# Comparative Analysis and Validation for Cyber Forensic Model using the NSL-KDD Dataset

**Sagargouda S Patil, Research Scholar, NCET Bangalore & INDIA, sagar.cs.kle@gmail.com**

**Dr. Dinesha H A, Professor & HOD, NCET Bangalore & INDIA, sridini@gmail.com**

Abstract : **Social media platform like twitter are facing the problems of the spam. In twitter fake users send undesired tweets to users to promote different services. The spam generally composed of malicious URLs, users that may steal your personal info, and hack accounts, which might be used for fraudulent activity. Also, nowadays, there are many websites on the internet which are being used for sharing the information, connecting people, video streaming, browsing etc. All these websites are accessed using the links which are provided by the host. The host provides the links with proper security and good content. But some of the sites have Malicious Uniform Resource Allocators (URL) using which the attacker can access the user information. When the user clicks or taps on the links or hyperlinks of these websites then he is redirected to some another website. In this case, the user has no idea that he is getting attacked by the user and he/she is providing the personal information to the attacker. To prevent the spam problem and malicious attacks there are many models which have been presented by various researchers. Hence, in this paper we compare the result of our model with the other existing model to show that our model performs well in terms of accuracy, precision, recall and F1-score.**

***Keywords — Cyber-attack, Model, Phishing , Twitter, URL, Validation***

## I. INTRODUCTION

Online Social platforms like Facebook, Instagram, WhatsApp and Twitter have changed the way of sharing the information between people. Users join social network usually to connect to their families, friends or who they are interested in. The information being shared by the users can be of any type. Some of the information shared between could be irrelevant to other users. Some of the users share the wrong information to gain the attention of the user. The best example of sharing the wrong information could be edited images and videos, fake news and other kind of irrelevant data that is being shared using the URLs in social platforms. To reduce these kinds of fake URLs, this model has been created to identify and classify the following URLs to reduce these kinds of attacks. The model mainly focusses on the network security and tries to identify using the four kinds of attacks: Dos (denial of service), probe, U2R (User to Root), and R2L (remote to local). The goal of this model is to check the malicious URLs and classify them into different types of attacks. In the recent years, since there was a huge elevation in the usage of the social network there have been many attacks like phishing in which the attacker sends or contacts the user using the legit information, asks their information and uses it for wrong purpose and the users fall into their prey. Generally, the users are unaware that the attacker has been attacked and the information has been leaked leading to many frauds. Many models have been created to stop these kinds of attacks before happening. Many machine learning algorithms have been used in the model, to predict these attacks. Some of the models have predicted the attacks but the accuracy rate has been compromised. Furthermore, nowadays most people cannot barely picture their lives without technological advancements. As a matter of fact, there are a wide range of applications, websites, and new online social websites that allow a huge number of people to exchange their knowledge and build a proper social and professional contact. These websites focus heavily on connecting people together either through the sharing of common interests. However, the act of spreading information and establishing contacts with people raises some important security issues. Furthermore, a phishing/malicious Uniform Resource Locator (URL) is a URL that has been designed to be used for fraud or spam attacks. In this attack, a virus is sent by the attacker and is installed on a computer if a given user or a customer tap on a URL that contains malware. Phishing and spam are two common outcomes of malicious Uniform Resource Locators. Credentials of users are compromised when they fall victim to phishing. As a result, it is critical to distinguish between legitimate and harmful linkages. Malicious Unified Resource Locators are being used as a vector for cyber-attacks. Moreover, the phishers are constantly tweaking their cyber-attack methods. The attacker has the ability to misuse shared data for his or her own ends. One of the most popular forms of cybercrime is the use of a malicious website or malicious uniform

DOI : 10.35291/2454-9150.2022.0397

resource locator. When you're not careful, you could end up becoming a victim of frauds including cash losses, personal information disclosures, malware installation, spyware installation, extortion, a false shopping site, an unexpected award, and so on. Visits to these sites may be prompted by email, adverts, web searches, or hyperlinks from other websites. In each scenario, the needs to tap on the malicious link. The rise in phishing, spamming, and malware situations demands a dependable solution that can categorize and detect bad URLs. Malicious uniform resource locators are still a major source of security breaches. Malware, phishing and spam are all frequent methods of spreading them. Black-listing is a widely used method of detecting harmful URLs. Blacklists keeps a track of URLs that have previously been associated with dangerous activity. When it comes to detecting newly produced malicious URLs, these lists fall short. Machine learning algorithms have been trained as a result to detect dangerous URLs. In this paper, we compare these models with our Data Imbalance Aware XGBoost (DIA-XGB) and Modified Weight Optimized XGBoost (MWO-XGB) using the NSL-KDD dataset to identify and detect the malicious URL using our model.

## II. LITERATURE SURVEY

In [1], Network anomaly detection aims to identify network anomalies, and it has obtained many achievements using the supervised classification technique. Since the supervised classifier depends on the prior data, it is difficult to accurately classify the rare anomalies when they account less in the training set. Data augmentation can tackle the imbalanced training set problem through creating artificial rare anomaly samples. However, the existing data augmentation methods either ignore the data distribution or ignore the spatial knowledge between features. Therefore, this article addresses this issue by proposing a Network Anomaly Detection Scheme based on feature Representation and data Augmentation (NADS-RA). Re-circulation Pixel Permutation strategy is first designed as feature representation strategy to construct images, and it rotates each feature left by the times of feature number to maintain the spatial knowledge between original network traffic features. We conduct experiments on five public benchmark datasets, including NSL-KDD and UNSW-NB15, and so on, and compare against 12 detection methods and 17 data generation methods. The experimental results demonstrate the superior effectiveness of our work to state-of-the-art methods and the general applicability in different scenarios.

In [2], The intrusion detection based on deep learning method has been widely attempted for representation learning. However, in various deep learning models for intrusion detection, there is rarely convolutional neural networks (CNN) model. In this work, we propose an image conversion method of NSL-KDD data. Convolutional neural networks automatically learn the features of graphic NSL-KDD transformation via the proposed graphic conversion technique. We evaluate the performance of the image conversion method by binary class classification experiments with NSL-KDD Test+ and Test−21.

In [3], Machine learning techniques are being widely used to develop an intrusion detection system (IDS) for detecting and classifying cyberattacks at the network-level and the host-level in a timely and automatic manner. However, many challenges arise since malicious attacks are continually changing and are occurring in very large volumes requiring a scalable solution. There are different malware datasets available publicly for further research by cyber security community. However, no existing study has shown the detailed analysis of the performance of various machine learning algorithms on various publicly available datasets. Due to the dynamic nature of malware with continuously changing attacking methods, the malware datasets available publicly are to be updated systematically and benchmarked. In this paper, a deep neural network (DNN), a type of deep learning model, is explored to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyberattacks.

In [4], This paper describes the advantages of using the anomaly detection approach over the misuse detection technique in detecting unknown net-work intrusions or attacks. It also investigates the performance of various clustering algorithms when applied to anomaly detection. Five different clustering algorithms: k-Means, improved k-Means, k-Medoids, EM clustering and distance-based outlier detection algorithms are used. Our experiment shows that misuse detection techniques, which implemented four different classifiers (naïve Bayes, rule induction, decision tree and nearest neighbor) failed to detect network traffic, which contained a large number of unknown intrusions; where the highest accuracy was only 63.97% and the lowest false positive rate was 17.90%. On the other hand, the anomaly detection module showed promising results where the distance-based outlier detection algorithm outperformed other algorithms with an accuracy of 80.15%. The accuracy for EM clustering was 78.06%, for k-Medoids it was 76.71%, for improved k-Means it was 65.40% and for k-Means it was 57.81.

In [5], Network intrusion detection systems (NIDSs) provide a better solution to network security than other traditional network defense technologies, such as firewall systems. The success of NIDS is highly dependent on the performance of the algorithms and improvement methods

DOI : 10.35291/2454-9150.2022.0397

used to increase the classification accuracy and decrease the training and testing times of the algorithms. We propose an effective deep learning approach, self-taught learning (STL)-IDS, based on the STL framework. The proposed approach is used for feature learning and dimensionality reduction. It reduces training and testing time considerably and effectively improves the prediction accuracy of support vector machines (SVM) with regard to attacks. The proposed model is built using the sparse autoencoder mechanism, which is an effective learning algorithm for reconstructing a new feature representation in an unsupervised manner. After the pre-training stage, the new features are fed into the SVM algorithm to improve its detection capability for intrusion and classification accuracy. Moreover, the efficiency of the approach in binary and multiclass classification is studied and compared with that of shallow classification methods, such as J48, naive Bayesian, random forest, and SVM. Results show that our approach has accelerated SVM training and testing times and performed better than most of the previous approaches in terms of performance metrics in binary and multiclass classification. The proposed STL-IDS approach improves network intrusion detection and provides a new research method for intrusion detection.

In [6], Network intrusion detection systems (NIDSs) play a crucial role in defending computer networks. However, there are concerns regarding the feasibility and sustainability of current approaches when faced with the demands of modern networks. More specifically, these concerns relate to the increasing levels of required human interaction and the decreasing levels of detection accuracy. This paper presents a novel deep learning technique for intrusion detection, which addresses these concerns. We detail our proposed nonsymmetric deep autoencoder (NDAE) for unsupervised feature learning. Furthermore, we also propose our novel deep learning classification model constructed using stacked NDAEs. Our proposed classifier has been implemented in graphics processing unit (GPU)-enabled TensorFlow and evaluated using the benchmark KDD Cup '99 and NSL-KDD datasets. Promising results have been obtained from our model thus far, demonstrating improvements over existing approaches and the strong potential for use in modern NIDSs.

In [7][8], Advances in communication and networking technology leads to the use of internet-based technology in Industrial Control System (ICS) applications. Simultaneously to the advantages and flexibility, it also opens doors to the attackers. Increased attacks on ICS are clear examples for the need of developing strong security mechanisms to develop defense in depth strategies for industries. Despite several techniques, every day a novel attack is being identified and this highlights the importance and need of robust techniques for identifying those attacks.

# III. METHODOLOGY

### XGBOOST

The architecture of data imbalance and malicious URL model using XGBoost Algorithm (see Fig.1). This architecture presents a method for the detection of different malicious URLs in the Social Network Platform and reduces the spam more efficiently than the existing model considering the data imbalance. It also presents the spam drift extraction and detection model using KL- divergence for obtaining drift time and changes the values in the XGBoost Classification model to check the efficiency of the model.

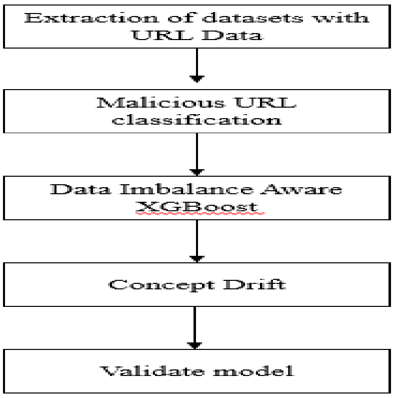
Extraction of datasets with URL Data
Malicious URL classification
Data Imbalance Aware XGBoost
Concept Drift
Validate model

**Figure 1. The architecture of Data Imbalance and Concept drift**

XGBoost is an enhanced distributed gradient boosting model intended to be exceptionally effective, adaptable, and versatile [9][10]. It carries out machine learning calculations under the Gradient Boosting structure. XGBoost gives a parallel tree boosting (otherwise called GBDT, GBM) that tackles numerous data science issues quickly and exactly. The architecture of the XGBoost model handling the concept drift and data imbalance (see Fig.2).

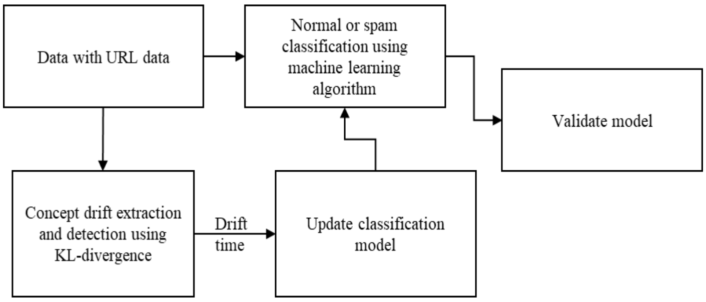
Data with URL data
Normal or spam classification using machine learning algorithm
Validate model
Concept drift extraction and detection using KL-divergence
Drift time
Update classification model

**Figure 2. Architecture of class imbalance and concept drift aware spam classification.**

# IV. RESULTS & DISCUSSION

In this section we present the results obtained by the various models and our proposed model for the detection of

DOI : 10.35291/2454-9150.2022.0397

the malicious attacks using the NSL-KDD dataset. In this section we discuss the results for the binary-classification and multi-classification of the NSL-KDD dataset. This work uses accuracy, precision, recall and F1-Score to evaluate performance.

The accuracy is calculated as follows

$$Accuracy(A_c) = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

The Precision is calculated as follows

$$Precision(P_p) = \frac{TP}{TP + FP} \quad (2)$$

The Recall is calculated as follows

$$Recall(R_n) = \frac{TP}{TP + FN} \quad (3)$$

The F1-score is calculated as follows

$$F1\ Score(F1) = \frac{2 * Precision * Recall}{Precision + Recall} \quad (4)$$

### A. *Performance Evaluation for the NSL-KDD dataset for binary-classification*

#### *NSL-KDD for test* $^+$

#### I. Accuracy

We have compared the accuracy of the proposed model with the existing machine learning and other models considering the test$^+$ dataset (see Fig.3). The Accuracy of the proposed model attains higher accuracy when compared with the existing models.

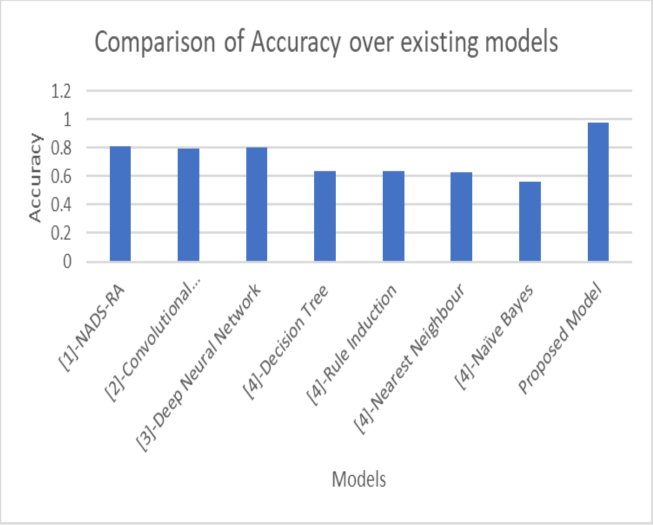

**Figure 3. Comparison of Accuracy using the NSL-KDD test+**

#### II. Precision

We have compared the precision of the proposed model with the existing machine learning and other models considering the test$^+$ dataset(see Fig.4). The Precision of the proposed model attains higher precision when compared with the existing models.

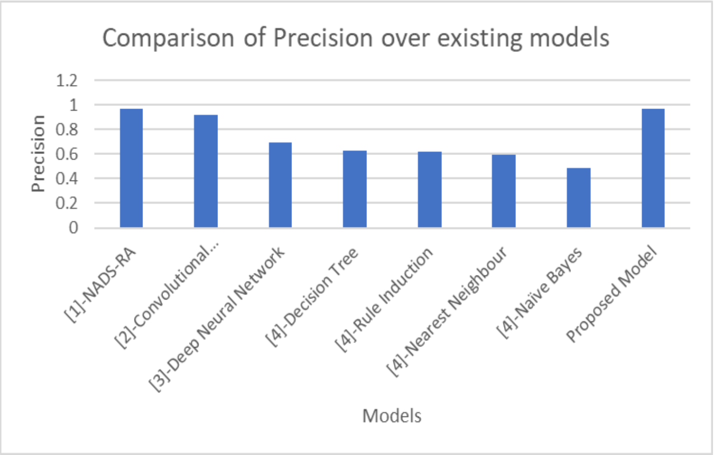

**Figure 4. Comparison of Precision using the NSL-KDD test+**

#### III. Recall

We have compared the recall of the proposed model with the existing machine learning and other models considering the test$^+$ dataset (see Fig.5). The Recall of the proposed model attains higher recall when compared with the existing models.

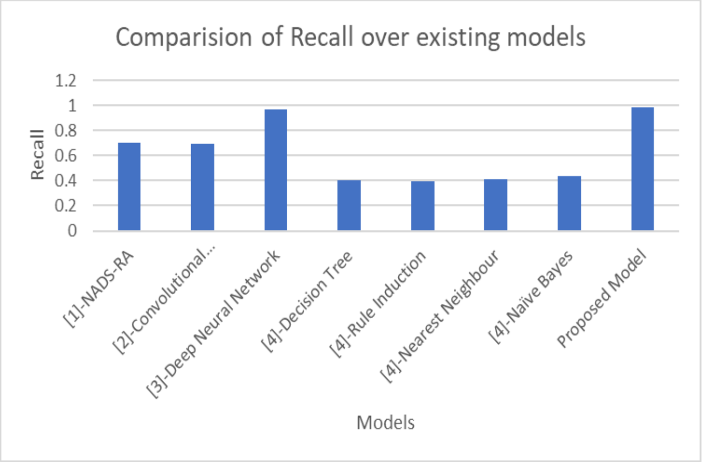

**Figure 5. Comparison of Recall using the NSL-KDD test+**

#### IV. F1-Score

We have compared the accuracy of the proposed model with the existing machine learning and other models considering the test$^+$ dataset(see Fig.6). The F1-Score of the proposed model attains higher F1-score when compared with the existing models.

DOI : 10.35291/2454-9150.2022.0397

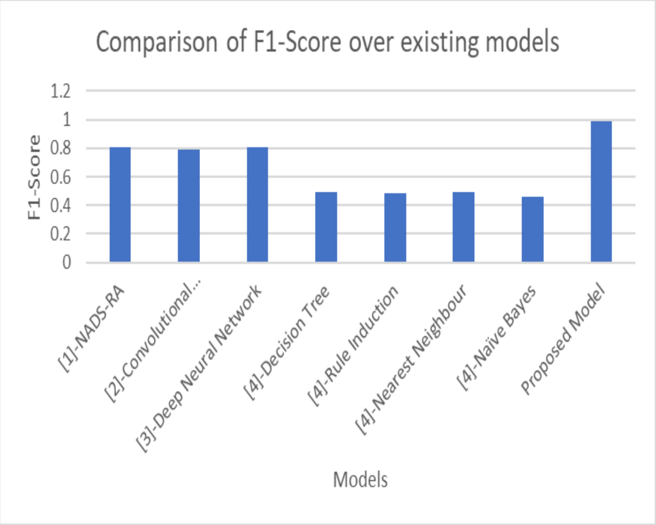

Figure 6. Comparison of F1-Score using the NSL-KDD test+

### NSL-KDD for test$^{-21}$

### I. Accuracy

We have compared the accuracy of the proposed model with the existing models considering the test$^{21-}$ dataset(see Fig.7). The proposed model attains higher accuracy when compared with the existing models.

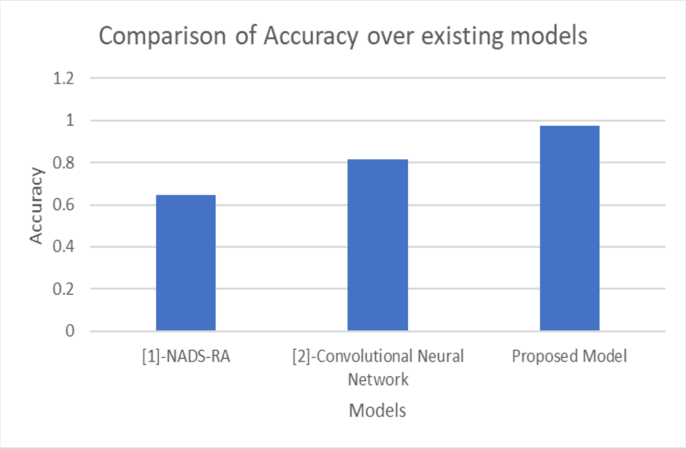

Figure 7. Comparison of Accuracy using the NSL-KDD test21-

### II. Precision

We have compared the precision of the proposed model with the existing models considering the test$^{21-}$ dataset(see Fig.8). The proposed model attains higher precision when compared with the existing models.

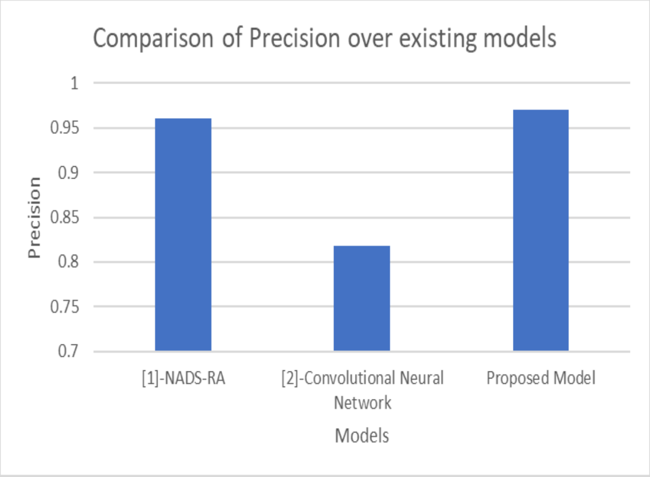

Figure 8. Comparison of Precision using the NSL-KDD test21-

### III. Recall

We have compared the recall of the proposed model with the existing models considering the test$^{21-}$ dataset(see Fig.9). The proposed model attains higher recall when compared with the existing models.

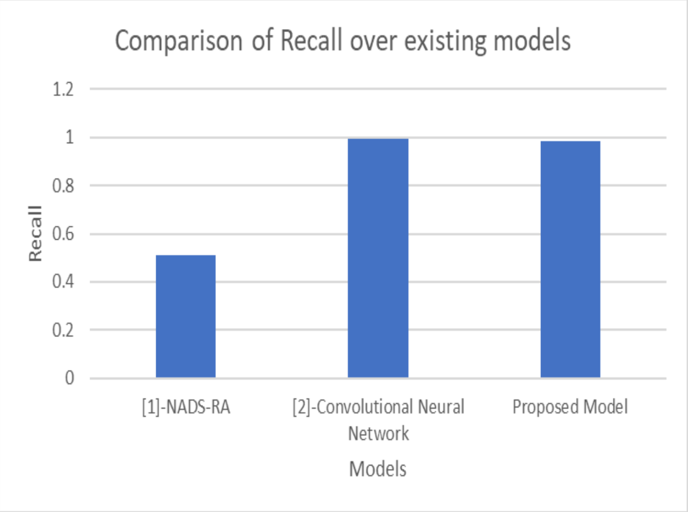

Figure 9. Comparison of Recall using the NSL-KDD test21-

### IV. F1-Score

We have compared the F1-Score of the proposed model with the existing models considering the test$^{21-}$ dataset(see Fig.10). The proposed model attains higher F1-Score when compared with the existing models.

DOI : 10.35291/2454-9150.2022.0397

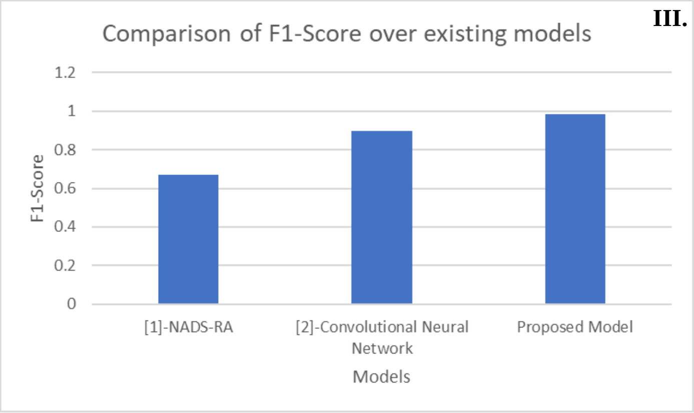

Figure 10. Comparison of F1-Score using the NSL-KDD test21-

### NSL-KDD for full set

#### I. Accuracy

We have compared the accuracy of the proposed model considering the NSL-KDD full dataset with the existing SVM model(see Fig.11). The SVM model has attained higher accuracy when compared by our model by 1%.

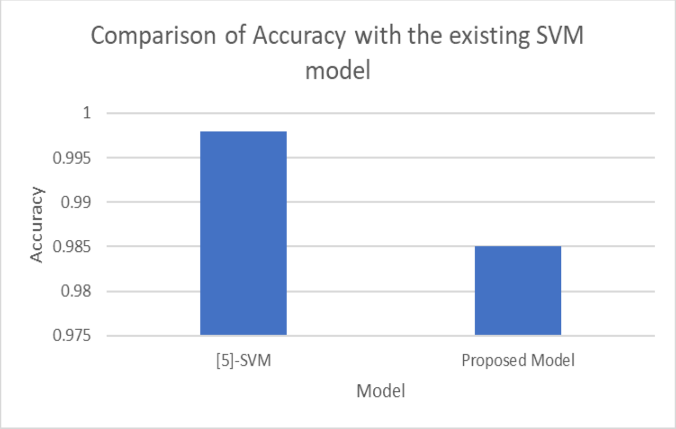

Figure 11. Comparison of Accuracy using the NSL-KDD full dataset

#### II. Precision

We have compared the precision of the proposed model considering the NSL-KDD full dataset with the existing SVM model (see Fig.12). The proposed model attains higher precision when compared with the existing SVM model.

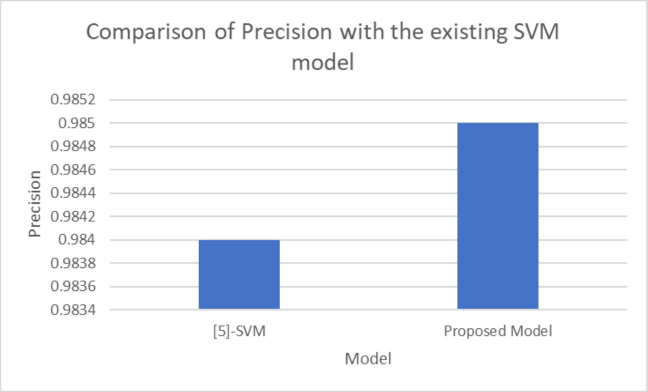

Figure 12. Comparison of Precision using the NSL-KDD full dataset

#### III. Recall

We have compared the recall of the proposed model considering the NSL-KDD full dataset with the existing SVM model(see Fig.13). The proposed model attains higher recall when compared with the existing SVM model.

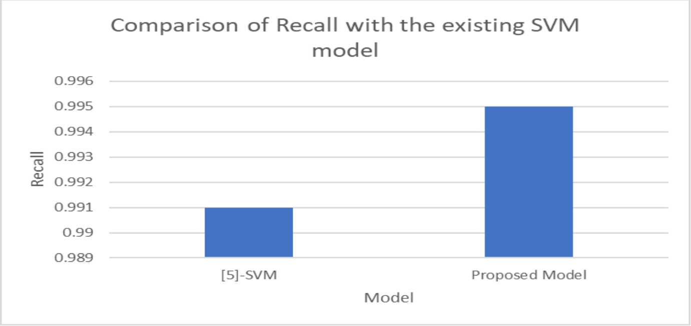

Figure 13. Comparison of Recall using the NSL-KDD full dataset

#### IV. F1-Score

We have compared the F1-Score of the proposed model considering the NSL-KDD full dataset with the existing SVM model(see Fig.14). The SVM model has attained higher F1-Score when compared by our model by 0.3%.

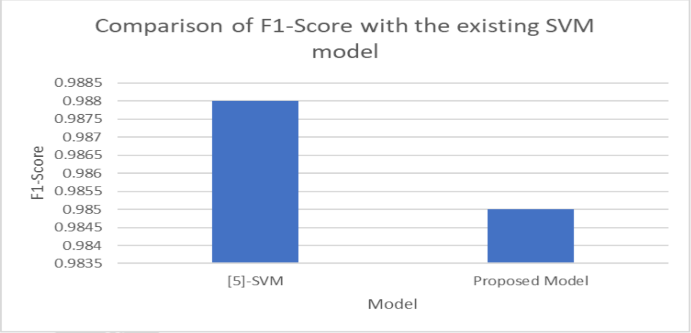

Figure 14. Comparison of F1-Score using the NSL-KDD full dataset

### *B. Performance Evaluation for the NSL-KDD dataset for multi-classification*

### NSL-KDD for full set

#### I. Accuracy

We have compared the accuracy of the proposed model with the existing models (see Fig.15). The proposed model attains higher accuracy when compared with the existing model.

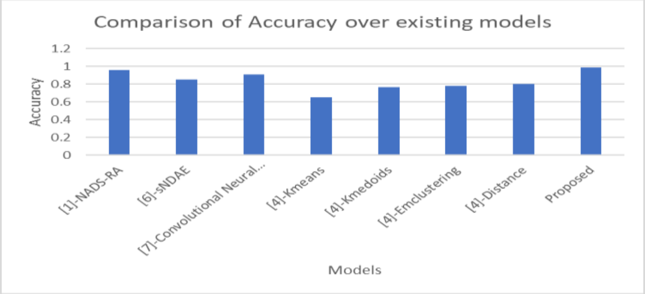

Figure 15. Comparison of Accuracy using the NSL-KDD full dataset

### II. Precision

We have compared the precision of the proposed model with the existing models(see Fig.16). The proposed model attains higher precision when compared with the existing model.

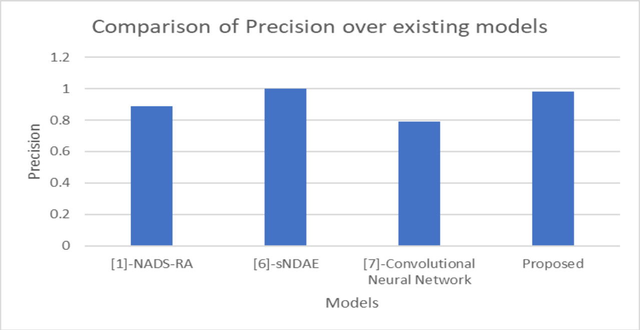

**Figure 16. Comparison of Precision using the NSL-KDD full dataset**

### III. Recall

We have compared the recall of the proposed model with the existing models (see Fig.17). The proposed model attains higher recall when compared with the existing model.

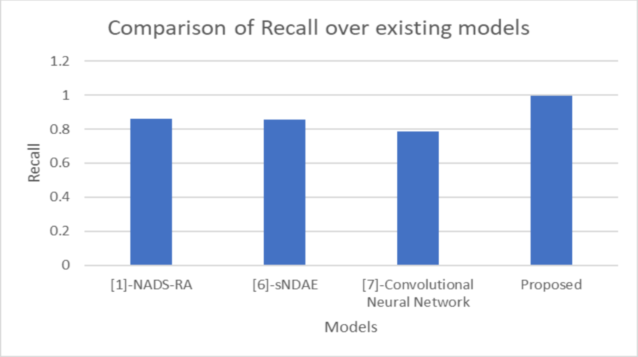

**Figure 17. Comparison of Recall using the NSL-KDD full dataset**

### IV. F1-Score

We have compared the F1-Score of the proposed model with the existing models (see Fig.18). The proposed model attains higher F1-Score when compared with the existing model.

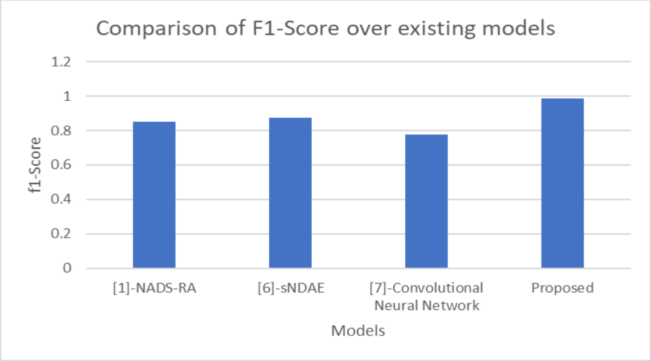

**Figure 18. Comparison of F1-Score using the NSL-KDD full dataset**

## V. CONCLUSION

In this paper first we have conferred the various problems faced in the cyber forensic models. After that, we have investigated the various spam attacks and malicious attacks in the online environment. Further, we have studied some research work in which they have also used the NSL-KDD dataset for evaluating the results of their model. Finally, after the whole study we have compared the results of our model with the existing research works. From the results and discussion section it can be said that the proposed model attains higher performance in terms of Accuracy, Precision, Recall and F1-Score. For future work we can evaluate our model using other dataset.

## REFERENCES

[1] X. Liu et al., "NADS-RA: Network Anomaly Detection Scheme Based on Feature Representation and Data Augmentation," in IEEE Access, vol. 8, pp. 214781-214800, 2020, doi: 10.1109/ACCESS.2020.3040510.

[2] Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, ‘‘Intrusion detection using convolutional neural networks for representation learning,’’ in Neural Information Processing. Cham, Switzerland: Springer, 2017, pp. 858–866.

[3] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, ‘‘Deep learning approach for intelligent intrusion detection system,’’ IEEE Access, vol. 7, pp. 41525–41550, 2019.

[4] I. Syarif, A. Prugel-Bennett, and G. Wills, ‘‘Unsupervised clustering approach for network anomaly detection,’’ in Networked Digital Technologies. Berlin, Germany: Springer, 2012, pp. 135–145.

[5] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, ‘‘Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,’’ IEEE Access, vol. 6, pp. 52843–52856, 2018.

[6] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, ‘‘A deep learning approach to network intrusion detection,’’ IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[7] S. Potluri, S. Ahmed, and C. Diedrich, ‘‘Convolutional neural networks for multi-class intrusion detection system,’’ in Proc. Int. Conf. Mining Intell. Knowl. Explor. Cham, Switzerland: Springer, 2018, pp. 225–238.

[8] Patil SS, Dinesha HA. (2022) URL Redirection Attack Mitigation in Social Communication Platform using Data Imbalance Aware Machine Learning Algorithm. Indian Journal of Science and Technology. 15(11): 481-488. https://doi.org/10.17485/IJST/v15i11.1813

[9] R. Hewett, S. Rudrapattana, P. Kijsanayoth. Cyber- security analysis of smart SCADA systems with game models. Proceedings of the 9th annual cyber and information security research conference, ACM, 2014, pp. 109– 112

[10] Yusheng Dai, Hui Li, Yekui Qian, Yunling Guo, Min Zheng, Anticoncept Drift Method for Malware Detector Based on Generative Adversarial Network, Security and Communication Networks, Article ID 6644107, 2021 (2021) 12. https://doi.org/10.1155/2021/6644107

DOI : 10.35291/2454-9150.2022.0397