 Decision Tree (J.48), Adaptive Intra/Inter Neural Network with Radial Basis Function (AINRBF+NN), Least Squares Support Vector Machine (LSSVM), and Random Forest (RF). These algorithms exhibit varying degrees of accuracy and efficiency, with RF consistently outperforming others, boasting a remarkable accuracy rate of 99%.

The IDS under consideration seeks to detect four primary attack categories: DoS, R2L, U2R, and Probe attacks, collectively covering a broad spectrum of potential intrusion scenarios. To gauge the effectiveness of these classification algorithms, an assortment of performance metrics are employed, including accuracy, detection false alarms, time accuracy, detection false positives, detection rate (DR), and the Matthews Correlation Coefficient (MCC). These metrics provide a comprehensive evaluation of the algorithms' ability to distinguish between normal network traffic and malicious attacks.

Each classification algorithm comes with its distinct set of advantages and drawbacks. For instance, Cluster Center K-NN offers swift classification but might not be as effective in detecting U2L and R2L attacks. In contrast, Naive Bayes combines high accuracy with low time complexity, yet it may exhibit limitations in identifying specific attack types. C 4.5 Decision Tree is valued for its interpretability and competitive accuracy rates. AINRBF+NN showcases the highest overall accuracy, while LSSVM excels in detection rates. RF stands out by outperforming other methods, attaining a remarkable 99% accuracy and offering the lowest false alarm rates.

The work of Nadeem combines neural network with semi-supervised learning, and uses a small number of labelled samples to obtain high accuracy.

Staudenmaier implemented intrusion detection based on LSTM regression neural network. The results show that the LSTM classifier lies certain advantages over other strong static classifiers. These advantages lie in detecting DoS and Robe attacks, both of which can produce unique time series characteristics. In order to compensate for the high false alarm rate.

Kim proposed a call language modelling method to improve the host intrusion detection system based on LSTM.

ssAgarap replaced Softmax by introducing linear support vector machine (SVM) into the final output layer of GRU model, and applied the model to the second classification of intrusion detection.

Kolosnjai realized a neural network consisting of convolution and feed forward neural structures. This paper presents a hierarchical feature extraction method, which vectorizes Ngram instruction features and convolution features.

Muna Mhammad, T. Jawhar and Monica Mehrotra presented an intrusion detection model derived from neural network and hybrid fuzzy logic. The key thought was to take benefit of different classification capacity of neural network and fuzzy logic for IDS. The model had capability to identify an attack, to distinguish one attack from another that is classifying attack and the essentially vital, to discover new attacks with the rate of high detection rate and low false negative. Required Training and testing data were acquired from the Defence Advanced Research Projects Agency (DARPA) intrusion detection assessment data set.

Denning myriad methods have been used into network security fields. Moreover, with the consistent development of big data as well as the increase in computational power, several deep learning approaches have been used in intrusion detection. Furthermore, deep learning can handle big data efficiently, and has the ability to extract the representative characteristics from raw data, therefore, many researchers focused their effort on deep learning techniques to create powerful IDSs. Maha Designed an intelligent BBFO-GRU intrusion detection systems in Industrial Cyber-Physical environment based on the Gated Recurrent Unit (GRU) model. In addition, in order to enhance the detection rate, NADAM optimizer is utilized to optimize the GRU hyperparameters. Jie proposed an Intrusion Detection System based on bidirectional simple recurrent unit. In addition, the skip connections is used to alleviate the vanishing gradient problem and improve the training effectiveness.

2.1 INFERENCES FROM LITREATURE SURVEY

The extensive literature survey on intrusion detection systems reveals a rapidly evolving field driven by advancements in machine learning and deep learning. Intrusion detection, initially conceptualized by Anderson with a focus on anomaly detection, has undergone significant transformation. Over the past five years, researchers, cybersecurity experts, and technology companies have collaborated to develop an array of solutions to tackle the ever-growing challenges of intrusion detection. These solutions, powered by diverse classification algorithms such as Cluster Center K-Nearest Neighbors, Naive Bayes, C 4.5 Decision Tree, AINRBF+NN, LSSVM, and Random Forest, have demonstrated varying degrees of accuracy and efficiency. Notably, Random Forest consistently stands out, achieving an impressive 99% accuracy rate. The significance of binary classification, differentiating "Normal" and "Attack" traffic, simplifies the problem and enables the utilization of these algorithms for effective intrusion detection.

Beyond traditional methods, the integration of deep learning into intrusion detection has garnered attention, offering new avenues for robust and adaptable intrusion detection systems. Researchers have explored diverse deep learning approaches, including LSTM-based systems and call language modeling, revealing their advantages in detecting specific attack types such as DoS and Probe attacks. The combination of deep learning techniques with conventional classifiers showcases the potential for enhanced accuracy and improved false alarm rates. Additionally, the incorporation of fuzzy logic and hybrid models into intrusion detection has demonstrated success in identifying and classifying attacks with high detection rates and low false negatives.

The utilization of convolution and feed-forward neural structures, hierarchical feature extraction, and the introduction of linear support vector machines within deep learning models underscores the continuous innovation in the field. Furthermore, the application of deep learning to big data and the ability to extract representative characteristics from raw data have positioned deep learning as a potent tool for developing powerful intrusion detection systems. Researchers have leveraged advanced models like the Gated Recurrent Unit (GRU) and bidirectional simple recurrent units, incorporating optimizations to improve detection rates.

Overall, the literature survey underscores the dynamic nature of intrusion detection and the relentless pursuit of more effective, adaptable, and efficient solutions to protect information and infrastructure from evolving cyber threats.

2.2 OPEN PROBLEMS IN EXISTING SYSTEM

(1) The recognition rate is not high enough. The existing intrusion detection technology has a low accuracy rate and a high false positive rate and a false negative rate. With the increasing amount of network data, the diversification of intrusion behaviour and the better disguise of intruders had become the bottleneck of intrusion detection.

(2) Poor adaptive ability. The adaptive ability mainly refers to the detection ability of the new intrusion behaviour, and the existing intrusion detection technology always lies certain defects in this aspect.

(3) The efficiency of processing large amounts of data is too low. With the advent of the era of big data, a large amount of network data will be generated in a short period of time. Intrusion detection is to identify intrusion behaviours in these large quantities of data, which brings great challenges to current intrusion detection technologies. In order to solve the problems mentioned above, we propose a realtime network intrusion detection system based on deep learning, which uses big data and deep learning technology to achieve real-time network intrusion detection.

There are mainly anomaly detection methods based on probabilistic statistical models, anomaly detection methods based on cluster analysis.

Anomaly detection methods based on neural networks. Anomaly detection methods based on data mining and so on.

These methods have been widely used in intrusion detection, but these technologies have their own advantages and disadvantages, and different technologies need to be selected according to the actual situation.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 FEASIBILITY STUDIES/RISK ANALYSIS OF THE PROJECT

FEASIBILITY STUDIES: The use of various classification algorithms, including Random Forest with an impressive 99% accuracy rate, demonstrates that the project can leverage existing solutions effectively. Furthermore, the integration of deep learning models, such as LSTM-based systems and fuzzy logic, showcases innovation in addressing complex intrusion detection challenges.

RISK ANALYSIS: Data normalization for machine learning-based intrusion detection systems, as discussed, is a crucial aspect. The selection of the most suitable normalization technique remains a critical concern, and any misstep could impact the system's overall performance. Additionally, the ever-evolving threat landscape in cybersecurity requires constant adaptation and research to ensure that intrusion detection systems remain effective against emerging cyber threats. Therefore, a comprehensive risk mitigation strategy is imperative to address these challenges and uncertainties.

3.2 SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

Jupyter:

Jupyter Notebook is an interactive computing environment that allows you to create and share documents that contain live code, equations, visualizations, and narrative text. It is a web-based application that runs in your browser and allows you to write and execute code in a variety of programming languages, including Python, R, Julia, and many others. The Jupyter Notebook is organized into cells, which can contain code, text, or media elements such as images or videos. You can execute code cells individually, allowing you to explore data, test ideas, and prototype solutions in an interactive manner. The output of code cells is displayed directly in the Notebook, making it easy to see the results of your code.

Jupyter Notebook is widely used in the data science and research communities, as it allows for easy collaboration and sharing of results. You can share your Notebook with others by sending them the file or by using one of the many online services that allow you to share and publish your Notebooks. Additionally, Jupyter Notebook supports the creation of interactive widgets and the use of extensions, which allow you to add new functionality to the Notebook.

Machine Learning:

Cyber attacks, anomalies, and other security threats in computer networks. Intrusion detection refers to the process of monitoring and analyzing network traffic to identify and respond to suspicious activity or attacks. Traditional intrusion detection systems (IDS) rely on rule-based or signature-based approaches to identify known patterns of attacks. However, these approaches may fail to detect new or unknown types of attacks, which is a common problem in today's rapidly evolving threat landscape.

Machine learning-based intrusion detection systems use algorithms and statistical models to learn from historical data and automatically identify patterns of normal and abnormal behavior. By analyzing network traffic, machine learning models can detect and flag suspicious activity, such as unusual network traffic patterns, communication between hosts that do not normally communicate, or unauthorized access attempts.

Machine learning algorithms can also be used to classify network traffic into different categories, such as normal, malicious, or suspicious, based on its characteristics. This enables IDS to prioritize and respond to security threats more effectively. Overall, machine learning can significantly improve the accuracy and efficiency of intrusion detection, allowing organizations to better protect their networks and data from cyber attacks.

Python:

Python can be used in intrusion detection to analyze network traffic, detect anomalies and security threats, and respond to them in real-time. Here are some steps to use Python in intrusion detection: Collect network traffic data: Use Python libraries like Scapy or Pyshark to capture and store network traffic data in a PCAP file.

Preprocess the data:

Use Python to preprocess the network traffic data to extract relevant features, such as source and destination IP addresses, port numbers, packet size, and protocol types.

Train a machine learning model:

Use Python libraries like Scikit-learn or TensorFlow to train a machine learning model on the preprocessed data. The model should be able to distinguish between normal and abnormal network traffic.

Deploy the model:

Deploy the machine learning model to a production environment, such as a network intrusion detection system or a security information and event management (SIEM) system. Monitor and analyze network traffic: Use Python to monitor incoming network traffic in real-time, and feed it into the machine learning model to identify anomalies and security threats. Based on the output of the model, trigger appropriate responses, such as blocking suspicious traffic, alerting security personnel, or logging the events for further investigation.

Python provides a wide range of libraries and tools for data preprocessing, machine learning, and realtime data processing, making it a popular choice for intrusion detection and other security applications.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

The proposed system aims to develop an Intrusion Detection System (IDS) capable of effectively identifying and preventing network intrusions. This IDS is designed to safeguard computer networks from unauthorized access and malicious activities by monitoring and analyzing network traffic. The proposed system utilizes various machine learning algorithms and methodologies to achieve this objective.

In the first phase, the system focuses on data preprocessing, which involves tasks such as data cleaning and feature engineering.

The system further performs data correlation analysis to identify highly correlated variables allowing it to eliminate redundant features and enhance model performance.

In the modeling phase, the system imports necessary libraries and splits the dataset into training and testing sets. Feature scaling is applied to ensure that features with large values do not dominate the results. The system then implements various machine learning classification algorithms, including Support Vector Machines, Random Forest, Naive Bayes, Decision Tree, Logistic Regression, and Gradient Descent. Each algorithm is trained on the training data, and the training times are recorded.

The system concludes this phase by analyzing the training and testing accuracy of each model, providing insights into their performance. The accuracy of each algorithm is assessed and compared to determine which one is most effective in detecting intrusions.

This proposed system is an integral part of enhancing network security by effectively identifying and preventing intrusions through the application of machine learning and data analysis techniques. It leverages the power of modern data science and artificial intelligence to create a robust defense mechanism against evolving cyber threats, ensuring the integrity, confidentiality, and availability of computer systems and networks.

4.1 SELECTED METHODOLOGY OR PROCESS MODEL

Intrusion detection systems primarily use two key intrusion detection methods: signature-based intrusion detection and anomaly-based intrusion detection.

Signature-based intrusion detection is designed to detect possible threats by comparing given network traffic and log data to existing attack patterns- These patterns are called sequences and could include byte sequences, known as malicious instruction sequences- Signature-based detection enables you to accurately detect and identify possible known attacks.

Anomaly-based intrusion detection is the opposite—it's designed to pinpoint unknown attacks, such as new malware, and adapt to them on the fly using machine learning. Machine learning techniques enable an intrusion detection system (IDS) to create baselines of trustworthy activity—known as a trust model—then compare new behavior to verified trust models. False alarms can occur when using an anomaly-based IDS, since previously unknown yet legitimate network traffic could be falsely identified as malicious activity.

4.2 ARCHITECTURE / OVERALL DESIGN OF PROPOSED SYSTEM

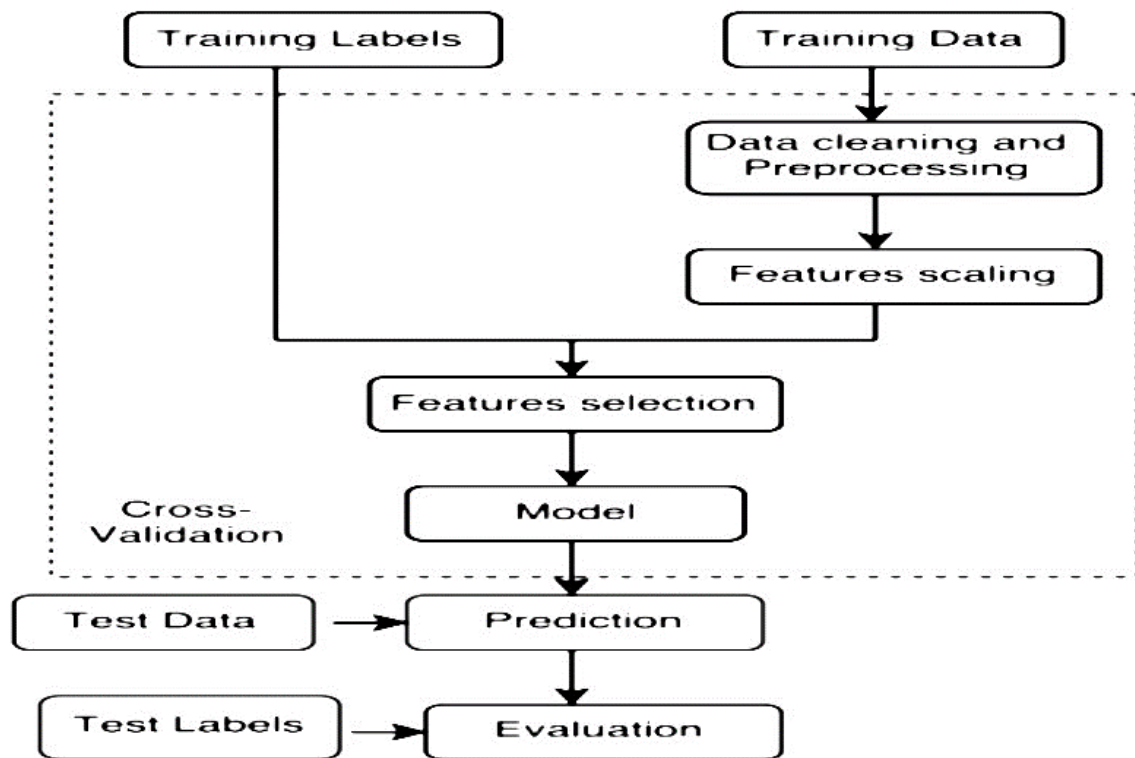


Fig 4.2: System Architecture for proposed system

4.3 Description of Software for Implementation and Testing plan of the Proposed Model/System:

The implementation and testing plan for the proposed Intrusion Detection System (IDS) based on machine learning involves a systematic and comprehensive approach to ensure the effectiveness and reliability of the system. The software development process will begin with the selection of appropriate machine learning algorithms tailored for intrusion detection, considering factors such as accuracy, efficiency, and adaptability to dynamic cyber threats.

The initial phase of implementation will focus on data preparation, where relevant datasets containing both normal and anomalous network activities will be collected and preprocessed. Feature extraction techniques will be applied to transform raw data into meaningful input features for the machine learning model. The selected algorithms, such as decision trees, support vector machines, or neural networks, will then be implemented to train the IDS on the labeled dataset.

Following the implementation, rigorous testing procedures will be carried out to assess the model's performance and generalization capabilities. This includes the creation of a testing dataset separate from the training data to evaluate the system's ability to accurately detect intrusions in unseen scenarios. Metrics such as precision, recall, and F1 score will be employed to quantify the model's efficacy in distinguishing between normal and malicious activities.

To enhance the system's robustness and adaptability, a continuous monitoring and feedback loop will be established. This involves periodically updating the model with new data to ensure it remains effective against evolving cyber threats. Additionally, stress testing and adversarial testing will be conducted to assess the system's resilience against sophisticated attacks and its ability to handle high volumes of network traffic.

The implementation and testing plan will also include the development of a user-friendly interface for system administrators to configure and monitor the IDS. Comprehensive documentation will be provided to facilitate seamless integration into existing network infrastructures. Regular maintenance and updates will be scheduled to address emerging threats and improve overall system performance.

In summary, the software implementation and testing plan for the proposed Intrusion Detection System by machine learning is a meticulous process encompassing data preparation, algorithm implementation, thorough testing, continuous monitoring, and user-friendly interface development. This comprehensive approach aims to deliver a robust, accurate, and adaptive IDS capable of safeguarding networks against a diverse range of cyber threats.

REFERENCES:-

- [1] Rohitha Goonatilake, Ajantha Herath, Suvineetha Herath, Susantha Herath, and Jayantha Herath, "Intrusion Detection Using the Chi-Square Goodness-of-Fit Test for Information Assurance, Network, Forensics and Software Security," The Journal of Computing Sciences in Colleges (JCSC), Vol. 23, No. 1, 2007, pp. 255-263.
- [2] Cengiz Kahraman, "Fuzzy Applications in Industrial Engineering," Springer-Verlag, 2006.
- [3] Denning. Dorothy E. "An intrusion-detection model." IEEE Transactions on software engineering 2 (1987): 222-232.
- [4] Heberlein, L. Todd, et al. "A network security monitor." Proceedings. 1990 IEEE Computer Society Symposium on Research in Security and Privacy. IEEE, 1990.
- [5] Nadeethn. Mutahir, et al. "Semi-supervised deep neural network for network intrusion detection." (2016).
- [6] Staudemcyer. Ralf C. "Applying long short-term memory recurrent neural networks to intrusion detection." South African Computer Journal 56.1 (2015): 136-154.
- [7] Kim, Gyuwan. et al. "LSTM-based system-call language modeling and robust ensemble method for designing host-based intrusion detection systems." arXiv preprint arXiv: 1611.01726 (2016).
- [8] Agarap, Abien Fred M. "A neural network architecture combining gated recurrent unit (GRU) and support vector machine (SVM) for intrusion detection in network traffic data." Proceedings of the 2018 10th International Conference on Machine Learning and Computing. ACM, 2018.
- [9] Kolosnjaji. Bojan, et al. "Deep learning for classification of malware system call sequences." Australasian Joint Conference on Artificial Intelligence. Springer. Cham. 2016.
- [10] Butun, Ismail. Salvatore D. Morgera.
- [10] P. Rama Murthy, "Production and Operations Management," Revised Second Edition, New Age International Publisher, 2007.
- [11] Cengiz Kahraman and Mesut Yavuz, "Production Engineering and Management under Fuzziness," Springer, 2010.

- [12] Petar Čisar and Sanja Maravić Čisar, "Quality Control in Function of Statistical Anomaly Detection in Intrusion Detection Systems," 4th Serbian-Hungarian Joint Symposium on Intelligent Systems (SISY 2006), 2006, pp. 209-220.
- [13] Paul E. Proctor "The Practical Intrusion Detection Handbook", Prentice Hall, 2001.
- [14] James C. Reynolds, James Just, Larry Clough, and Ryan Maglich, "On-Line Intrusion Detection and Attack Prevention Using Diversity, Generate-and-Test, and Generalization," Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), 2002, pp. 1-8
- [15] Thakur S, Chakraborty A, De R, Kumar N, Sarkar R. Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model. *Computer Electrical Eng.* 2021;91(107044):0045–7906. <https://doi.org/10.1016/j.compeleceng.2021.107044>