Real-Time Cyber Threat Detection and Response System

Pulicherla Hari Krishna[1], Dr M C Bhanu Prasad[2]

Department Of CSE, Tadipatri Engineering College, Tadipatri

Abstract

As wireless communications evolve, many community protection threats additionally evolve. Intrusion Detection System (IDS) detects assaults and facilitates perceive attackers. In the past, various system mastering (ML) strategies have been used with intrusion detection systems (IDS) in an attempt to improve intrusion detection effects and enhance the accuracy of IDS. Using major issue analysis (PCA), random woodland class, SVM, and naive base algorithms, this work proposes a method to expand an effective IDS. According to the effects of the proposed approach, the execution time (min) is three.24 mins, the accuracy charge (%) is 96.Seventy eight%, and the mistake rate (%) is zero.21%.

Keywords: Artificial Intelligence; Cyber Security; Internet, Mobile Application, PCA, Random Forest

1. INTRODUCTION

An attacker tried to hack or misuse a laptop device. An intrusion is an act that compromises the integrity, type, or functionality of any laptop device or facility. Through a weak spot within the abilities of the gadget or a flaw in its shape, an attacker tries to skip the authentication or authorization technique. With the fast increase of online bills and bookkeeping in society, social protection is more essential than ever. One solution to this hassle is the use of social intrusion detection structures (NIDS), which target many social video games thru surveillance assaults. It is consequently important that these structures are especially correct in detecting attacks, trying out them fast, and generating as few false positives as feasible. Intrusion detection systems (IDS) assist keep a at ease network via detecting malicious intrusions. The first-rate manner to do that is to read IDs. The requirements for IDS are flexibility and mobility. Security is critical in any place of work damage prevention attempt. A critical position of IDS is to provide a point of reference for peculiar activity and to alert community leaders to restoration/block and/or compress suspicious links. In addition, an IDS can differentiate between internal assaults (from personnel, customers or others) and external attacks (hacking assaults). Common types of intrusion detection structures (IDS) are community-primarily based (network-based IDS) and host-primarily based (HIDS). Social IDS is especially centered on detecting illegal, abusive and ordinary behavior among social audiences.

2. LITERATURE SURVEY

A literature study is unquestionably an essential part of the software program enhancement process. Prior to developing a tool, the time factor, cost savings, and enterprise reliability must be determined. Finding a beneficial gadget and language to increase the device comes next, once these items are satisfied. Programmers demand a lot of outside assistance when they begin creating the device. Websites, books, and seasoned programmers can all provide this assistance. The aforementioned issues are taken into account when developing the device in order to maximize the suggested tool.

Examining every task improvement need in detail is a crucial component of the process improvement service. A literature review is a crucial phase in the software development process for every task. Before creating the device and associated format, the elements of time, resource requirements, labour, economics, and organizational electricity should be identified and examined. The next stage is to ascertain the laptop's software program specifications, the operating engine needed to complete the operation, and any more software needed after these factors have been thoroughly examined and approved. a step like creating the relevant tools and chances. This email access is a "residing" format that currently classifies your article's components (title, subject, heading, etc.) according to your style. Given how quickly distant organizations are organized, the concept of local protection is fraught with risks.

Table.1. Summary of Existing Related Works

S. NO	AUTHOR/YEAR	TECHNIQUES	RESULTS	DISADVANTAGES
1	Jafar Abo Nada; Mohammad Rasmi Al-Mosa/2020[1]	To predict the attack by using the algorithm Attack Intention Analysis (AIA)	Now let's start by talking about the structure of this system.	Difficult to handle this process.
2	Sydney M. Kasongo and Yanxia Sun/2020[2]	We then implement the following MLapproaches using the reduced feature space: SVM, kNN. LR, ANN and Decision Tree (DT).	In our experiments, we considered both the binary and multiclass classifcation configurations. The results demonstrated that the XGBoost-based feature selection method	it requires careful tuning in general and especially when the input dimension is greater than the number of examples.
3	M.Akshay Kumaar, Duraimurugan Samiayya, P. M. Durai Raj Vincent, Kathiravan Srinivasan, Chuan-Yu Chang and Harish Ganesh/2022[3]	We compared five machine learning algorithms: Logistic Regression, Decision Trees, random forests, XGB, and Artificial Neural Network.	We have created a new Artificial Neural Network architecture that surpassed performance compared to the other algorithms obtaining ~99.2 % accuracy.	They have obtained an accuracy of only around 81% on the ADFA Intrusion Detection dataset. Anomaly-based detection has its disadvantages.
4	Neil Dalal, Nadeem Akhtar, Anubhav Gupta, Nikhil Karamchandani, Gaurav S. Kasbekar, Jatin Parekh/2021[4]	We propose a design for a signature-based IDS, which incorporates techniques to detect all the above attacks.	Our experimental results show that the AP is vulnerable to eight out of the nine attacks and the IDS is unable to detect any of them.	The main disadvantages of this system is IDS is unable to detect any of them
5	Sibi Chakkaravarthy Sethuraman,Sangeetha Dhamodaran, Vaidehi Vijayakumar/2020[5]	The performance of the proposed KDE-HMM technique	The proposed KDE-HMM technique/method combines the advantages of both statistical and probabilistic .	The major disadvantage of their method is that it selects top-ranked features.

6	Mohammad Idhom ; Henni Endah Wah anani/2021[6]	SECURITY , BRUTEFORCE.	Network security is critical to be able to maintain the information.	Complexity in Implementation
7	D. Gotseva; P. Stoynov, 2021. [7]	NEURAL NETWORK.	Intrusion Detection and Prevention Systems are widely used to detect network intrusions	Interpretability
8	Tsung-Han Lee, Taichung , Taiwan ; Lin-Huang Chang, Jun e 2020.[8]	Convolutional Neural Network.	The Software Defined Network (SDN) provides higher programmable functional ity for network configuration.	Sensitivity to Data
9	Oscar Rodas; Marc o Antonio To; Jose Alvarez; Step hane Maag,2020[9]	Intrusion	Wireless Mesh Networks (WMN) are growing rapidly in the research community	Imbalance
10	M. Selvaganesh; P. Naveen Karthi; Ap ril 2022.[10]	Brute force prevention	A brute force is a Hacking methodology used to decrypt login passwords, keys and credentials.	High computational resources are needed.

So protection arrangements need to be made. There isn't any standard method to guard networks from attacks. An intrusion detection system that operates on intricate networks, for instance, is not useful in remote agencies. Remote discovery has unfolded a brand new area for gadget administration for clients. Due to its ease of use and configuration, this era is gaining recognition and is growing swiftly. However, the most important protection possibility inside the subject is the Wi-Fi trouble. The equal goes for the overall performance of this suite. In the face of these growing demanding situations, it is crucial to consider security management. The aim of this newsletter is to assist the ultra-modern system to prevent intrusions and assaults on Wi-Fi networks to improve network safety. Therefore, the item discusses the development of a Wi-Fi intrusion detection engine, a Wi-Fi intrusion detection and prevention device "WIDPAS". It is primarily based on 3 key competencies: monitoring, evaluation and protection. While protecting network users, it simultaneously keeps an eye out for denial-of-attacks from the operator or rogue networks, blocks the attack, and identifies the attackers [1].

The results of our analyses to see the identification of various attack suites (e.g., IDS, malware, and shellcode) are presented in this study. We examine the overall validation performance of a hard and fast random woodland policy on a variety of datasets created in Kyoto 2006+, which reflects the state-of-the-art network capabilities amassed for intrusion detection system enhancement. We finish with a discussion and studies proposals at the mission [2].

In this text, we gift a set of studies on random forests (RF). In the "classic" RF induction method, a restricted range of randomly decided on bushes are supplied to generate the calculations. This type of rule has essential negative aspects: (i) the number of trees is predetermined (ii) the outline and assessment abilities of a degree of the selection tree type are not applicable due to the randomization precept. This sort of process, which involves becoming a member of timber without becoming a member of, does now not assure that everyone trees will work efficaciously at the identical board. This concept increases the following questions: Are there recuperation trees in the Russian Federation which can be praised for decay? So, is it feasible to clean the way for the decrease secondary faculty examination and create a complete panel? By answering those questions, the class hassle is solved. In this way, we show that huge selection bushes can be created even when the sub classification selection method is used. This "classical" RF

induction method, which involves bringing random timbers into combinations at random, isn't the best way to build accurate RF classifiers. Tree-based RF induction, which has previously been completed in "classical" RF induction methods, is of interest to us [3].

Intrusion detection structures (IDS) have grown to be a fundamental a part of PC and local location network protection. The NSL-KDD intrusion localization dataset, a not on time model of the KDDCUP'99 dataset, is used as a take a look at gadget in this paper. Due to the inherent characteristics of intrusion detection, the NSL-KDD dataset has a massive disparity among exercises, making it hard to extract structured facts in the subject of intrusion detection. To conquer the orientation mismatch problem, this paper makes use of a synthetic (deleted) minority trying out technique at the schooling information. For the NSL-KDD dataset, a log-primarily based absolute mark choice approach is provided to employ fewer inclusion devices. The suggested intrusion detection system uses the chaotic woodland as a classifier. The results of the experiments show that the information-based decisions and chaotic clustering of neighbouring forests with disturbances provide excessive average efficiency in producing effective and potential SDIs for intrusion detection[4].

An intrusion detection system (IDS) is a gadget or software bundle that looks for harmful intrusions in a local area or system. A standard IDS cannot locate difficult to understand digital signals inclusive of low-frequency DoS attacks and stealth attacks. In latest years, considering structure has inspired more and more human beings to conquer these barriers. In this paper, we advise a specific strategy for outlier detection using GRUs and PCA and PCA-minima classifiers in the GRU layer, supporting the proposed PCA with variations. The two interplay methods explicitly use graphs designed for the ones factors that most affect the problem due to a few covariance. This method may be implemented to GRU models with very little additional computational fee. We gift experimental results from two actual worldwide benchmarks, KDD Document ninety nine and NSL-KDD, which display that the GRU version achieves tremendous performance upgrades over the PCA-scale method [5].

Iftikhar Ahmed et al. Studied various machine getting to know algorithms for intrusion localization system. They take into consideration several strategies such as SVM, fuzzy gaining knowledge of system and random forest. In order to get the gadget to finish the truck higher than other calculations, the authors of the outcomes described a more thorough method. B. Riaz and associates here, they tried to construct an intrusion localization shape by hand. They optimized the reality set using a well-known complete selection feature. They ultimately discovered a dynamic growth inside the IDS results using a KDD dataset. We recognized research gaps inside the present related paintings that are described beneath.

- Web infrastructures are particularly used for lots malicious games.
- The predominant problem recognized on this regard is hacking the machine to get rid of information.
- The authors of the results explained a more comprehensive technique to get the device to finish the truck higher than prior computations. B. Riaz and colleagues here, they attempted to manually create an intrusion localization shape. They used a well-known complete selection function to maximize the reality set. Using a KDD dataset, they finally found a dynamic growth inside the IDS results. Furthermore, the observation indicates that some of the methods within the dataset may be advanced.
- Improve the first-class of enter statistics within the proposed system.

Evaluation of the Rationale and Feasibility of the Proposed System

The corporation's most important purpose is to detect attacks the use of PCA (Principal Component Analysis) and Random Forest, SVM, Naive Bayes set of rules.

3. PROPOSED MATERIALS AND METHODS

Intrusion detection system protects the device from intrusive assaults. Reveals what is needed for brand new people. The proposed device attempts to conquer the preceding troubles seen in real-international programs. The proposed machine getting to know techniques include: feature extraction and random inversion forest. The first evaluation changed into used to lessen the size of the dataset; with this technique, the grasp elegance database advances because the index has its personal capabilities.A random hopping set of rules is used to locate intruders, attaining each better detection and fake alarm prices than SVM, that is a naive Bayes set of rules.

The image of the overall characteristics of the product is related to the cloth of the premises and the extreme degree of the necessities of the device. Countless net pages and their links are described and generated at some point of the architectural design. Key software additives are identified, divided into processing blocks and conceptual structures, and the relationships among them are described. The proposed framework classifies the assisting modules.

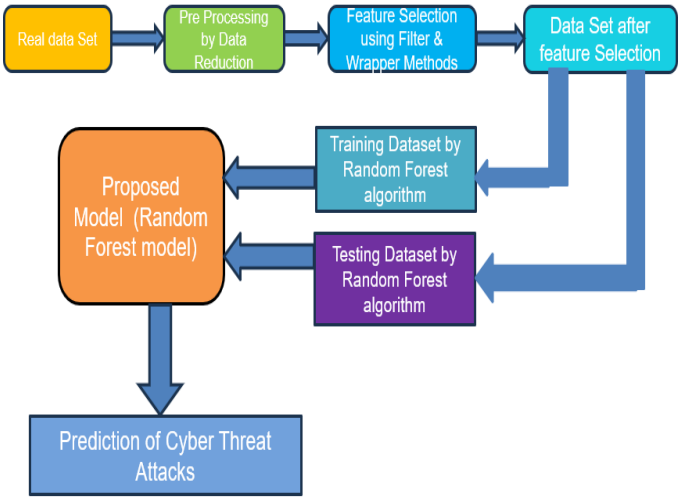

Fig 1: Overall System Architecture of Cyber Threat Detection

3.1. SYSTEM MODULES:

3.1.1.Information Collection

This is the first actual step closer to really constructing a gadget learning version for a statistical collection. This is a critical step that relies upon on a great model: the better the realism, the extra whole our version might be. There are many file maintaining methods together with text content material extraction, guide intervention, and many others. The dataset used in this intrusion detection engine dataset is taken from the kdd hyperlink: http://kdd.Ics.Uci.Edu/databases/kddcup99/kddcup99. HTML.

3.1.2.Facts Series

The dataset consists of 125, 974 character elements. The data set defined below has forty two columns.

3.1.3. Records Education

Let's make alternative entries. Rejecting lacking information and getting rid of a couple of classes. First, we show the names of the types that we need to store or save. In this step, we clear or eliminate a couple of classes other than those who need to be saved. Finally, we take away or get rid of rows with lacking functions from the dataset. There is a distinction among education and evaluation.

3.1.4.Sample Analyzing

Head mining is a method used to reduce the dimensionality of a information set. Headend search is one of the greenest and maximum accurate structures for reducing the scale of facts and prioritization selections. This technique reduces statistical capabilities to preferred features referred to as primaries.

This approach considers every facts report as records with the largest variety of possibilities, subsequently the biggest information set length. This technique reduces the quantity of facts by putting the alignment factors on a single axis. The statistics elements are transformed as an axis and become key factors. PCA can be done thru associated advances:

Take evaluation records with global capabilities. Add the counseled vector to every prediction d. Compute the eigenvectors (e1, e2, e3...Ed) and eigenvalues (v1, v2, v3, VD) the use of the embedding question and compute the n ordered eigenvectors to obtain the biggest eigenvalues.

Unordered scaffolding is one of the most primary methods of device gaining knowledge of for solving classroom issues. Random forests belong to the magnificence of supervised algorithms. This set of rules is completed in discrete steps: the primary is to build a wooded area of the given dataset and the second one is to construct the magnificence predictions.

3.1.5.Analysis and Forecasting

Table.2. Features Explanation

S.No	Features	Attributes
1	Duration	Length (number of seconds) of the connection
2	Protocol type	Type of the protocol, e.g. tcp, udp, etc.
3	Src_bytes	Number of data types from source to destination
4	Dst_bytes	Number of data types from destination to source
5	Is_host_login	1 if the login belongs to the "host" list; 0 otherwise
6	Is_guest_login	1 if the login is a "guest login" ; 0 otherwise
7	Diff_srv_rate	% of connections to different services
8	Srv_diff_host_rate	% of connections to different hosts
9	Flag	Normal or error status of the connection
10	Labels	Normal or attacker

3.1.6. Save Learned Version

We achieved 99.1% accuracy at the validation set.

If you actually need to customize your template and see it in production, the first step is to convert it to .H5 or .H5. PKL library using Alex. Make sure ALEX is mounted on your environment. Then import the module and dump the model right into a .Pkl report.

3.2 Dimensionality reduction

Principal Feature Analysis (PCA) is a statistical approach. PCA is a broadly used tool inside the look at of devices for studies assessment and prediction models. PCA is especially useful in the identity manner while

there's heterogeneity between abilities/variables. The amount of data required to supply a statistically significant end result will increase exponentially with the number of features or dimensions in a data set. The curse of dimensionality is a trouble whilst operating with excessive-dimensional records, leading to difficulties which include overfitting, extended computation time, and decreased accuracy of system studying models.

The wide variety of possible function combos will increase exponentially with the number of dimensions, making it hard to obtain a consultant pattern of the facts. Performing tasks together with clustering or category is high priced because the algorithms must navigate a totally massive characteristic area, growing computation time and complexity. Additionally, a few device gaining knowledge of algorithms are sensitive to the wide variety of dimensions, requiring more data to gain the same stage of accuracy as low-dimensional facts. Feature engineering strategies, which includes function choice and extraction, are used to overcome the curse of dimensionality. As a subset of function extraction techniques, dimensionality discount objectives to reduce the quantity of input capabilities whilst keeping as lots of the authentic statistics as possible.

*3.3 **Machine Learning Classifiers***

Using information and algorithms to simulate how AI mimics human search and steadily increases its accuracy is relevant to the system mastering (ML) field of AI and pc generation. Decision-making methods Predictions and classifications are normally made the use of laptop mastering algorithms. Based on various dimensional records, your computation predicts the example in the logs. The errors feature that estimates the model score is known as the mistake function. Using samples, correlations may be set up to examine the accuracy of the trouble mapping version. The model refinement method assumes that the model first-rate fits the information considered within the training dataset and that the weights are suitable to control the discrepancy between the regarded phenomena and the predicted representation. It reframes this “assessment and merchandising” manner by means of continuously updating the burden until the computational accuracy threshold is reached.

Since deep getting to know and AI are frequently used interchangeably, the nuances among the 2 are vital. Subsets of artificial intelligence include neural networks, deep learning, and gadget gaining knowledge of. However, mind networks are a subset of AI, and deep studying is a subset of brain systems. Deep studying and AI vary in how every computation learns. “Deep” computational mastering, additionally called directed learning, may use named information codes to carry its guiding standards, however it is not surely a feature data code. A deep learning technique can continuously perceive a set of non-stop functions from uncooked statistics, such as text or photographs that distinguish one kind of data from some other. This lets in for using large amounts of statistics and eliminates the want for human intervention. As Lex Friedman placed it in his speak at MIT, deep mastering can be concept of as a "deterministic stage of gaining knowledge of" (hyperlink is external to IBM.Com).

Random forest algorithm:

It combines the effects of a couple of selection trees into a unmarried quintessential end result. Their ease of use and flexibility have contributed to their adoption, as they remedy each partitioning and regression problems. Surprising advances were made within the subject of machine gaining knowledge of that is an attractive aggregate of information and computer technological know-how. One of those strategies is random woodland. A collaborative group of decision bushes, known as random forests or random decision bushes, paintings together to generate a decision. Random forests have been created through Leo Breiman in

2001, and they have on the grounds that come to be a staple amongst machine learning lovers. In this text, we will cowl the fundamentals and applications of the random woodland algorithm.

The random wooded area set of rules is one of the useful techniques for education timber in machine learning. During the training phase, it generates some of choice timber. A random subset of the dataset is used to construct every tree to degree a random subset of the capabilities in every partition. By introducing variability in character trees, this randomness reduces the danger of overfitting and improves universal prediction overall performance. The algorithm combines the results from each tree into predictions, either via averaging (for regression troubles) or vote casting (for class issues). This collaborative choice-making procedure, facilitated through the understanding of multiple trees, is an instance of dependable and correct effects. Random forests are frequently used for category and regression problems due to the fact they could deal with complicated records, lessen overfitting, and bring accurate predictions underneath a spread of situations.

Support Vector Machine (SVM)

A popular machine studying method for linear and nonlinear category, regression, and outlier detection is the Support Vector Machine (SVM). Because SVMs are versatile, they can be used for a ramification of duties, together with face recognition, anomaly detection, handwriting recognition, junk mail detection, image class, text classification, and gene expression evaluation. Since SVMs awareness on determining the maximum separating hyperplane among more than one lessons in a goal feature, they carry out thoroughly in binary and multiclass classification. The subject matter discusses the Support Vector Machine (SVM) set of rules, its utility, and how it performs linear and nonlinear class in addition to regression and outlier detection obligations.

One of the maximum extensively used supervised studying strategies for category and regression troubles is the Support Vector Machine or SVM. But its fundamental application is in machine studying to resolve classification troubles. To facilitate the type of extra information factors inside the future, the SVM tries to attract a best line or selection boundary that divides the n-dimensional space into instructions. We call this most reliable decision boundary a hyperplane. The SVM selects intense factors and vectors to form the hyperplane. The algorithm is called a Support Vector Machine due to the fact those extreme instances are known as Support Vector Machines.

Naive Bayes

Naive Bayes classifiers are a hard and fast of classification techniques based totally on Bayes' theorem. Rather than being a unmarried algorithm, it is a set of algorithms that follow a single pattern, that means that every pair of classifiable capabilities is unbiased of the others. Let’s first look at the dataset. One of the most effective and most powerful class algorithms, Naive Base type makes it clean to fast create system learning models with rapid predictive abilities. When faced with class problems, Naive Base is used. It is widely utilized in textual content classification. Since every word inside the information represents a function, text classification responsibilities contain high-dimensional facts. It is used in rating class, sentiment analysis, spam filtering, and other regions. One of the advantages of the use of Naive Base is that it's miles fast. With high-dimensional data, you can make predictions fast and without difficulty. Based on predefined function values, this model calculates the possibility that a given instance belongs to a specific elegance. It performs the function of type. This is formed because of the assumption that one characteristic of the model is impartial of the opposite. In different words, each characteristic contributes independently to the predictions. In the real world, this requirement is not often met. For both schooling and prediction, this method integrates Bayesian theorem.

4. RESULT AND DISCUSSION

Fig 2.* Implementation-*Home Page

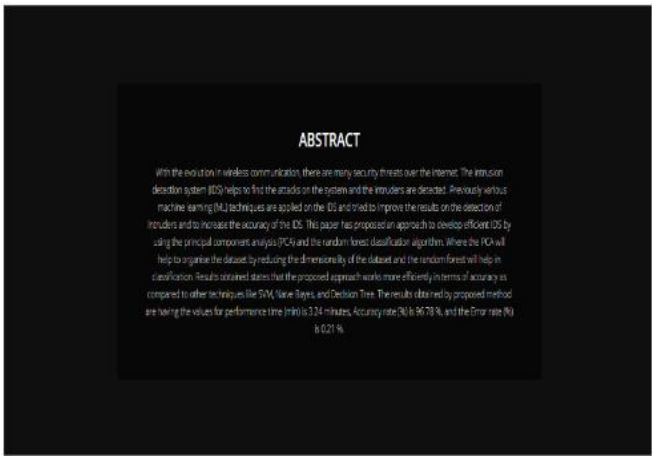

Fig 3. Implementation

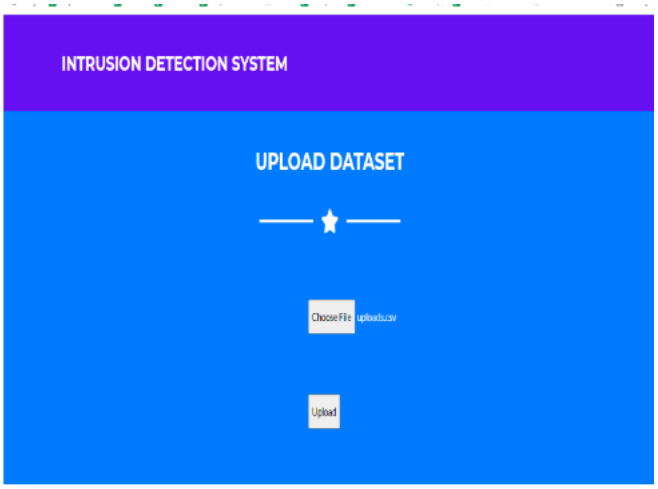

Fig 4. Implementation-Upload Dataset

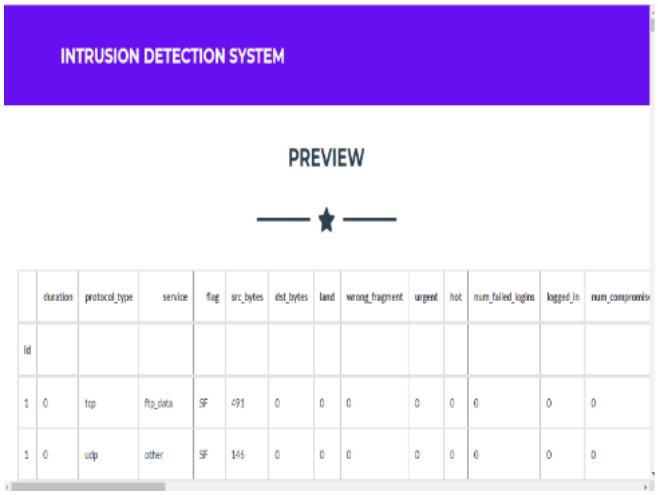

Fig 5. Implementation-Preview Page

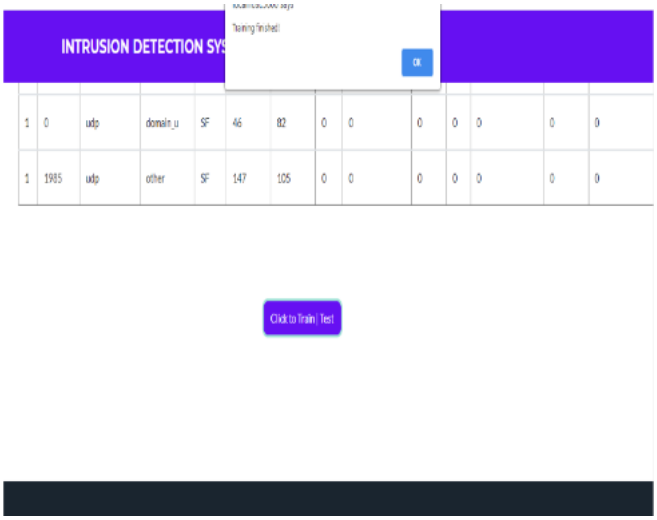

Fig 6. Implementation-Preview Page

Fig 7. Implementation-Prediction Page

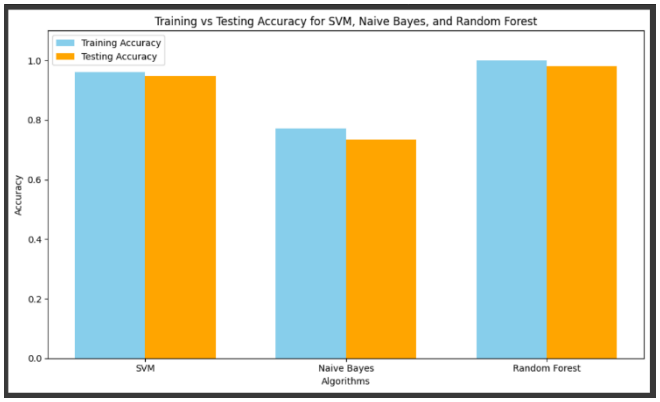

Fig 8. Comparative Analysis of Machine Learning Classifiers

Figure [2] shows the implementation domestic page. Figure [3] shows the processing page for loading the dataset. Figure [4] suggests the loading of the dataset. Figure [5] shows a top level view of loading the dataset. Figure [6] shows the education dataset. Figure [7] suggests the prediction. The bar chart compares the training and checking out accuracy for SVM, Naive Bayes and Random Forest. Random Forest plays high-quality with 100% schooling accuracy and 98.1% testing accuracy, observed with the aid of SVM with 94.8% checking out accuracy. Naive Bayes plays worst with 73.5% trying out accuracy.

5. CONCLUSION

Security issues have additionally emerged with the increasing use of Internet systems. The proposed technique efficiently solves the problem of detecting online attackers. Compared with the previously proposed PCA algorithms, Random Forest, SVM and Naive Base executed excellent. Both the false errors fee and the detection price are significantly improved by the suggested method. This is where we use the information discovery dataset. The results of our suggested method showed an accuracy (%) of 96.72 percent, an error charge (%) of 0.21%, and a going for walks time (min) of 3.24 minutes.

6. FUTURE ENHANCEMENT

Intrusion detection equipment are the most critical means of detecting malicious behaviour within the community. Machine gaining knowledge of techniques had been used especially to build intrusion detection systems, which ensure nearly best accuracy and occasionally false positives. Recently, many classifiers had been used, which includes ensemble system studying techniques. This approach proposes a method for detecting intrusions via a mechanical joint tilt. The ensemble technique is an advanced gadget mastering method that provides better accuracy than popular class. A robust and speedy tool manage technique is proposed to gain high accuracy for intrusion detection. First, three rules were found out using the KDD99 dataset. Using the idea of common overall performance, these three pre-classifications are combined. The feature functions had been decided on from a hard and fast of learning statistics the use of the "first come, first served" question rule. By lowering the scale and validity of the records, this technique reduces the time required for formatting. A high-accuracy, valid dataset is critical for a reliable intrusion detection engine. Any classifier should preserve type accuracy throughout all new samples studied within the dataset.

REFERENCES

1. JafarAbo Nada; Mohammad Rasmi Al-Mosa, 2018 International Arab Conference on Information Technology (ACIT), A Proposed Wireless Intrusion Detection Prevention and Attack System

2. Kinam Park; Youngrok Song; Yun-Gyung Cheong, 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigData Service), Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm

3. S. Bernard, L. Heutte and S. Adam "On the Selection of Decision Trees in Random Forests" Proceedings of International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 14-19, 2009, 978-1-4244-3553- 1/09/$25.00 ©2009 IEEE

4. A. Tesfahun, D. Lalitha Bhaskari, "Intrusion Detection using Random Forests Classifier with SMOTE and Feature Reduction" 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 978-0-4799-2235-2/13 $26.00 © 2013 IEEE

5. Le, T.-T.-H., Kang, H., & Kim, H. (2019). The Impact of PCA-Scale Improving GRU Performance for Intrusion Detection. 2019 International Conference on Platform Technology and Service (PlatCon). Doi:10.1109/platcon.2019.8668960

6. Anish Halimaa A, Dr K.Sundarakantham: Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) 978-1-5386-9439-8/19/$31.00 ©2019 IEEE "MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM."

7. Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly (2019). Deep Learning-Based Intrusion Detect ion for IoT Networks, 2019 IEEE 24 th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 256-265, Japan.

8. R. Patgiri, U. Varshney, T. Akutota, and R. Kunde, "An Investigation on Intrusion Detection System Using Machine Learning" 978-1-5386-9276 9/18/$31.00 c2018IEEE.

9. Rohit Kumar Singh Gautam, Er. Amit Doegar; 2018 8 th International Conference on Cloud Computing, Data Science & Engineering (Confluence) "An Ensemble Approach for Intrusion Detect ion System Using Machine Learning Algorithms."

10. Kazi Abu Taher, Billal Mohammed YasinJisan, Md. Mahbubur Rahma, 2019 International Conference on Robot ics, Electrical and Signal Processing Techniques (ICREST)"Network Intrusion Detect ion using Supervised Machine Learning Technique with Feature Selection."

11. L. Haripriya, M.A. Jabbar, 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)" Role of Machine Learning in Intrusion Detection System: Review"

12. Nimmy Krishnan, A. Salim, 2018 International CET Conference on Control, Communication, and Computing (IC4) "Machine Learning-Based Intrusion Detection for Virtualized Infrastructures"

13. Mohammed Ishaque, Ladislav Hudec, 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) "Feature extraction using Deep Learning for Intrusion Detection System."

14. Aditya Phadke, Mohit Kulkarni, Pranav Bhawalkar, Rashmi Bhattad, 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)"A Review of Machine Learning Methodologies for Network Intrusion Detection."

15. Iftikhar Ahmad , Mohammad Basheri, Muhammad Javed Iqbal, Aneel Rahim, IEEE Access (Volume: 6) Page(s): 33789 – 33795 "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection."

16. B. Riyaz, S. Ganapathy, 2018 International Conference on Recent Trends in Advanced Computing (ICRTAC)" An Intelligent Fuzzy Rule-based Feature Selection for Effective Intrusion Detection."