# HIGH PERFORMANCE NETWORK INTRUSION DETECTION ENGINE

**K. S. Dhanalakshmi**
Assistant professor III, Department of ECE, School of Electronics and Electrical Technology.
Kalasalingam Academy of Research and Education, Anand Nagar.
Krishnankoil, Virudhunagar District, (India).
E-mail: k.s.dhanalakshmi@klu.ac.in
ORCID: https://orcid.org/0000-0001-6285-3656

**S. Sorna Bala**
Student, Electronics and Communication Engineering.
Kalasalingam Academy of Research and Education. Madurai, (India).
E-mail: balaabi2608@gmail.com
ORCID: https://orcid.org/0000-0003-0112-493X

**M. Subha**
Student, Electronics and Communication Engineering.
Kalasalingam Academy of Research and Education. Madurai, (India).
E-mail: subhamuthuraj1998@gmail.com
ORCID: https://orcid.org/0000-0002-7945-451X

**R. Subharisha**
Student, Electronics and Communication Engineering.
Kalasalingam Academy of Research and Education. Madurai, (India).
E-mail: subharisha29@gmail.com
ORCID: https://orcid.org/0000-0002-5374-8800

**Recepción:** 16/10/2019 **Aceptación:** 28/09/2020 **Publicación:** 30/11/2021

**Citación sugerida:**
Dhanalakshmi, K. S., Sorna, S., Subha, M., y Subharisha, R. (2021). High performance network intrusion detection engine. *3C Tecnología. Glosas de innovación aplicadas a la pyme, Edición Especial,* (noviembre, 2021), 53-69. https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

# ABSTRACT

Security administration plays a significant role in network management tasks. The intrusion detection systems are designed to shield the provision, confidentiality and integrity of vital network information systems. The system we have planned to design can scan, classify and monitor the network traffic in real time while not affecting network throughput. Since most of the business intrusion detection systems are at usually expensive or abundant costly and that they tend to represent a major resource demand in themselves, for tiny networks, use of such IDS isn't possible. Thus, principally open supply IDS are being employed. IDS are one in everything about preeminent tried and dependable advances to watch the approaching and active system traffic to spot unapproved utilization and no right treatment of PC frameworks arrange. NIDS are normally incapable to execute whole system bundles, which winds up in fragmented investigations and in this way considerable postponements in fast and high-load conditions. HIDSs can watch malevolent networks and multiple actions happening isolated the endangered host. An HIDS stays located next to the tip purpose of an electronic network that has anti-threat applications like spyware detection, firewalls and antivirus software system plans, which give access to outdoor backgrounds like the Web.

# KEYWORDS

Intrusion detection system, Network Security, Network Intrusion Detection System, Intrusion Detection Expert System.

# 1. INTRODUCTION

In this project we've the world design of SOC box in addition as many strategies accustomed take a look at its accuracy and performance.

Security could be a noteworthy worry in every aspect of our reality. New systems and instrumentation are conceived to affirm protection. Notwithstanding, PC systems still face a few dangers. There are normally three phases to accomplishing security in processing framework systems: interference, location and amendment. Interference is attractive to recognition and redress, anyway it is beyond the realm of imagination to expect to stop 100 percent of assaults. In addition, identification methods give extra right leads in recognizing malignant aggressors than redress procedures.

Redress methods are embraced to shield PC frameworks. Together with aversion, they effectively work to dam interruptions, however, it will still battle a thriving intrusion. All the same variety of thriving attacks can be controlled exploitations, various effective assaults can be controlled utilizing counteractive action procedures if an assault is recognized at the between time phases of bar frameworks. This is regularly intense, because of some independent assaults will overcome the anticipation framework. It's a matter of a framework being assaulted, traded off, and therefore breaking down. Here we require a between time stage like the discovery stage, that should be certain all through interruptions.

Accordingly, the discovery approach is most well-gotten a kick out of the chance to constrict system cost and fill inside the hole among revision and avoidance components.  Snort could be a tool for tiny, gentle utilized network. Snort is beneficial when it is not cost efficient to deploy NIDS. Snort includes a real time alerting capability. Snort will be designed for long periods of your time while not requiring observance or body maintenance, and might so evenly utilized as an integral a part of most network security infrastructures. Accuracy and False Negative Rate (FNR) & False Positive Rate (FPR) are accustomed compare performance of algorithmic rule. Accuracy is used for mensuration the share of failure and proper detection similarly as the range of false alarms generated from IDS. FNR could be a proportion of samples that are according as traditional. FPR could be a proportion of set to give traditional instances that is incorrectly classified.

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

This section offers a short review of the prevailing analysis work associated with intrusion detection system. From Big Data Analytics for Network Intrusion Detection paper, we tend to came to understand that this analogy network flows, logs and system events for intrusion detection by Wang and Jones (2018), in this projected system, the big data analysis will correlate multiple information sources into coherent read, determined suspicious activities and eventually accomplish economical intrusion detection. Wei Wa Nge conferred a Light Weight Intrusion Detection in laptop Networks. In this paper, the intrusion detection in big data environment needs for light weight models that are ready to accomplish real time performance throughput detection. It improves the potency of information process in intrusion detection. In this work we projected three strategies of information abstraction particularly, ideal extraction, attribute choice and attribute abstraction.

Roesch (1999) conferred a Snort Light Weight Intrusion Detection for Network. In this paper, Roesch (1999) had realized the various applications wherever the snort can be terribly helpful as a component of an integrated network security infrastructure. Snort was designed to fulfil the necessity of a prototypic lightweight network intrusion detection system. Lee and Huang (2013) given a Pattern Matching Scheme with High Throughput Performance and Low Memory Requirements. Serving and detection of malicious attacks against networks was mentioned in this paper (Lee & Huang, 2013). The pattern-matching architecture with high throughput performance and low memory requirements.

Armstrong, Korah, and Salivahanan (2018) presented an Efficient String Matching FPGA for Speed Up Network Intrusion Detection. In this paper, the authors had discussed about the efficiency of IDS using FPGA that designed by string- matching system. The proposed system can maintain throughput of 19.2 Gbps with performance in terms of Performance Efficiency Metric (PEM). In this paper Armstrong *et al.* (2018) discussed about the emerging new artificial intelligence technique which can be used in the real-life problems. They have also made an approach for user behavior modelling and presented the display results from the preliminary testing needed for their project. Zhang *et al.* (2001) presented a Hide: A Hierarchical Network IDS. In this paper, Zhang *et al.* (2001), described about the architecture of their system i.e., Hierarchical Network Intrusion Detection System. They had also briefed the contents about statistical pre-processing techniques and components.

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

Jyothi, Addepalli and Karri (2018) presented a DPFEE: a High Performance Scalable Pre-Processor for Network Security Systems. In this paper, the authors, had discussed about the Deep Packet Field Extraction Engine (DPFEE) for application layer field extraction to software. It also Provides software acceleration for field extraction and operates at their maximum efficiency. Sadhasivan and Balasubramanian (2017) presented a Novel LWCSO-PKM Based Feature Automation and Classification of Attack Types in SCADA Network. In this paper the authors had explained about the Linear Weighted CSK Optimization (LWCSO) algorithm which is used to achieve better performance than the existing classification techniques and Intrusion Detection System algorithms (Sadhasivan & Balasubramanian, 2017a). This also helped a lot for our project in detecting Intrusions that more often affects the network systems.

## 2. LITERATURE SURVEY

An Intrusion Detection System (IDS) is a device or software application that monitors a networks or systems for malicious activity or policy violations. Any malicious activity or violations are typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system (Roesch, 1999). In the past years, there are no techniques available for the detection of Intrusion occurring in a system or engine since 1984 (Lee & Huang, 2013). Between 1984 and 1986, Dorothy and Denning and Peter Neuman researched and developed the primary model of the Intrusion Detection System. This image was named as Intrusion Detection Expert System (IDES). This ady was at first rule primarily based expert system trained to discovered the malicious activity (Armstrong *et al.*, 2018).

In 2017, under the title "Big Data Analytics for Network Intrusion Detection" Randy Jones bought a conclusion for the problem of investigating the progressive of strategies techniques in network intrusion detection. His conclusion is that cleaning and querying information with incomplete creaky records (Zhang *et al.*, 2001). In 2016, Martin Roesch (1999) has revealed a paper on the title "SNORT- Light-weight Intrusion Detection for Networks". Within the paper he designed Snort to fulfill the necessities of a prototypic light-weight network intrusion detection system that may be an answer for the matter of finding totally different applications wherever it is terribly helpful as a component of an integrated network security infrastructure.

For the purpose of achieving high throughput performance and low memory requirements by helping and detecting malicious attacks against networks by Lee and Huang (2013).

## 3. BLOCK DIAGRAM

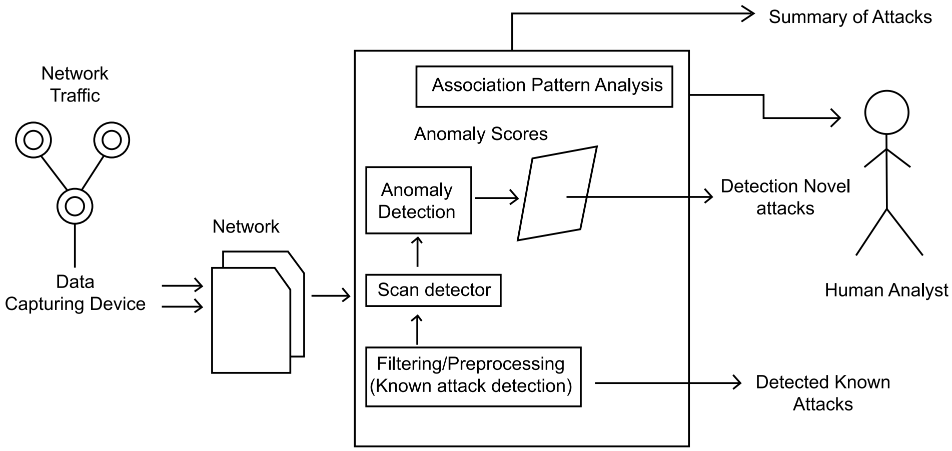

**Figure 1.** Block Diagram of Intrusion Detection Systems.
**Source:** own elaboration.

Anomaly detection is needed to scan the attackers which will intrude the network. It is needed because nowadays the network traffic was very high which is having many possibilities of assaulting the data's which are valuable. Hence the network intrusion system is very important for analyzing the attackers such as Harmful viruses etc. The above diagram Figure 1 explains the IDS system which will works to safeguard the data's present in the network.

## 4. DESCRIPTION

We begin by providing a general summary of the system, followed by the presentation of the design wherever we tend to detail every part. The proposed system of our work is explained here with the steps involved in the Intrusion Detection System to safeguard the Data. The Steps involved are Preprocessing, DOS analysis with respective classification and clustering methods.

## 4.1. PRE-PROCESSING

Pre-processing may be a data mining technique that involves remodeling raw information into a comprehensible format. Real world information is commonly incomplete, inconsistent, or lacking in sure behaviors or trends and is probably going to contain several errors. Pre-processing may be a verified methodology of partitioning such problems. Pre-processing prepares raw information for any processing. The normal data pre-processing methodology is reacting because it starts with data that's assumed prepared for analysis and there's no feedback and impact for the manner of data assortment. The information inconsistency between data sets is that the main issue for pre-processing.

The Major task of pre-processing are:

- Data Cleaning: may be a method of fill in missing values, smoothing the noisy data, establish or take away outliers and resolve inconsistencies.
- Data Integration: Integration of multiple data bases, data cubes or files.
- Data Transformation: is a task of data standardization and aggregation.
- Data Reduction: Data reduction is that the method of reduced illustrations in volume however produces the identical or similar analytical results.
- Data Discretization: It may be a part of data reduction however with explicit importance, particularly for numerical information.
- Segmentation: may be a method dividing the market of potential customers into totally different teams and segments on the idea of sure characteristics. Segmentation suggests that to divide the market place into components, or segments that are determinable, accessible and profitable and have a growth potential.
- Feature extraction: may be a transformation of the computer file into a group of options that are distinctive properties of input pattern that helps in differentiating between the classes of input pattern. It's the method of etymologizing new options from the initial features so as to scale back price of feature mensuration, increase classifier potency, and permit higher classification accuracy. Remodeling the computer file into the set of options is named feature extraction. If the feature

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

extractors are rigorously chosen it's expected that the feature set can perform the required task victimization the reduced illustration rather than full size input. Feature extraction refers to extraction of linguistic item from the documents to produce a sample distribution of their content. This can be the method by that a brand-new set of discriminative options is obtained from those accessible new set of features. This can be a method of reducing information by measure of sure or options. These options are employed in a classifier. Once the information is simply too massive to be processed, the information is remodeled into a reduced illustration set of options. The methods of choosing a set of variables that's to be employed in the development of the feature vector. It's spatiality reduction method, wherever associate degree initial set of raw variables is reduced to lot of manageable teams for process. Classification of intrusions is based on:

- Location.
- Functionality.
- Deployment approach.
- Detection mechanism.

## 4.2. DENIAL OF SERVICE (DOS)

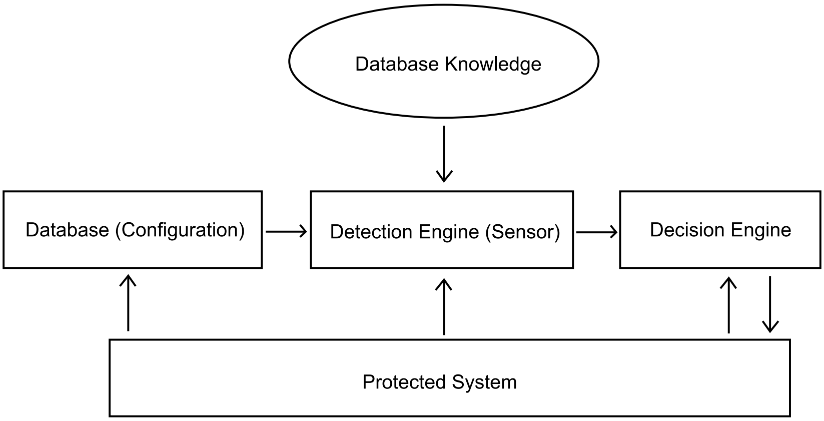

**Figure 2.** Denial of Service.
**Source:** own elaboration.

The above Figure 2 describes a DOS attack. It's associate degree attack within which the attacker floods a computing or memory resource with false request so it is unable to function

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

as the legitimate request and therefore denying users access to the service. Probing is an attack with the goal of gaining the configuration of the target machine or network.

User to Route (U2R): These attacks have the goal of gaining body access to the machine within which the attacker encompasses a user level access.

Remote to Local (R2L): R2L is an attack within which the user sends packet to a machine over web which the user doesn't have access to so as to show the vulnerabilities and exploit privileges which a neighborhood user would wear a pc. Performance Analysis: It is a measure of the success or failure of a project using various parameters. It helps in developing a positive culture of project management that yields excellent results.

A good program performance typically needs: proper management of stack holders, Performance Analysis may be method of examination actual project value and schedule performance to the performance activity baseline for the aim of analyzing this standing of a project. Intrusion Detection System: An intrusion detection system (IDS) is utilized to make security experts mindful to bundles coming and takeoff a checked system. IDSs are ordinarily acclimated smell out system bundles, in this manner giving an OK comprehension of what's very occurring on the system. An IDS depends on either equipment or code, any place approaching and cordial individuals and additionally system traffic are tuned in to, and can possibly notice and report any evidence of assaults.

The common activities of IDS code will be named pursues:

- Monitoring whole or potentially fractional packets.
- Detecting suspicious exercises.
- Recording required occasions and making refreshes the system manager.

The specialized IDS mechanism is predicted on however, wherever and what it detects, together with obligatory necessities. In particular, IDSs should be bolstered flexible and ascendible system parts to oblige the powerful increment in the present system situations. They should give simple give direct administration and operational systems and ventures as opposed to confusing basic undertakings, and that they should give simple ID components. Intrusion Detection System (IDSs) can be classified into 3 types: a Network-Based Intrusion Detection System (NIDS) and a Host-Based Intrusion Detection System

(HIDS), and a Hybrid-Based Intrusion Detection System (hybrid IDS) associate an HIDS detects malicious activities on a one personal computer whereas an NIDS distinguishes interruption by recognition numerous hosts and looking at system traffic. IDS technologies like HIDS, NIDS are used along to correlate information from every device and create choices consistent with what these IDSs monitors.

IDS are classified into 3 primary sorts: network-based, host-based and hybrid. Network-based IDSs: Network-based IDSs (NIDSs) have become a vital element of an associate organization's security solution. Associate NIDS is equipped for location a wide fluctuate of noxious and undesirable assaults happening in an application, system and transport layers, together with unforeseen administrations bolstered on various applications. Moreover, NIDSs can find and screen system traffic and secure PC frameworks from system based dangers while not arrange approach infringement.

NIDS are normally incapable to execute whole system bundles, which winds up in fragmented investigations and in this way considerable postponements in fast and high-load conditions.

It is currently normal to check NIDSs in rapid frameworks with massive accounts of information, however they're not able amend pernicious exercises and dangers. NIDS are effective and helpful in dominant malevolent activity and intimidations underneath environments wherever traffic is consistently upward. NIDSs are additionally divided into software or hardware-based. It's conjointly ascertained software-based NIDSs still need improvement for a network with a high capacity of high-speed knowledge, however they're helpful for little networks. However, one in all foremost robust and common ASCII text file NIDS is Snort. Host-based IDSs: Host-based IDSs (HIDSs are authorized to viewed alleged occasions occurring in home-grown host machines.

HIDS are adaptable because of their installation over servers, workstations and notebooks, as compared to NIDS. Additionally, HIDSs can watch malevolent networks and multiple actions happening isolated the endangered host. An HIDS stays located next to the tip purpose of an electronic network that has anti-threat applications like spyware detection, firewalls and antivirus software system plans, which give access to outdoor backgrounds like the Web.  It's going to battle with present security policies of firewalls and operational

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

schemes. It cannot simply investigate intrusion trials on several CPUs. It will be terribly troublesome to keep-up in massive networks with totally diverse operative systems and arrangements.

It will be restricted by assailants once the system is negotiated. Hybrid-based IDSs: In around things, HIDSs and NIDSs could incapable to accomplish the necessities aimed at intrusion detection as a result of somebody sort of IDS has each essential merits and faults. Consequently, a mix of an HIDS and a NIDS is thought as a Hybrid IDSs. Snort Summary: Snort is handy freed from price besides is stratified between the highest systems obtainable todays through the simplest options. It's discharged as an ASCII text file NIDS supported a rule-based IDS, that provisions data in text files, such text files will be changed by a text editor. Rules remain classified into categories wherever the principles that belong towards every class are hold on as information in isolated files; such records are then combined to the main configuration folder. The information is seized in standings supported on delineated rules, that are browse at the data configuring of the Snort.

Snort part roles: A Snort-based NIDSs incorporates the subsequent of the resulting foremost components:

- Packet Decoder.
- Pre-processors
- Detection Engine.
- Work and Alerting System and
- Output Modules.

Snort will drop few packets as a result of it runs in real time if the maneuver is in NIDS method with significant and high-volume traffic flow. This system employments the Snort instruction to sight the intrusion action to remain bestowed within the information packet. The Snort rule can read the chains which need to be matched against all packets.

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

# 5. EXPERIMENTAL RESULTS AND DISCUSSION

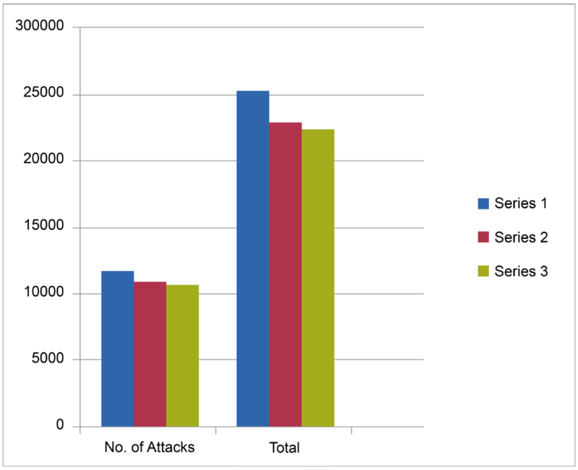

**Figure 3.** Graph representing no. of attacks and total datas.
**Source:** own elaboration.

The above Figure 3 shows the graph representing number of attacks and total datas. The graph is plotted between the number of attacks and total. The blue colour represents the number of attacks and the total of the first normal record. The red colour represents the number of attacks and the total of the second normal record. The green colour represents the number of attacks and the total of the third normal record.

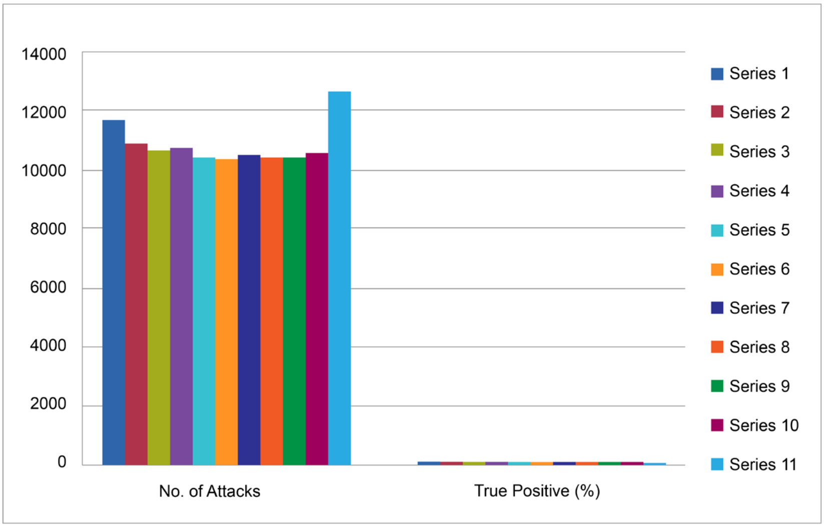

**Figure 4.** Graph representing no. of attacks and true positive %.
**Source:** own elaboration.

The above Figure 4 represents the graph of number of attacks and true positive

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

percentage. The graph is plotted against number of attacks to true negative percentage of the intrusion. The colour variations show the corresponding attack and its true negative percentage.

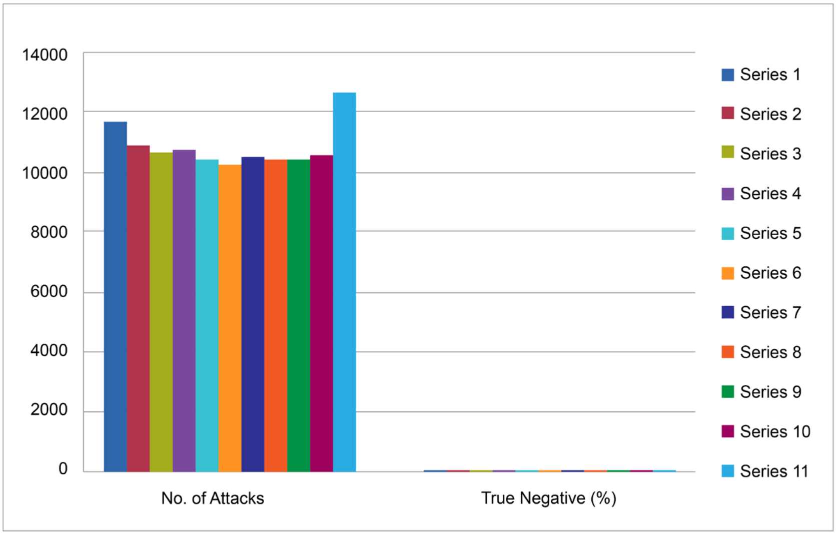

**Figure 5.** Graph representing no. of attacks and True negative %.
**Source:** own elaboration.

The above Figure 5 represents the graph of number of attacks and true negative percentage. The graph is plotted against number of attacks to true positive percentage of the intrusion. The colour variations show the corresponding attack and its true positive percentage.

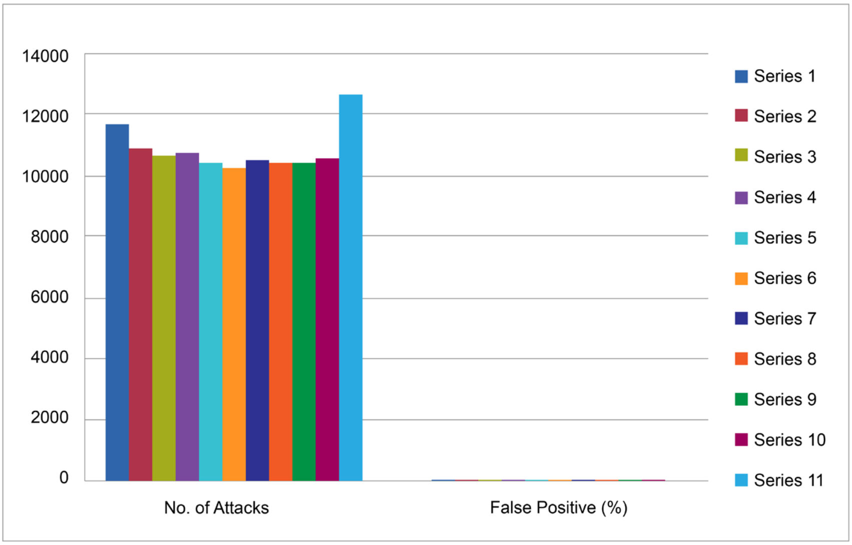

**Figure 6.** Graph representing no. of attacks and False positive %.
**Source:** own elaboration.

The above Figure 6 represents the graph of number of attacks and false positive percentage. The graph is plotted against number of attacks to false positive percentage of the intrusion. The colour variations show the corresponding attack and its false positive percentage.

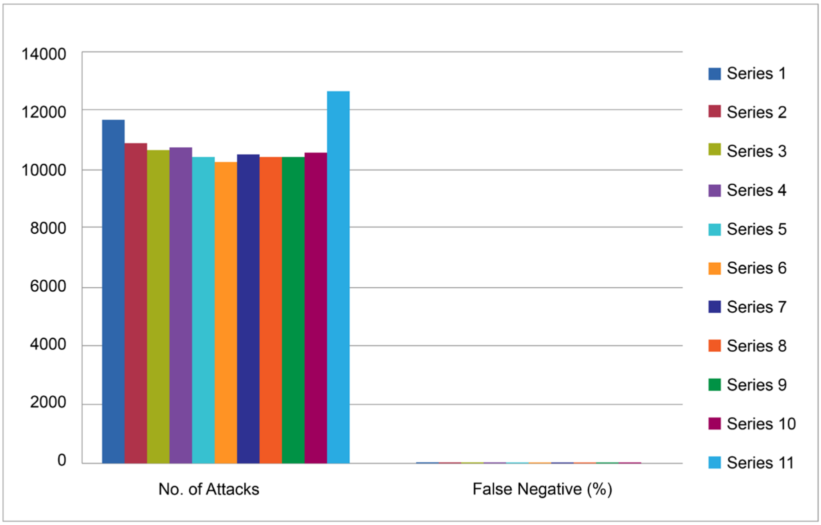

**Figure 7.** Graph representing no. of attacks and false negative %.
**Source:** own elaboration.

The above Figure 7 represents the graph of number of attacks and false negative percentage. The graph is plotted against number of attacks to false negative percentage of the intrusion. The colour variations show the corresponding attack and its false negative percentage.

# 6. CONCLUSIONS

We have considered a most recent dataset KDD set for detailed analysis keeping in view its increasing demand in the research community. Various shortcomings of the dataset have been studied and outlined. Solutions to counter such issues, has also been provided. We tried to solve such issues through experiment. We also re-label the dataset with the labeling information provided by Canadian Institute of Cyber security. Moreover, we have also seen a major issue of class imbalance has been reduced by such class relabeling. As a future work the dataset can be class wise resampled to generate two or more training and testing samples set separately to be used by research community. Snort was designed to fulfill the wants of a prototypal a light weight network intrusion detection system, it became a tiny

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69

low, flexible and extremely capable system that's in use round the world on each giant and tiny network.

## ACKNOWLEDGEMENT

We thank the Department of Electronics and Communication Engineering, School of Electronics and Electrical Technology of Kalasalingam Academy of Research and Education, Tamil Nadu, India for permitting to use the computational facilities available in Centre for Research in Signal Processing and VLSI Design which was setup with the support of the Department of Science and Technology (DST), New Delhi under FIST Program.

## REFERENCES

**Armstrong, J., Korah, R., & Salivahanan, S.** (2018). Efficient String Matching FPGA for speed up Network Intrusion Detection. *Applied Mathematic & Information Sciences, 12*(2), 397-404. http://www.naturalspublishing.com/files/published/u40jti0ukf6096.pdf

**Dhanalakshmi, K. S., & Kannapiran, B.** (2017). Analysis of KDD CUP Dataset Using Multi-Agent Methodology with Effective Fuzzy Based Intrusion Detection System. *Journal of Applied Security Research, 12*(3), 424-439. https://doi.org/10.1080/19361610.2017.1315760

**Jyothi, V., Addepalli, S. K., & Karri, R.** (2018). DPFEE: A high performance scalable pre- processor for network security systems. *IEEE Transactions on Multi-Scale Computing Systems, 4*(1), 55-68. https://ieeexplore.ieee.org/document/8078262

**Kabiri, P., & Ghorbani, A. A.** (2005). Research on intrusion detection and response: A survey. *IJ Network Security, 1*(2), 84-102. https://www.researchgate.net/publication/45681663_Research_on_Intrusion_Detection_and_Response_A_Survey

**Lee, T.-H., & Huang, N.-L.** (2013). A pattern-matching scheme with high throughput performance and low memory requirement. In *IEEE/ACM Transactions on Networking*

*(TON), 21*(4), 1104-1116. https://cial.csie.ncku.edu.tw/presentation/group_pdf/(TON)%20A%20Pattern-Matching%20Scheme%20With%20H.pdf

**Roesch, M.** (1999). Snort-Lightweight intrusion detection for network. *Proceedings of the 13th System Administration Conference.* Seattle: USENIX Association. Vol. 238. https://www.semanticscholar.org/paper/Snort%3A-Lightweight-Intrusion-Detection-for-Networks-Roesch/363d109c3f00026f9ef904dd8cc3c935ee463b65

**Sadhasivan, D. K., & Balasubramanian, K.** (2017a). A fusion of multiagent functionalities for effective intrusion detection system. *Security and Communication Networks. Article ID 6216078*. https://doi.org/10.1155/2017/6216078

**Sadhasivan, D. K., & Balasubramanian, K.** (2017b). A novel LWCSO-PKM-based feature optimization and classification of attack types in SCADA network. *Arabian Journal for Science and Engineering, 42*(8), 3435-3449. https://doi.org/10.1007/s13369-017-2524-0

**Wang, L., & Jones, R.** (2018). Big Data Analytics of Network Traffic and Attacks. In *IEEE National Aerospace and Electronics Conference (NAECON),* pp. 117-123. https://ieeexplore.ieee.org/document/8556802

**Wang, W., Liu, J., Pitsilis, G., & Zhang, X.** (2018). Abstracting massive data for lightweight intrusion detection in computer networks. *Information Sciences, 433-434,* 417-430. https://www.semanticscholar.org/paper/Abstracting-massive-data-for-lightweight-intrusion-Wang-Liu/6ee2cffa04c7ab2121c52734bf5238113ec6f9e0

**Zhang, Z., Li, J., Manikopoulos, C. N., Jorgenson, J., & Ucles, J.** (2001). HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. *Proceedings of the IEEE Workshop on Information Assurance and Security.* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.67.857&rep=rep1&type=pdf

https://doi.org/10.17993/3ctecno.2021.specialissue8.53-69