Information Security Analysis and Audit – CSE3501

PROJECT REVIEW-3

TOPIC: Machine Learning for Wireless Networks

TEAM MEMBERS:

19BIT0002 - Naman Sethi

19BIT0009 - Keshav Agarwal

19BIT0044 - Chaitanya Singh

19BIT0048 - Sourabh Karmakar

SLOT: F1

FACULTY: Prof. Sumaiya Thaseen

Project Title

Machine Learning for Wireless Networks

Abstract:

Intrusion detection is an important requirement in wireless mesh network and the intrusion detection system (IDS) provides security by monitoring data traffic in real time. But the major issue in the implementation of machine learning technique-based IDS in WMN is its dimensionality problem. The requirement of large amount of energy to deal with the dimensionality affects the efficiency of IDS in WMN. Another major drawback in the implementation of IDS with large number of features is the requirement of large execution time. Hence it requires the removal of a large number of irrelevant features for better accuracy.

So, in this work, with the help of feature selection techniques like Mutual Information and Genetic Algorithm, we assist in selecting the most relevant features from an IDS dataset, so as the facilitate IDS with better execution time. We have used various ML algorithms like Artificial Neural Network (ANN), Random Forest, Decision Tree, K-Nearest Neighbors and Linear Regression for prediction purpose, out of which Random Forest came out to be the best algorithm.

Keywords:

IDS (Intrusion detection System), Mutual Information (MI), Genetic Algorithm (GA), Logistic Regression (LR), Artificial neural network (ANN), Random Forest, Decision Tree, KNN, Python

Introduction:

In this project, our main was to solve the dimensionality problem i.e., a large amount of time and energy is required to deal with the dimensionality which affects the efficiency of Intrusion Detection System (IDS) in Wireless Mesh Network (WMN). When a large number of features are implemented in IDS, execution time required is also large. To overcome this problem, a Mutual Information (MI) and Genetic algorithm (GA) based feature selection technique is proposed to reduce the dimensionality and select the optimal subset of features for the intrusion detection system. The filter method-based MI

technique selects the semi-optimal feature subset from the original subset. The features selected through MI were thereby used to train the 4 different ML models:

- Random Forest
- Decision Tree
- K-Nearest Neighbors (KNN)
- Logistic Regression.

And by 1 deep learning model:

- Artificial Neural Network (ANN)

The accuracy of the given five models were compared in between and for both GA and MI techniques, and the result shows that Random Forest Classifier gave the highest accuracy score value on the testing dataset for both MI and GA.

Related Work (Content of Review-1)

BASE PAPER ANALYSIS

The main aim of this paper is to solve the dimensionality problem i.e., a large amount of energy is required to deal with the dimensionality which affects the efficiency of Intrusion Detection System (IDS) in Wireless Mesh Network (WMN). Also, when a large number of features are implemented in IDS, execution time required is also large. To overcome this problem, a novel hybrid Genetic Algorithm (GA) and Mutual Information (MI) based feature selection technique is proposed to reduce the dimensionality and select the optimal subset of features for an intrusion detection system. The wrapper method-based GA select the semi-optimal feature subset from the original subset. Then the MI technique placed inside the GA selects the optimal feature subset with the help of SVM classifier and the process repeats till the maximum accuracy of IDS is achieved. The proposed IDS is compared with the IDS based on features selection techniques of MI, GA and GA+MI in SVM and ANN classifier using ADFA-LD dataset. Results show that the proposed intrusion detection system with hybrid GA and MI based technique with SVM classifier has high accuracy and can be suitable for intrusion detection system in wireless mesh network and other applications, but for implementing in WMN based sensitive applications like smart grid, IoT, etc, the training time of the classifier need to be further reduced.

REVIEW OF OTHER PAPERS

[1] Deep learning approach for intelligent intrusion detection system – 2019

In this paper, author's main aim in to find a solution for the problem that there is no 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.

So, in this paper, a deep neural network (DNN), a type of deep learning model, is explored to develop a flexible and effective IDS (intrusion detection system) to detect and classify unforeseen and unpredictable cyberattacks. Deep neural networks are a powerful category of machine learning algorithms implemented by stacking layers of neural networks along the depth and width of smaller architectures. The advantage of selecting DNN model was to comprehensively evaluating their performance in comparison to classical machine learning classifiers on various benchmark IDS datasets. The main drawback of proposed study is that it does not give detailed information on the structure and characteristics of the malware. Although the performance can be further improved by training complex DNNs architectures on advanced hardware through distributed approach.

[2] Evaluation of machine learning algorithms for intrusion detection system – 2017

In this paper the main aim is to perform several experiments and test to evaluate the efficiency and the performance of the several machine learning classifiers such as: J48, Random Forest, Random Tree, Decision Table, MLP, Naive Bayes, and Bayes Network. For this the KDD intrusion detection dataset technique is used. In this technique, testing phase is implemented based on 60000 random instances of records. Several performance metrics are computed (accuracy rate, precision, false negative, false positive, true negative and true positive). The most important advantage of this technique is that Random forest classifier gets the highest accuracy rate (93.77%), with the smallest RMSE value and false positive rate.

Also, a greater number of algorithms could be used in order to compare with rest of the algorithms so as to increase the chances of getting a higher accuracy.

[3] Survey on SDN based network intrusion detection system using machine learning approaches – 2019

In this paper, author's aim to protect computer networks and to overcome network security issues. And for this Machine/Deep Learning (ML/DL) technique approaches have been implemented in the SDN-based Network Intrusion Detection Systems (NIDS). More specifically, they evaluated the techniques of deep learning in developing SDN-based NIDS. In this survey, they covered tools that can be used to develop NIDS models in SDN environment. This survey is concluded with a discussion of ongoing

challenges in implementing NIDS using ML/DL and future works. The advantage of using DL/ML is that they emphasized software-defined networking (SDN) technology as a platform using ML/DL approaches to detect vulnerabilities and monitor networks. And also gained importance due to its efficiency in evaluating network security. The main drawback of this research is that none of the approaches implementing SDN-based NIDS are applied to critical infrastructure and high-speed network infrastructure. Similarly, various issues need to be considered while implementing NIDS, since the nature of the attacks are dynamic. So, adaptability of detection method is required.

[4] Building an efficient intrusion detection system based on feature selection and ensemble classifier – 2020

In this paper, author's main aim in to achieve good performance in IDS((Intrusion detection system) because there are lots of redundant and irrelevant data in high-dimensional datasets interfere with the classification process of an IDS and Second, an individual classifier may not perform well in the detection of each type of attacks. Third, many models are built for stale datasets, making them less adaptable for novel attacks. So, they propose a new intrusion detection framework in this paper, and this framework is based on the feature selection and ensemble learning techniques. For this a heuristic algorithm called CFS-BA is proposed for dimensionality reduction. Then, they introduce an ensemble approach that combines C4.5, Random Forest (RF), and Forest by Penalizing Attributes (Forest PA) algorithms. Finally, voting technique is used to combine the probability distributions of the base learners for attack recognition. The advantage of this technique is that it outperforms related feature selection approaches in terms of Acc, F-Measure, ADR, and efficiency while limiting FAR at relatively low levels. In addition, their solution shows outstanding performance in terms of ADR metric when compared to other classification algorithms, , and the comparison results with the state of the art methods indicate that the proposed CFS-BA-Ensemble method can provide a powerful competitive advantage in the intrusion detection domain.

[5] An effective analysis on intrusion detection systems in wireless mesh networks - 2017

Issues for developing IDSs in WMNs are 1) supporting interoperability and 2) handling volatile parameters. Also, security standards for WMNs are still in draft stage, and to protect the WMN, IDSs of similar wireless networks such as wireless sensor, Ad-Hoc, MANET can be adopted, but best performance is not guaranteed. If we look for solution in Intrusion Prevention Systems (IPSs), the problem of internal attackers cannot be addressed completely using their mechanisms. Hence, IPSs are of no use. The support from IDSs becomes mandatory, who are comprehensive to detect internal attackers. In this work, they have analysed IDS instead of IPS. The key issue of IDS is to set the parameters to identify the attacks such as packet drop, delay etc. So, we have classified the existing IDSs for wireless networks into four categories namely single layer IDS, cross-layer IDS, reputation-based IDS, reputation based cross-layer IDS, and analyzed their performance with core-layer attacks and detection methodology. They address loopholes in existing IDSs and specify research directions for improving the existing IDSs and for developing new efficient IDSs w.r.t. mesh networks. Each type of IDS has its own advantages and drawbacks w.r.t. core layer attacks and resource constraint devices. This information is very beneficial for the development of new IDSs. Though this study has proposed some helpful classifications for the identification of each type of IDS, but they didn't provide any methods on how to utilize these information in developing the current IDSs.

[**6] A Novel Feature Selection Method Using Whale Optimization Algorithm and Genetic Operators for Intrusion Detection System in Wireless Mesh Network – 2020**

The noisy and redundant features of network data degrades the performance of attack detection classifiers. So, the selection of informative features plays a vital role in enhancement to the IDS. In this paper, a wrapper-based approach is proposed using the modified Whale Optimization Algorithm (WOA). To overcome the issue of local optimal solution due to premature convergence in WOA, a method in which the Genetic Algorithm (GA) operators were combined with the WOA is proposed. The crossover operator was used to improve the search space of whales, and the mutation operator helped in the local solution issue. The proposed method selects informative features from network data, which helps to accurately detect intrusions. Using a Support Vector Machine (SVM), types of intrusions based on the selected features are identified. The performance of the improved method was analyzed using the CICIDS2017 and ADFA-LD standard datasets. The proposed method had better attack detection rate than the standard WOA and other evolutionary algorithms; it had good accuracy and was suitable for IDS in the WMNs. Performance of IDS was increased with the improved WOA. The attack detection ratio was higher than standard WOA. Also, result shows that the proposed method takes more time for training because of the selection of more informative features, so its time taking.

[7] Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection - 2018

The redundant and irrelevant variables in the monitored data affect the accuracy of attack detection by the system. Hence, feature selection techniques are essential to improve the performance of the system. In this paper, an IDS with genetic-algorithm-based feature selection and multiple SVM classifiers for WMNs are proposed. The proposed system selects the informative features of each category of attacks rather than the features common to all the attacks. The proposed system is evaluated using intrusion datasets generated by simulating a wireless mesh network in Network Simulator 3 and considering packet delivery ratio, delay, etc. as parameters. Experimental results of GA+SVM based feature selection on different datasets show that the False Negative Rate(FNR) values of all the attacks were quite higher. But at the end, use of the informative features of each category of attacks yields a higher accuracy of detection than the use of common informative features, for particular attacks.

[8] Efficacy of Machine Learning-Based Classifiers for Binary and Multi-Class Network Intrusion Detection - 2021

There are two categories of intrusion detection methods: signature-based IDS (SIDS) and anomaly-based IDS (AIDS). Both of them have drawbacks. SIDS is unable to detect zero-day attacks and AIDS produce false results caused by changes in user habits. Hence, a simple, efficient method is proposed where the rare attacks are regrouped into new classes to reduce the number of target classes and increase the number of instances in the target class providing a better intrusion detection rate in a real scenario NIDS. The number of classes are reduced, which increases the performance of ML classifiers. Deriving highly correlated features with the output class, improving the ML model's performance on intrusion datasets. Benchmarking different ML algos on different intrusion datasets providing similar insight into the approach's efficacy. Though, deep learning method requires the high computing power where high random access memory (RAM) and graphical processing units (GPU) are required to process the big NIDS dataset. Still, results reveal that the ML classifiers' performance improved when the number of

target classes decreased. The addition of a highly correlated feature to the output class increases the performance of classifiers and hence improved the intrusion detection accuracy.

[9] Trust-based hybrid IDS for rushing attacks in wireless mesh networks - May 2020

The main aim of this paper is to prevent several types of attacks like blackhole, grayhole, wormhole and rushing attacks due to some vulnerable features like shared wireless medium, multi-hop, highly dynamic network topology and decentralized architecture. These can be prevented by Trust-based hybrid IDS since they can secure the network performance even in hostile environment. At first, the trust nodes consider the minimum delay parameter to suspect a node as rushing attack. Then, the trust nodes monitor the suspected node behaviour and maintain the reputation value. In the calculations, the network coverage area is considered as two-dimensional space (X,Y). Based on the network dimensions, around nine trust nodes are required to monitor all network nodes. If we compared the proposed IDS approach goodput with non-attack and jellyfish attack scenarios goodput, the proposed IDS has shown poor network performance from 1 – 3 sec before the detection of rushing attacks. From the 4 sec, it improves the throughput. Based on the simulation analysis, we conclude that the proposed IDS have detected and isolated the three rushing attacks within 3 secs.

[10] An optimized intrusion response system for MANET - June 2017

The main aim of this paper is to address MANET security issues through a comprehensive analysis of blackhole, gray hole and the selfish behavior attack with the help of an intrusion response system called MASID-R-SA. It is used because it provides autonomic systematic responses based on the severity level. It consists of a set of agents in charge of performing a distributed and cooperative intrusion detection. If an anomaly is detected and there is not enough evidence, the neighboring LIDSs will participate in the detection process by providing some additional information. The study revealed that the proposed system solves some critical issues related to network partitioning and remerging efficiently. The approach reduces the effects of false positive alarms and the possibility of network partitioning. The limitation is that the node mobility makes the problem of detecting intruders harder. Also, this paper is limited to the detection of blackhole, gray hole, and the selfish behavior attacks.

[11] Detection of interruption attack in the wireless networked closed loop industrial control systems - Sept. 2019

The main aim of this paper is to detect the interruption attacks in the industrial control systems. This is because many attackers try to corrupt the information by making traffic. To overcome this problem, Mesh Intruder detachment scheme has been proposed because it not only detects the interruption attacks but also remove unwanted distortions. In the wireless network, XN is remotely connected to the SCADA. In the SID design, redundant data Ri is deducted by correlating all values to 0′s and 1′s. Extra information added by the intruder IN is pre-processed to detect and separate the information containing extra noise. The real data set is taken from the wind turbine SCADA and it is stored in an excel sheet. The time complexity is calculated using the optimization and classification technique. This analysis is compared with the existing method to find accuracy in detecting time complexity and better performance is evaluated. The limitations are degradation in network performance due to time delay and each wind turbine produces different data analytics because it depends on the weather and operational conditions.

[12] A Binary Classification Approach for Time Granular Traffic in SDWMN based IoT Networks - Jan. 2020

The main aim of this paper is to perform a binary classification on time granularity based IoT network traffic by employing different Machine Learning techniques to solve the problem of large amount of varying granular network traffic with the help of Traffic Classification (TC) technique. It helps to classify this multi-granular traffic and also proves to be beneficial in firewall building, intrusion detection, etc. The proposed architecture mainly consists of IoT Nodes, MRs, and a controller. The statistics module monitors the traffic coming to and going from the controller node, and forwards the extracted statistics to the FGT based classification module. The performance metrics, such as throughput, packet loss, and time is considered to determine the current network congestion state in the traffic networks. The data-set is comprised of multiple time-based multi-granular data subsets. DT, SVM, and KNN are well known ML classifiers. The best minimum accuracy for 45 sec OTP data subset is produced by SVM and KNN and for 50 sec OTP data subset is DT and SVM. Thus, the achieved reliable accuracies can be used to implement the proposed architectural model in real-environment in future.

[13] Compressed Sensing based Intrusion Detection System for Hybrid Wireless Mesh Networks – 2018

The main aim of this paper is to decrease intrusion detection overhead as it is a severe challenge for IDS to reduce detection overhead and delay while keeping high detection accuracy. So to overcome this problem a compressed sensing (CS) theory based IDS for hybrid WMN was proposed and also a new attack metric called Active State Metric (ASM) to detect intrusions was proposed In Intrusion Detection System Architecture, each mesh node calculates attack metric data with compressive sampling. The attack metric data are encapsulated into independent detection packets and sent to the mesh gateways. Then by using CS theory to reconstruct the complete metric data and make detections. A new attack metric named ASM (Active State Metric) was introduced to recognize the attacks like black hole attack. For Signal Reconstruction and Detection, Greedy algorithm called Sparsity Adaptive Matching Pursuit (SAMP) was used. The Main Advantage of SAMP is that it is capable of signal reconstruction without prior information of the Sparsity. Through intensive simulations, the result showed that the ASM can recognize the attacks well with high DR, low FPR and FNR.

[14] RTT based wormhole detection for wireless mesh networks – 2020

The main aim of this paper is to detect the malicious nodes in order to prevent AODV routing protocol against wormhole attack in WMNs. For that a wormhole detection algorithm was proposed which is based on the calculation of round trip time (RTT) and processing time Tran et al. Proposed Transmission Time based Mechanism (TTM) to resist wormhole attack to secure AODV routing protocol but this system suffers from vulnerabilities such as detecting wrong wormhole link in the presence of multirate transmission. So, a new protocol, RTT based algorithm in conjunction with processing time for the detection of malicious nodes in WMNs was proposed. It is able to detect the higher rate of malicious nodes . This new proposed protocol is better than the existing protocol. Here Comparison was based on the detection rate.

[15] Support vector machine-based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid – 2017

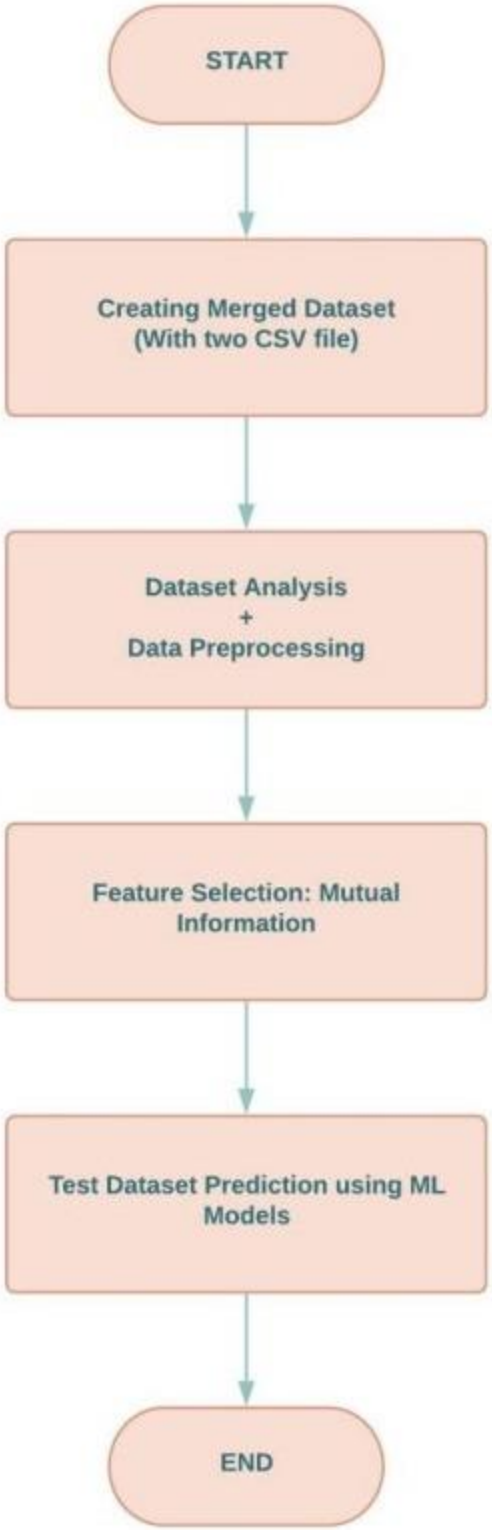
The main of this paper is to detect the cyber-attacks occurring in AMI communication network of smart grid. So for that a multi-SVM based intrusion detection system is developed for detecting different attacks from the collected data efficiently. The different topology and communication networks of smart grid requires the intrusion detection system as second layer of defense to detect security breaches and attacks unnoticed by security algorithms and authentication systems. The security is improved by placing IDS at each data concentrator or gateway in distributed manner. The feature dimensionality issue in the implementation of multi-SVM based IDS to smart grid is solved by feature selection using mutual information technique. Mutual information technique is a filter method that measures how much the individual feature tells about the classes in the dataset. The informative features selected by mutual information technique given as input to multi-SVM classifier has high detection ratio than artificial neural network. The simulation result proves that the proposed IDS accurately detects the attack and is most suitable to secure the AMI communication of smart grid.

[16] A Deep Learning Method with Filter Based Feature Engineering for Wireless Intrusi on Detection System – 2019

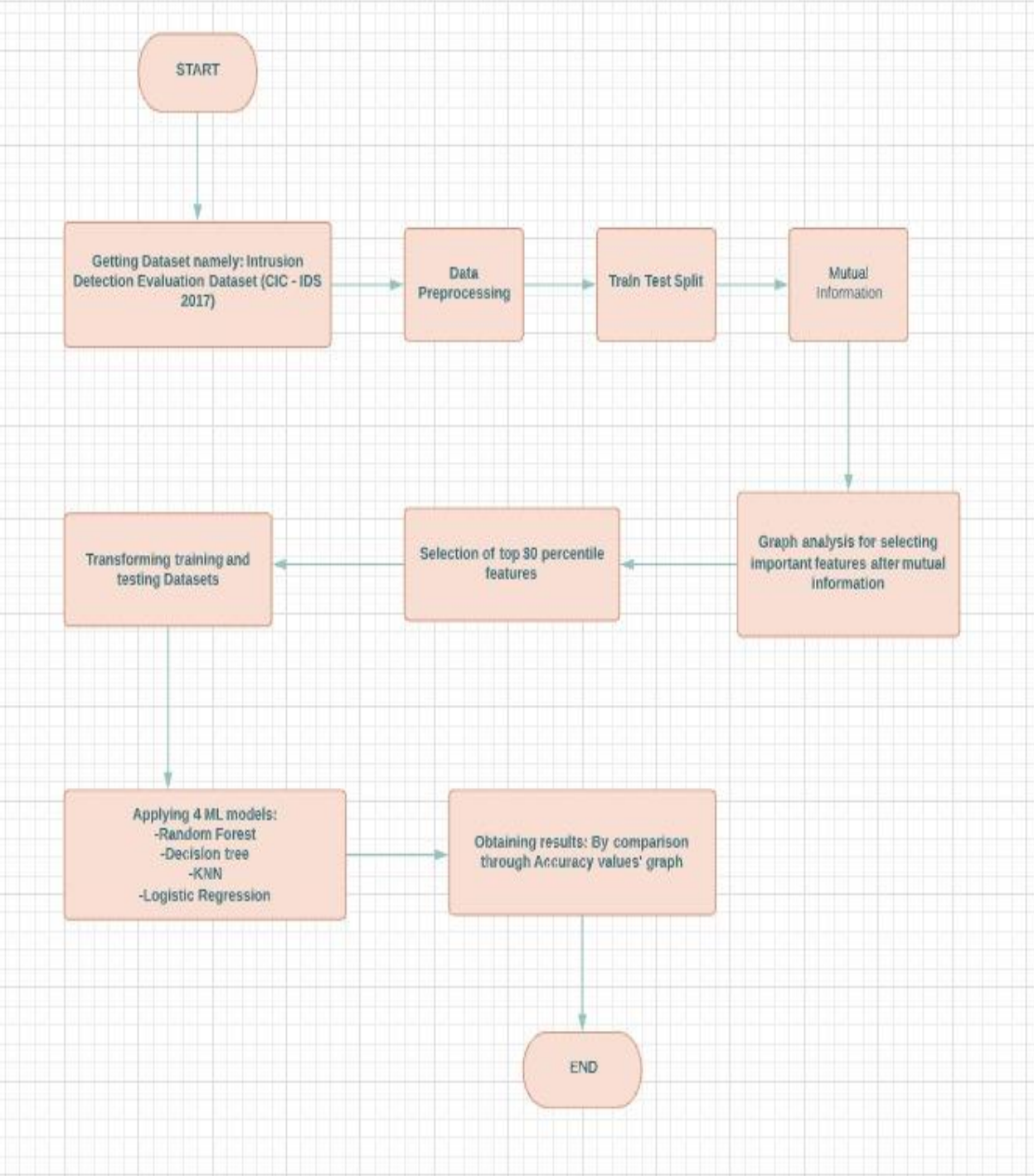
This paper presented the design, implementation and testing of a DL based intrusion detection system using FFDNNs. A literature review of ML and DL methods was conducted and it was found that the most efficient approach to intrusion detection has yet to be found. The FFDNN models used in this research were coupled to a FEU using IG in a bid to reduce the input dimension while increasing the accuracy of the classifier. The dataset used in this work is the NSL-KDD. For the binary and the multiclass classifications problems, the FFDNNs models both with a full and a FEU-reduced feature space achieved a performance that is superior to SVM, RF, NB, DT and KNN.

Proposed Work:

High-Level Architecture:



Low-Level Diagram:



Explanation:

In architecture, Firstly the dataset is acquired from the website namely “Intrusion Detection Evaluation Dataset of 2017”.

Then we move on to data preprocessing, In this the main aim is to process the data by removal of all unwanted features such as constant, Quasi constant & Duplicate features.

After its completion we split the total data in training &testing samples.

Then we apply the mutual information (MI) techniques as mentioned in the given base paper for selecting best features out of total features.

We did this by performing the graph analysis on the values obtained by appling Mutual information (MI) on each and every features.

After the analysis we decided to select to 30 percentile features for the model training purpose.

Now before training the models, training and testing dataset are transformed correspondingly for convenience of further computations.

Then for our project we choose four Machine Learning (ML) models. As follows:

1. Random forest

2. Decision tree

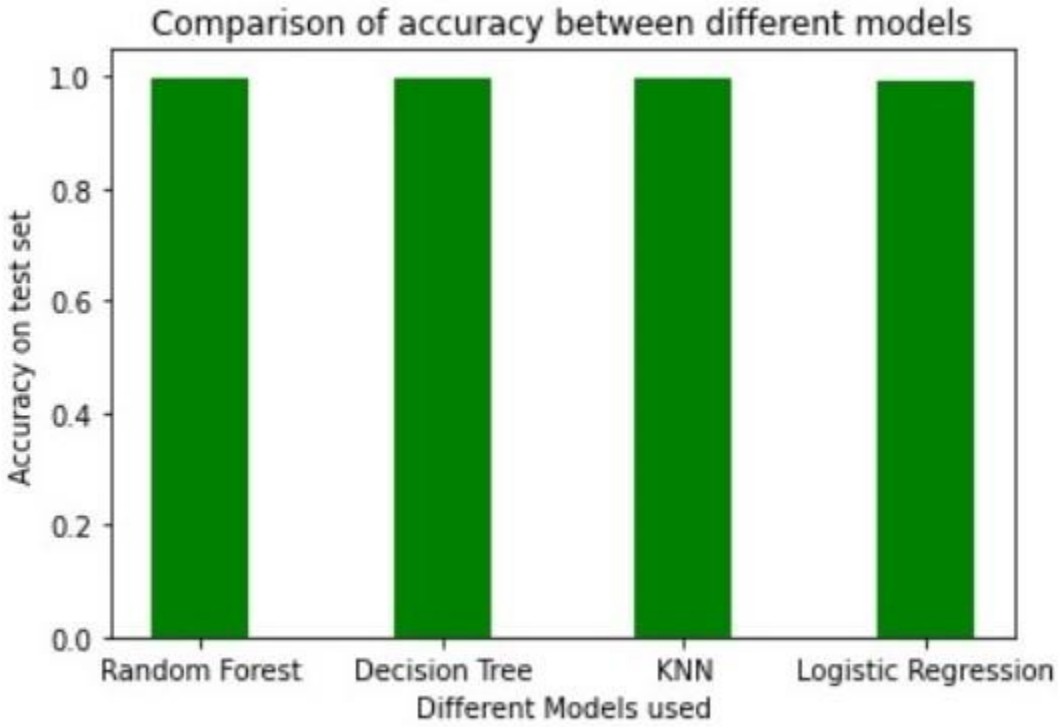
3. KNN

4. Logistic regression

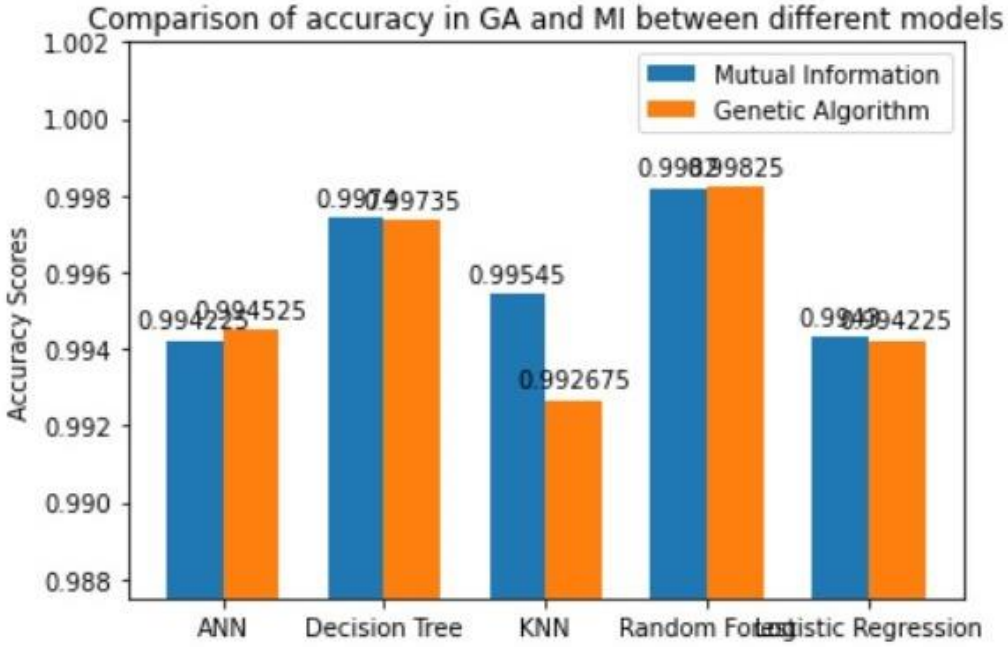
After its application, Finally the accuracy results of each and every models are obtained and compared. And the best model is found out of all.

Results – Review 2 and Review 3 results (Graphs, Tables preferred, Comparative analysis with individual algorithms)

<u>Review 2</u>: Mutual Information ML algorithm's comparison:



<u>Review 3</u>: Comparison between all ML algorithms with MI and GA



Conclusion:

At the end of the project, we found Random Forest Classifier. To be the most accurate Machine Learning Model when feature selection process was carried out in both Mutual Information (MI) and Genetic Algorithm (GA).

The accuracy score of Random Forest in MI is 0.9982 and GA is 0.99825 which was way higher than the rest ML models such as Decision Tree, KNN, Logistic Regression. Even it exceeded the accuracy score of the deep learning model that is Artificial Neural Network (ANN).

References:

[1] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in IEEE Access, vol. 7, pp. 41525-41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[2] M. Almseidin, M. Alzubi, S. Kovacs and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), 2017, pp. 000277-000282, doi: 10.1109/SISY.2017.8080566.

[3] Sultana, N., Chilamkurti, N., Peng, W. et al. Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Netw. Appl. 12, 493–501 (2019). https://doi.org/10.1007/s12083-017-0630-0

[4] Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai, Building an efficient intrusion detection system based on feature selection and ensemble classifier, Computer Networks, Volume 174, 2020, 107247, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2020.107247.

[5] K. G. Reddy, V. P. Raju and P. S. Thilagam, "An effective analysis on intrusion detection systems in wireless mesh networks," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 2213-2220, doi: 10.1109/ICACCI.2017.8126174.

[6] Vijayanand, R. and Devaraj, D. (2020) ‘A Novel Feature Selection Method Using Whale Optimization Algorithm and Genetic Operators for Intrusion Detection System in Wireless Mesh Network’, IEEE Access, Access, IEEE, 8, pp. 56847–56854. doi: 10.1109/ACCESS.2020.2978035.

[7] Vijayanand, R., Devaraj, D. and Kannapiran, B. (2018) ‘Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection’, Computers & Security, 77, pp. 304–314. doi: 10.1016/j.cose.2018.04.010.

[8] T. Acharya, I. Khatri, A. Annamalai and M. F. Chouikha, "Efficacy of Machine Learning-Based Classifiers for Binary and Multi-Class Network Intrusion Detection," 2021 IEEE International Conference on Automatic Control & Intelligent Systems (I2CACIS), 2021, pp. 402-407, doi: 10.1109/I2CACIS52118.2021.9495877.

[9] Reddy, K. & Thilagam, P.. (2020). 5 TRUST-BASED HYBRID IDS FOR RUSHING ATTACKS IN WIRELESS MESH NETWORKS: Recent Advances in Computer based Systems, Processes And Applications © 2020 by Taylor & Francis Group, London, ISBN 978-1-003-04398-0

[10] Mechtri, L., Tolba, F. D., & Ghanemi, S. (2018). An optimized intrusion response system for MANET: Peer-to-Peer Networking & Applications, 11(3), 602–618.

[11] Benisha RB, Raja Ratna S. Detection of interruption attack in the wireless networked closed loop industrial control systems. Telecommunication Systems. 73(3):359-370. doi:10.1007/s11235-019-00614-3

[12] R. Kumar, U. Venkanna and V. Tiwari, "A Binary Classification Approach for Time Granular Traffic in SDWMN based IoT Networks," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020, pp. 531-534, doi: 10.1109/COMSNETS48256.2020.9027336.

[13] T. Shi, W. Shi, C. Wang and Z. Wang, "Compressed Sensing based Intrusion Detection System for Hybrid Wireless Mesh Networks," 2018 International Conference on Computing, Networking and Communications (ICNC), 2018

[14] Roy, A.K., Khan, A.K. “RTT based wormhole detection for wireless mesh networks”. Int. j. inf. tecnol. 12, 539–546 (2020)

[15] R. Vijayanand, D. Devaraj and B. Kannapiran, "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017

[16] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System," in IEEE Access, vol. 7, pp. 38597-38607, 2019

Google drive link of code of review-2 and review-3

Review-2

Google Drive Links of individual works of Team members:

Naman Sethi - 19BIT0002
https://drive.google.com/file/d/1IvLjgTI8z4sSav3tcknPxRhp0G0zCI94/view?usp=sharing

Keshav Agarwal - 19BIT0009
https://drive.google.com/file/d/1NKPLW2ATckF6r2xELAcSDj5FQTrZqmW-/view?usp=sharing

Chaitanya Singh – 19BIT0044 https://drive.google.com/file/d/1Y-gsOZh28wzopQVMakqHk_SMqI1lI2mb/view?usp=sharing

Sourabh Karmakar – 19BIT0048
https://drive.google.com/file/d/1WmKFWcH47JdYobmR-ZU8Nk1Ngciaxxky/view?usp=sharing

Google Drive Link of Supplementary Material related to the Project:
https://drive.google.com/file/d/1KXCtV4QVLrInadNUWbzkJ-WULRqzG0Eh/view?usp=sharing

Review-3

https://drive.google.com/file/d/1dnQfwyvLbub8W30qki3VR7o5lpAEF9pn/view?usp=sharing