Intrusion Detection System using Homomorphic Encryption

Aakash Singh
Student, B.Tech Information Technology
Sardar Patel Institute of Technology(S.P.I.T)
Mumbai, India.
aakash.singh@spit.ac.in

Parth Kitawat
Student, B.Tech Information Technology
Sardar Patel Institute of Technology(S.P.I.T)
Mumbai, India.
parth.kitawat@spit.ac.in

Shubham Kejriwal
Student, B.Tech Information Technology
Sardar Patel Institute of Technology(S.P.I.T)
Mumbai, India.
shubham.kejriwal@spit.ac.in

Swapnali Kurhade
Professor, B.Tech Information Technology
Sardar Patel Institute of Technology(S.P.I.T)
Mumbai, India.
swapnali.kurhade@spit.ac.in

Abstract — IT infrastructures are more at risk of attacks related to cybersecurity. Modern businesses need a great deal of security in order to be protected against various attacks like U2R, Probe, R2L, and denial-of-service (DoS) etc. The issue with current IDS is that the analysis of the system data is done by external SOC(Security Operational Centers) which brings up many security concerns like revealing the details of the network packet which in turn reveals really important information about the company's regular activities. We are proposing a method in which we are basically assessing the detection model on the system data privately such that the system data, as well as the detection model, is encrypted which helps in minimizing information leakage. Our desired security goal will be that the security operation centre isn't able to learn anything about data owners data, as well as the data owner isn't able to learn anything about SOC's model. We encrypt the DO's data and the SOC's model. The various machine learning algorithms can be explored for the detection model like support vector machines, decision trees and neural networks.

Keywords—Intrusion Detection System(IDS), Security Operation Center, Homomorphic Encryption

I. INTRODUCTION

Our project lies in the domain of Cyber Security, in which it mainly focuses on Intrusion Detection. Intrusion Detection System is one of the major topics going on in the world. With hackers using new techniques and technologies, there is an increased interest in the field of Cyber Attack Detection System as we now have more advanced threats. For defence against cyberattacks like Denial of Service(DoS), R2L, U2R and Probe Intrusion Detection Systems are a valid and convenient solution. Many IDS rely on two techniques for efficient detection: (1) surveilling IT systems to collect data such as system logs and network packets, or (2) using detection models like anomaly detection, classifiers, attack signatures, which is used to classify the system data. Needless to say, a precise detection model plays a critical part in the operation of an IDS. Moreover, an IDS which is accurate enough can be formed only when we have a set containing an ample amount of historical data indicating attacks and good expertise in this field. Also, alleviation, prevention, and reaction after an attack has occurred need teams which have some well-defined skill sets. Thus, externalizing the IDS to cybersecurity specialists is a good policy for many organizations. The security operation center, also called SOCs, are a convenient and economical alternative. The issue with current IDS is that the analysis of the system data is done by external SOC(Security Operational Centers). Intrusion Detection Systems classify attacks by tracking various activities in IT systems containing various computers and network links. This is done by monitoring system data, which can be taken from multiple sources like system network traffic or log files which can reveal sensitive information about the firm or organization. This brings up many security concerns like revealing the details of the network packet which in turn reveals really important information about the company's regular activities. The main objectives of this paper include providing an end to end encrypted model such that the SOC is not able to learn anything about the Data Owner's data, to evaluate the

Intrusion detection model on the system data using different machine learning algorithms. To evaluate this model with other traditional or existing Intrusion Detection Systems with respect to security analysis and performance. For this, we tried various machine learning models and different types of encryption techniques. The main crux of our paper is to create an Intrusion Detection System which is highly efficient, secure, and maximizes the leakage prevention of sensitive information from the Data Owner's side.

II. Related Work

Intrusion Detection System is one of the major topics going on in the world. All the work done by a company can be stolen in moments if the company cannot stop intruders from stealing their data or if the company does not know that someone has hacked their system, or if an attack has occurred or not in either of which cases the data is going to be leaked. IDS at the moment has two types based on Data source: either network based or host based. In Intrusion Detection using a host based system the data is being taken from the Host's computer, it also keeps check on log Files and network traffic in accordance with Host Computer[4]. Network-Based IDS keeps checking on data packets of user's work in a network[4]. In this paper by Roshan Kumar, the authors worked on a misuse based intrusion detection system. Intrusion detection based on Anomaly and Misuse are also 2 categories of IDS's [5]. Anomaly Intrusion Detection System takes into account the history of user's actions whereas Misuse IDS uses a set of predefined rules in order to work[5]. Updation of these rules should be regular. As defined by S.Niksefat, we learn how to classify privacy issues in intrusion detection systems[1]. There are no techniques that can identify all types of intrusion, therefore to protect data, the model is chosen on the specific application[1]. The dataset is very difficult to obtain for intrusion detection projects. The dataset must contain various types of cyber-attacks which can be used to attack the data owner. I.Sharafaldin takes a dataset which includes various attacks and defines the best set of features to be considered while tackling those attacks[6]. In this paper by R.A.Popat, they encrypted the data before sending it to SOC and also encrypt features used in IDS to prevent data leakage to security system owner and model to the data owner. R.A.Popat implements three different algorithms in encryption where the Decision Tree is three times more efficient than other methods[7]. D. Archer implements steganography to secure data storage on the cloud[3]. The most optimizable and secure encryption we have seen is Homomorphic Encryption. As it easily works on Big Data[2]. In their scenario, they used machine learning to their advantage by using such models for intrusion detection purposes. We can put to work a Machine learning model which first ranks the security features based on the effect those features had and later on help construct a specialised tree based Intrusion Detection System on the basis of the features that had previously been selected[12]. Also, we can use an algorithm in which we first make random combinations of 3 features using simulated annealing and then SVM is applied on that feature combination, which is then able to detect anomalous behaviour from the internet data traffic[9]. Also using a good fusion of machine learning feature selection techniques and classifiers we can produce high performance generating combinations[10]. Now Deep learning is one of the complex branches of ML that helps us learn the ranked feature depiction and constant, continuous relationships by passing the network information through various layers that are hidden. This field of Deep learning has been successful to achieve significant results in artificial intelligence, recognition of speech, processing of image, etc. Now, these performances are also used for various cybersecurity things like IDS,classifying virus attacks,
analyzing and predicting possible network traffic, detecting ransomwares, categorizing texts that are encrypted, detecting URLs that can be harmful, detecting various anomalies, and detecting domain names which can be harmful. The paper basically concentrates on doing the analysis regarding the efficiency of several classical ML models with Deep learning models for Network based Intrusion Detection System using the datasets of NIDS that are accessible openly like the KDD Cup dataset, the NSL KDD dataset, etc[13]. A lot of academic analysis to better the efficiency of Intrusion Detection System has been done using the benchmark KDDCup dataset. Attacks can be classified into Probe attacks, Denial of Service attacks, User to Root attacks, and the Remote to local attacks. The Intrusion Detection System created using the RNN model has a good ability for creating efficient systems for detecting an intrusion, with a great precision for both multiclass and binary classification[11]. We can create a system using the techniques that are stated above as an alternative to the traditional Intrusion Detection Systems.

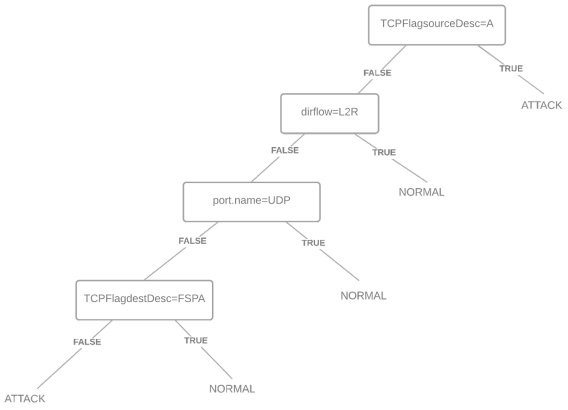
III. Technologies and Concepts

Security data:- If a data which is obtained from a networked system, that basically helps us to find if attacks, threats, suspicious behaviour, anomalies, or any type of unsanctioned action has occurred, then this data is known as security data. Eg network packets, system log files, etc. The company or firm, which is responsible for providing security data is known as the Data Owner.

IDS:- IDS a system that has been specifically designed for surveillance of software security. It raises an alarm or an alert whenever an attack on the software occurs, or if there is a breach of privacy.

Detection Model:- Detection model is basically a machine learning model which takes the historical data pertaining to security as input and uses it for intrusion detection. In the image shown below, the decision tree depicted is one of the eg. of model used for detection where the node of the tree are

the TCP flag description for source and destination, flow direction and the name of the protocol



Intrusion Policy:- It is just a bunch of attack policies which when enforced, applying the OR operation indicate if or what type of an attack has occured.

Homomorphic encryption:- It is a technique of encryption that allows us to operate on encrypted data without decrypting it first. It is a very important concept used in our paper is it basically helped us to prevent the leakage of Data Owner's data at the Security Operation Center(SOC).There are four main functions provided to us by the Homomorphic Encryption system, these are:-

Encryption: Encryption to Cipher text from normal text.

Decryption: Decrypting a Cipher text to a normal text.

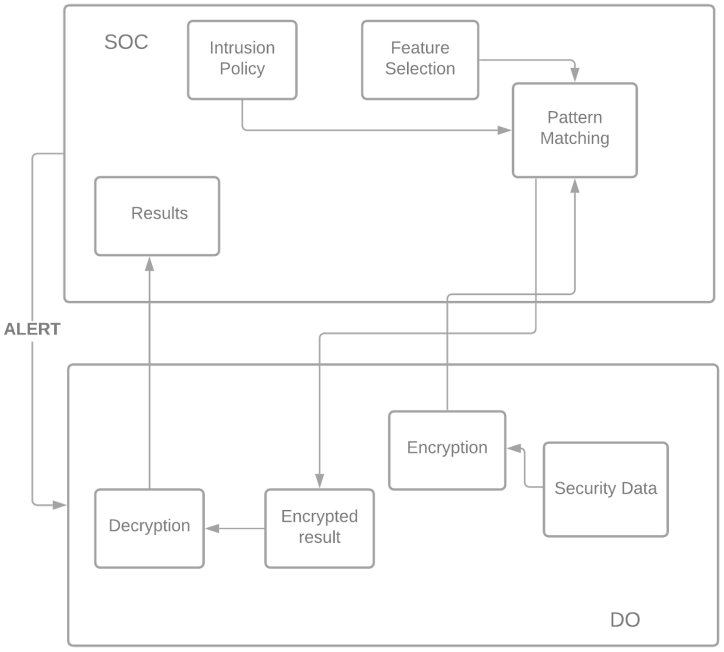
Key generation: Producing private and public keys.

Evaluating: The process of performing on data that has been encrypted, carrying out the procedure represented in the binary circuit. In every binary circuit it is compulsory to describe the depth, number of inputs, and the size.

Partial Homomorphic Encryption: Partial Homomorphic Encryption(PHE) subset of encrypting using homomorphic systems in which only a certain amount of arithmetic procedures or functions can be executed on the values that have been encrypted. The basic essence of the PHE is that only certain functions like multiplication or addition can be executed an endless number of times on the Ciphertext. Paillier Cryptosystem is also a PHE, what is it and how we can use it is explained in the below stated paragraph.

Paillier Cryptosystem: Paillier Cryptosystem is a Partially Homomorphic System which was created by Pascal Paillier in the year 1999. It is supposed to have to have only two types of operations. First operation is for the addition of the ciphertext, and the second operation is for multiplication of the same. What we used in our paper for encryption was this paillier Cryptosystem which helped us convert the data into ciphertext and help us perform operations on this encrypted data which was later decrypted at the Data Owner's Side.

IV. System Diagram

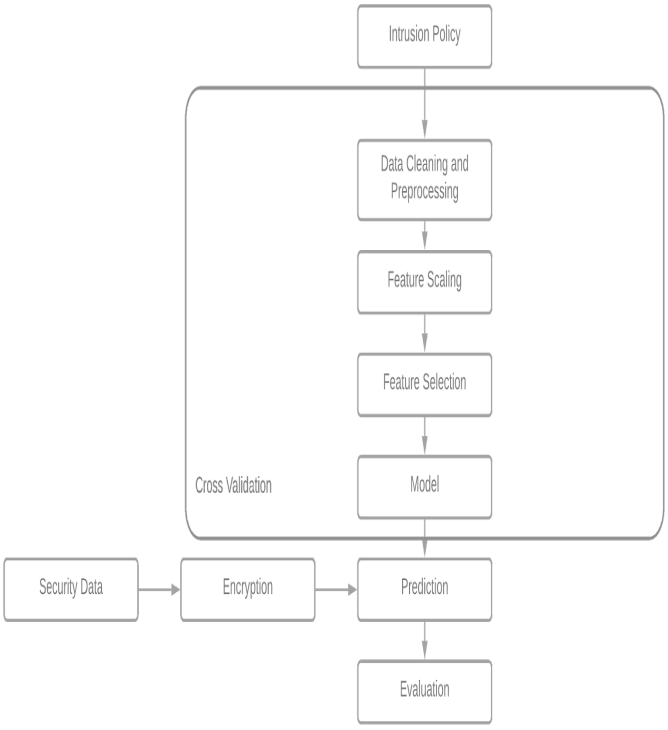


In the proposed system, there are two entities involved: Data Owner(DO) and Security Operation Center(SOC). Security data is owned by the Data owner but lacks the expertise in the field of intrusion detection and thus shares its data with the external SOC which has the required expertise and offers its intrusion detection service to the data owner. DO but it's hesitant to share the data with an external party because of security concerns and does only after having taken all the necessary precautions.

1. First, SOC with the help of an intrusion policy which is just another defined bunch of intrusion detection configurations forms its proprietary detection model.
2. The feature selection process is used to eliminate features which are either redundant or irrelevant to lower the computing time.
3. The data owner then encrypts the security data with its public key using partial homomorphic encryption and sends it to the SOC.
4. After the pattern matching phase, the result of the phase which is encrypted by default is sent to the DO. The DO then decrypts the results using its private key and sends it to the SOC for examination.
5. The SOC then decrypts the result and learns about the offensive records and to which rule in the intrusion policy are these records matched.

6. It then alerts the Data Owner in case of an intrusion and sends the offensive records and also advises on the steps to be taken in case of an attack.

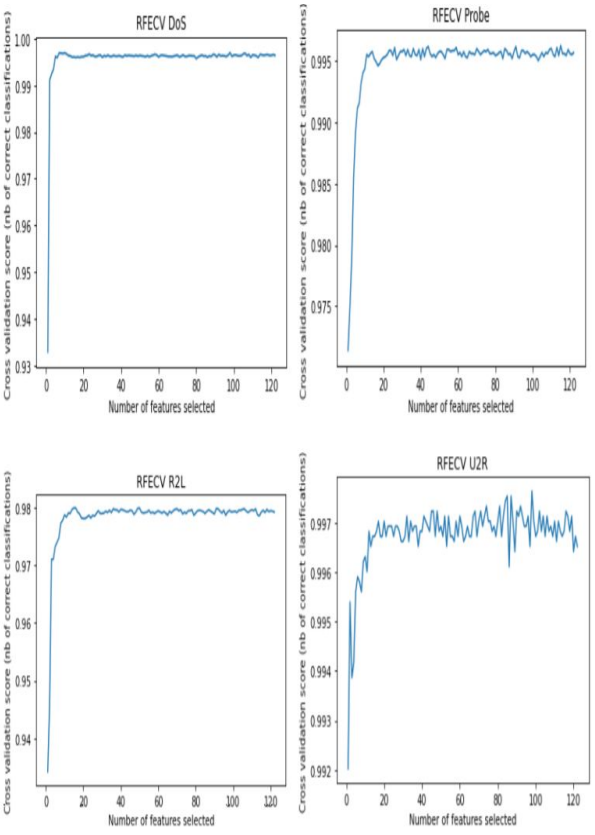
V. Implementation Details



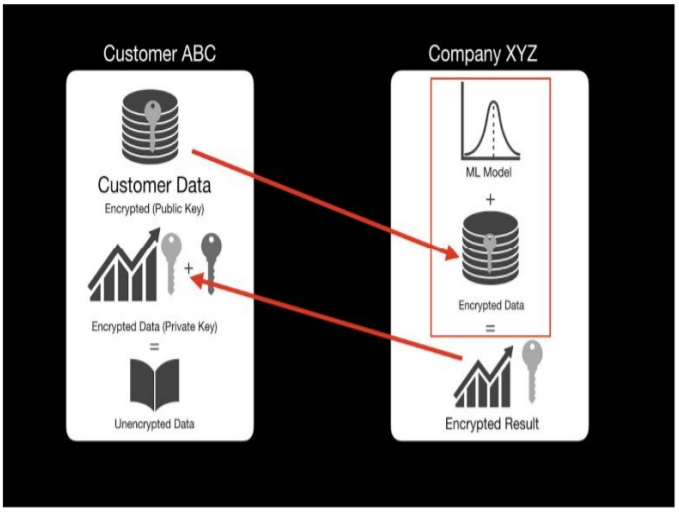
Data Cleaning and Preprocessing:
The duplicates have already been removed as NSL KDD dataset is already standardised. The nan and Infinity values are replaced with zero initially. Preprocessing operation is done on the dataset as the dataset contains numerical and non-numerical values. One-Hot Encoding is used for this operation. An integer matrix denoting the values of the categorical features is an input to the One Hot Encoder. This will transform all the categorical features to their corresponding binary features out of which one will be active at a time. The dataset is then divided into four parts based on the attacks(U2R, Probe, DoS, R2L) which need to be classified.

Feature Scaling:
Featuring scaling is performed to steer clear of features which have large values as this will affect the final result. Standard Scaler is used to perform this operation. In Standard Scaler the average for a feature is calculated and then the mean is subtracted from the current value of the feature and the result is divided by the Standard Deviation. The standard deviation will be 1 after each feature is scaled.

Feature Selection and Model:
It is the process in which irrelevant and unnecessary features are eliminated with minimal information loss. Subsets of the features are selected which fully represents all the features in the dataset in terms of accuracy and other metrics. It is also possible that there is a correlation between features when a large number of features are present. Feature selection also helps to eliminate this problem. We have used Recursive Feature Elimination(RFE) to perform this operation. We plot the graph for the accuracy against the number of features and based upon that we select the optimal number of features for each of the attacks. Here, we have built two models: Decision Trees, Random Forest. Both machine learning models are built for all 4 types of attack i.e U2R, R2L, DoS and Probe. This model is used on the dataset containing every feature(123) and also separately for the features(13) selected after feature selection operation.



Encryption:



- The customer data is encrypted using a public key at the Data Owner and is sent to the SOC and the encryption scheme used is a paillier cryptosystems based partial homomorphic encryption system.
- At the SOC the encrypted data is applied to the machine learning model which produces the encrypted result as an output
- That encrypted result is sent to the Data Owner where it can be decrypted using a private key which is only available with the Data Owner and not the SOC.
- Then the unencrypted data is again encrypted using a simple encrypted scheme to maintain end to end encryption and protect the system from external adversaries knowing about the system.
- The result is decrypted at the SOC and an alarm is raised if an intrusion has happened and appropriate steps to be taken in this situation to reduce the severity of the attack damage will be provided to the DO.

VI. Results and Evaluation

Evaluation Metrics:

Intrusion Detection is considered and approached as a problem where the records need to be categorized into two classes either malicious(Intrusion attack) or normal state . SOC raises an alarm when the record is categorized as malicious. In practice the Intrusion Detection System misses some attacks or falsely classifies some attacks. The evaluation metrics of any Intrusion Detection System therefore must take all of the above mentioned points into consideration. We calculate four metrics on the basis of which we assess the performance of our Intrusion Detection System. Given below is the confusion matrix which is a collection of four values: TP, TN, FP, FN.

	ACTUAL VALUES		
PREDICTED VALUES		Actual: NO	Actual: YES
	Predicted: NO	True Negative	False Negative
	Predicted: YES	False Positive	True Positive

METRICS	FORMULA
Accuracy Rate	TP+TN/TP+FP+FN+TN
Recall(Detection Rate)	TP/TP+FN
Precision	TP/TP+FP
F-1 Score	2*(Recall * Precision) / (Recall + Precision)

Results:

All the implementations which include training the data,extracting the features and homomorphic encryption have been implemented using the python libraries. Partial Homomorphic encryption based on paillier cryptosystems is achieved using the paillier library in python. Below is the result for attacks(DoS, Probe, U2R, R2L) obtained when Decision Trees is used as Intrusion Detection Model.

DoS	
Accuracy	0.99738
Precision	0.99692
Recall	0.99705
F- Score	0.99698

U2R	
Accuracy	0.99652
Precision	0.87538
Recall	0.89540
F- Score	0.87731

Probe	
Accuracy	0.99085
Precision	0.98674
Recall	0.98467
F- Score	0.98566

R2L	
Accuracy	0.97459
Precision	0.96689
Recall	0.96086
F- Score	0.96379

Given below is the result obtained for attacks when Random Forest is used as an Intrusion Detection Model. There are 4 types of attacks included here namely DoS, R2L, U2R, Probe

which are included in the KDD dataset.(KDD dataset is the benchmark dataset when it comes to Intrusion Detection).

DoS	
Accuracy	0.99819
Precision	0.99866
Recall	0.99718
F- Score	0.99792

U2R	
Accuracy	0.99795
Precision	0.96125
Recall	0.88784
F- Score	0.98710

Probe	
Accuracy	0.99571
Precision	0.99392
Recall	0.99267
F- Score	0.99329

R2L	
Accuracy	0.98182
Precision	0.97544
Recall	0.97298
F- Score	0.97419

VII. Conclusion And Future work

In this paper we present a protocol for signature based IDS on security data which is encrypted. This protocol helps the data owner to trust the third party security operations center which has the required expertise in IDS, because he is confident that the security data will remain encrypted during the entire protocol and can never be decrypted without the private key which is held only by the data owner. Decision trees and Random forest are used for the machine learning model which are then privately evaluated over the encrypted network data using Homomorphic Encryption. This intrusion detection protocol has several drawbacks mainly because of the high computing power required by Homomorphic encryption algorithm and significantly higher overhead generated by HE compared to the traditional approaches. Also the IDS generates alerts after a certain time lag as the SOC does not have any clear information on the output of the intrusion detection model which is also encrypted and needs to be sent to the data owner where it is decrypted using the private key. The decrypted results are then sent to the SOC for analysis and thus the time lag. The Future work would be to try to use parallel execution to reduce the overhead that comes with homomorphic encryption and to include other intrusion detection models and classification methods in our proposed system.

References

[1] S.Niksefat, P.Kaghazgaran and B.Sadeghiyan “Privacy issues in intrusion detection systems: A taxonomy, survey and future directions”. Comput. Sci. Rev., 25, 69–78,2017.

[2] D. Archer, L. Chen, J. H. Cheon, R. Gilad-Bachrach, R. A. Hallman, Z. Huang, X. Jiang, R. Kumaresan, B. A. Malin, H. Sofia, Y. Song, and S. Wang, “Applications of homomorphic encryption,” Homomorphic Encryption.org, Redmond WA, Tech. Rep., July 2017.

[3] J. Anitha Ruth ; H. Sirmathi ; A. Meenakshi, “Secure Data Storage and Intrusion Detection in Cloud Using Mann and Dual Encryption through Various Attacks”, IET Information Security (Volume: 13 , Issue: 4 , 7 2019), Tamil Nadu, India, 17 June 2019, Tamil Nadu, IEEE.

[4] Sarathiel Chaipa ; Mariki M Eloff ; Mariki M Eloff, “Towards the development of an Effective Intrusion Based Detection Model”, 2017 Information Security for South Africa (ISSA), Johannesburg, South Africa, 16-17 Aug. 2017, Pretoria, IEEE.

[5]R. Kumar and D. Sharma, "Signature-Anomaly Based Intrusion Detection Algorithm," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2018, pp. 836-841, doi: 10.1109/ICECA.2018.8474781.

[6] I.Sharafaldin, A. H.Lashkari,, and A. A.Ghorbani “Toward generating a new intrusion detection dataset and intrusion traffic characterization” ICISSP, Funchal, Madeira-Portugal, 22–24 January 2018.

[7] R.Bost, R. A.Popa, S.Tu, and S.Goldwasser, “Machine learning classification over encrypted data”, presented at the 2015 NDSS conference, CA, USA, Feb.8–11, 2015.

[8] L. P. Dias, J. J. F. Cerqueira, K. D. R. Assis and R. C. Almeida, "Using artificial neural networks in intrusion detection systems to computer networks," 2017 9th Computer Science and Electronic Engineering (CEEC), Colchester, 2017, pp. 145-150, doi: 10.1109/CEEC.2017.8101615.

[9] Md. N.Chowdhury and K.Ferens, M.Ferens, “Network Intrusion Detection Using Machine Learning”,In 2016 Int. Conf.on Security and Management SAM'16.

[10] Saroj Kr. Biswas CSE dept., NIT Silchar, Assam, India, 788010,”Intrusion Detection Using Machine Learning: A Comparison Study”, Volume 118 No. 19 2018, 101-114

[11]C. Yin, Y. Zhu, J. Fei and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," in IEEE Access, vol. 5, pp. 21954-21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[12] I.Sarker, A.Yb, F.Alsolami, A.Khan, “IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model”, may 6, 2020, doi:10.20944/preprints202004.0481.v1

[13] G. Meena and R. R. Choudhary, "A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA," 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, 2017, pp. 553-558, doi: 10.1109/COMPTELIX.2017.8004032.