iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6010

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

A Review on Intrusion Detection System and Various Attacks on Network

Govind Narayan[1], Jyotir Moy Chatterjee[2]
[1]*M.Tech Scholar GD-RCET, Bhilai, Chhattisgarh, India*
[2]*Assistant Professor GD-RCET, Bhilai, Chhattisgarh, India*

Abstract: ***Intrusion detection systems are frameworks that can identify any sort of vindictive attacks, corrupted information or any sort of intrusion that can posture risk to our frameworks. In this paper, an investigation of different sorts of intrusion detection framework is done alongside the guide of many research papers which have utilized machine learning, DNA sequence, pattern matching, data mining as a strategy for learning attacks and taking preventive activities when comparable sorts of attacks are experienced later on. Investigation of these papers has given a profound knowledge to additionally investigate the related procedures in the field of Intrusion Detection Systems.***

Keywords: Intrusion Detection Systems, Data Mining, Clustering, Security, Anomaly based Intrusion Detection System.

I. INTRODUCTION

At present network, revolution is a fundamental piece of communication. In any case, with new patterns of the web, the dangers to the network is likewise expanding. The conventional gadgets, for example, firewall, and virus scanner are in their breaking points to adapt up to the developing number of astute attacks from the web. An attack is an acknowledgment of a risk to discover and exploit the framework powerlessness [11].

An intrusion detection framework is utilized to recognize a wide range of malicious network traffic and PC use that can't be identified by an ordinary firewall. An intrusion detection framework is a gadget normally an assigned PC framework that persistently screens movement to distinguish vindictive cautions. A solitary intrusion in a network can be the reason of data spillage and can perform data adjustments that are exceptionally hurtful to an association [12].

II. INTRUSION DETECTION SYSTEM (IDS)

Intrusion detection is characterized as the way toward observing the occasions happening in a PC framework or network and examining them for indications of intrusions, characterized as endeavors to bargain the secrecy, trustworthiness accessibility or to bypass the security instrument of PC or network [14]. The fundamental segments of IDS are appeared in Fig.1.

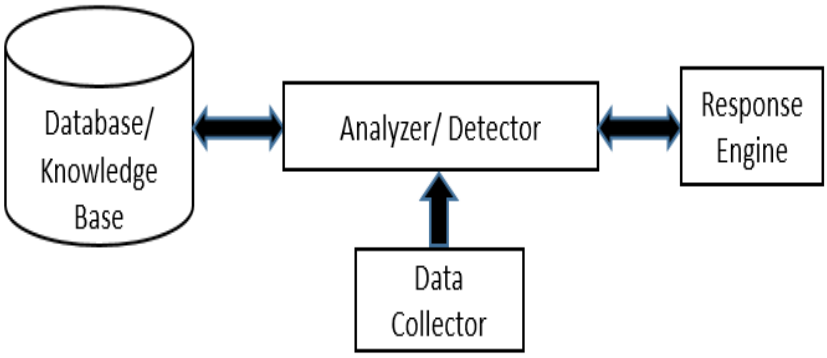


Fig. 1. IDS with its Components

III. COMPONENTS OF IDS

A. Data Collection/Preprocessor

Data collection segment is in charge of gathering and giving the review data that will be utilized by next part to decide. Data utilized for identifying intrusion ranges from user get to example to network parcel level highlights [13].

B. Analyzer (Intrusion Detector)

The analyzer or the intrusion detector is the center part which examines the review examples to identify attacks. This is a basic part and a standout amongst the most looked into. Different procedures are utilized as intrusion indicators [13]

C. System profile (database or knowledge base)

The framework profile is utilized to describe the typical and anomalous behavior. It is the knowledge base for attacks, setup data about the present condition of the framework and review data portraying the occasions that are going on the framework.

D. Response Engine

The response engine controls the response component and decides how to react. The framework may raise an alert and answer to overseer or may block the source of attack [13].

IV. IDS WORKING

A. An Ideal IDS must do the accompanying

1) It must run consistently without human supervision. The framework must be sufficiently dependable to enable it to keep running out of sight of the framework being watched.

2) It must be fault tolerant as in it must survive a framework crash and not lose its knowledge-base at restart.

3) It must force negligible overhead on the framework.

4) It must adapt to changing framework conduct after some time as new applications are being included.

V. ATTACKS ON IDS

In PC and PC networks an attack is any endeavor to wreck, uncover, modify, handicap, take or increase unapproved access to or make unapproved utilization of a source.

A. Denial of Service (DoS)

A denial-of-service (DoS) is any sort of attack where the attackers (programmers) endeavor to keep authentic users from getting to the service. In a DoS attack, the attacker ordinarily sends unnecessary messages asking the network or server to validate demands.

B. R2L(remote to local)

A R2L attacks are misuses in which the programmer begins off on the framework with a typical user record and endeavors to mishandle vulnerabilities in the framework to increase super user benefits.

C. U2R(remote to user)

A remote to user (U2R) attack is an attack in which a user sends bundles to a machine over the web, which he/she doesn't approach keeping in mind the end goal to uncover the machines vulnerabilities and endeavor benefits which a local user would have on the PC.

VI. CLASSIFICATION OF IDS

Intrusion Detection System can be classified into following categories below as shown in Fig. 2.

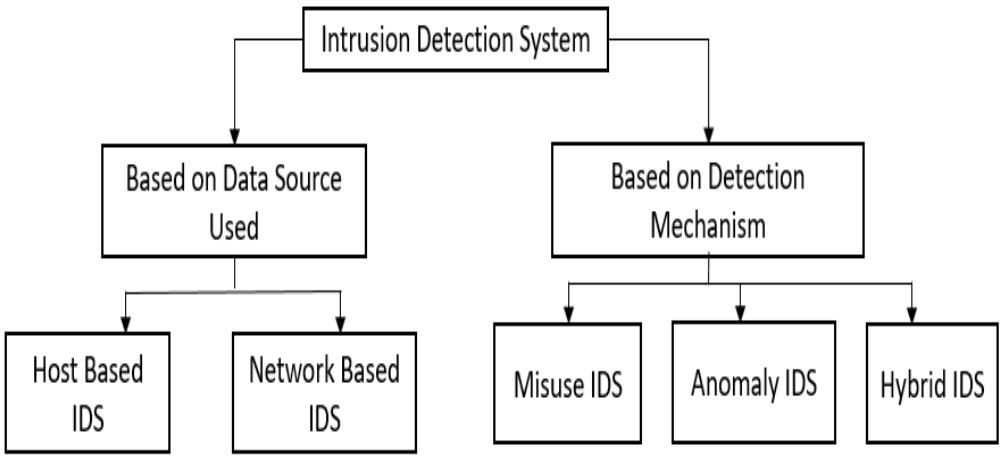


Fig. 2. Classification of IDS

A. Host Based Intrusion Detection

Host based IDS lives on the framework being observed. It comprises of a specialist on a host which recognizes intrusions by dissecting framework calls, application logs, record framework alterations and other host exercises and state.

B. Network Based Intrusion Detection

A Network Based Intrusion Detection System monitors and investigates the movement on its network section to distinguish intrusion endeavors. Execution for it requires

1) Network interface card to catches all movement that experiences the network.
2) Sensor which screens to decide whether, parcel stream matches with known mark [14].

C. Misuse Intrusion Detection System

This detection method utilizes particularly known examples to distinguish malicious code. These particular examples are called as marks. On the off chance that present movement coordinate with any of known marks a caution is activated.

1) *Low Rate of False Alarms:* The principle favorable position of misuse detection framework is their capacity to distinguish known attacks and the generally low false caution rate when rules are accurately characterized.
2) *Only Known Attacks:* The chief downside of misuse detection framework is their total failure in identifying obscure attacks [3].

D. Anomaly Intrusion Detection System

These strategies are intended to distinguish irregular conduct in the framework. The typical utilization design is base lined and alarms are produced when use goes deviates from the ordinary conduct.

1) *Unknown Attack Detection:* The fundamental preferred standpoint of anomaly detection framework is that in opposition to misuse detection framework, they can identify obscure or novel attacks.
2) *High Rate of False Alarms:* Very high rate of false alarms prompts exceptionally poor precision of anomaly detection framework [14].

E. Hybrid Intrusion Detection System

Early research works on intrusion detection frameworks recommended that the intrusion detection capacities can be enhanced through a hybrid approach comprising of both mark (misuse) detection and in addition anomaly detection. In such a hybrid framework, the mark detection system identifies known attacks and the anomaly detection method recognizes novel or obscure attacks.

Low False Rate: This strategy decreases the extensive number of false cautions produced by current anomaly detection approaches [11].

VII. LITERATURE SURVEY

In this segment, we survey the existing literature on IDS frameworks.

M. E. L. Ajjouri et al. [1], the advancement of data frameworks requires the usage of an abnormal state of security to limit the issues related with these frameworks. Intrusion Detection Systems (IDS) plays a critical part in the security of systems by identifying when an attack is going on, yet most current IDS are by and large brought together and experience the ill effects of noteworthy constraints. This paper depicts another security specialist engineering in light of adapting new attacks. We exhibit the inspiration and portrayal of the approach, at that point the system embraced for learning is Case based Reasoning (CBR).We additionally give our examination show utilizing the AUML dialect.

L. M. L. de Campos et al. [2], the point of this examination is to simulate a system movement analyzer that is a piece of an Intrusion Detection System - IDS, the primary concentration of research is information digging and for this sort of use the means that go before the information mining : information arrangement (conceivably including cleaning information, information transformations, choosing subsets of records, information standardization) are viewed as major for a decent execution of the classifiers amid the information mining stage. In this specific circumstance, this paper talks about and exhibits as a commitment not just the classifiers that were utilized as a part of the issue of intrusion location, yet in addition the underlying phase of information planning. In this manner, we tried the execution of three classifiers on the KDDCUP'99 benchmark intrusion identification dataset and chose the best classifiers. We at first tried a Decision Tree and a Neural Network utilizing this dataset, proposing changes by decreasing the number of attributes from 42 to 27 thinking about just two classes of recognition, ordinary and intrusion. At last, we tried the Decision Tree and Bayesian Network classifiers thinking about five classes of attack: Normal, DOS, U2R, R2L and Probing. The

test comes about demonstrated that the algorithms utilized accomplished high identification rates (DR) and critical diminishment of false positives (FP) for various kinds of system intrusions utilizing restricted computational resources.

S. Dhivya et al. [3], in the present web-empowered world, the interchanges occurring over the system is strengthening at a vast rate. Not all interchanges are valid and malpractice can emerge anywhere, anytime. In the event that the ordinary movement is marginally changed to misdirect the intrusion location framework, at that point the customary frameworks won't not have the capacity to perceive the same successfully. Hence, a framework that could recognize and uncover the novel attacks has been proposed. Since any number of clients can utilize a page, keeping up the accessibility of the resources and dispensing them to the dynamic clients according to their need is exceptionally fundamental. The multithread idea is utilized to share the resources that every customer can utilize. Property Selection Algorithm is utilized as the element extraction algorithm in weka, to yield those important highlights relating to the client's demand and aides in accomplishing a more exact outcome. Memory productivity is gotten with the falling twofold pursuit tree. The examples are productively put away and consequently the look for the nearness of an attack is proficient adequately. An Intrusion Detection System which is memory productive and sufficiently compelling in identifying attacks and lessening the false positives is subsequently proposed.

Y. Gao et al. [4], in this paper, the authors have proposed a two-tier design to identify intrusions on network level. System conduct can be delegated abuse identification and abnormality recognition. According to their investigation they considered information packets of TCP/IP as their information. After, pre-handling the information by parameter filtering, they assemble a self-ruling model on preparing set utilizing various leveled agglomerative clustering. Further, information gets delegated customary activity example or intrusions utilizing KNN classification. This decreases cost overheads. Abuse recognition is directed utilizing MLP algorithm. Irregularity discovery is directed using Reinforcement algorithm where arrange operators gain from the earth and take choices in like manner. The TP rate of our design is 0.99 and false positive rate is 0.01. Along these lines, our design gives an abnormal state of security by giving high TP and low false positive rate. Furthermore, it additionally investigates the typical system designs and adapts incrementally (to fabricate self-ruling framework) to isolate ordinary information and threats.

I. Lee et al. [5], in this paper, authors have proposed a novel string looking algorithm and an Intrusion Detection System utilizing this algorithm. What's more, they have investigated few correct example searching algorithms and their similar examination as our background study. A dataset of five thousand records (a subset of KDD Cup dataset) with forty-one highlights is taken for assessing the adequacy of the proposed IDS. The comparing worldwide nucleotide arrangements of the considerable number of highlights of the dataset helped us to execute our IDS. In this paper, they have proposed an inventive string coordinating algorithm which helped us to outline an IDS. For this reason, they have utilized DNA encoding technique where every one of the highlights of each record are being converted into nucleotide sequence.

C. Science et al. [6], in this paper, authors have proposed a framework that could identify and uncover the novel attacks. Since any number of clients can utilize a page, keeping up the accessibility of the resources and designating them to the dynamic clients according to their need is extremely fundamental. The multithread idea is utilized to share the resources that every customer can utilize. Quality Selection Algorithm is utilized as the element extraction algorithm in weka, to yield those significant features pertaining to the client's demand and aides in accomplishing a more accurate result. Memory productivity is gotten by the falling paired inquiry tree. The examples are proficiently stored and thus the look for the nearness of an attack is refined adequately. An Intrusion Detection System which is memory proficient and sufficiently successful in identifying attacks and diminishing the false positives is in this manner proposed.

N. Sharma et al. [7], In this paper, the authors have proposed a system intrusion detection display in view of information mining innovation, which can distinguish known intrusion adequately and has a decent ability to perceive obscure information pattern which can't be detected effectively in conventional IDS. The paper for the most part does the accompanying work: by examining the intrusion profoundly, separate the properties which can reflect intrusion attributes adequately; combine misuse discovery, irregularity location and human intercession, build up run library in light of C.45 choice tree algorithm and utilize the ideal example coordinating to enhance discovery rate; the hosts are bunched to be IP aggregate in view of visit number by k implies clustering algorithm, the review information are partitioned into parts under the IP gathering's course, and the classifiers are developed by isolated review information individually, at that point the distinguished Data apply different rules as indicated by their own IP gathering, in this manner reduce false positives. The analyses demonstrated that the strategy is powerful to distinguish intrusion, for example, filtering what's more, Deny of Service.

N. Sheikh et al. [8], A Network Intrusion Detection System (NIDS) is a software application that screens the system or framework exercises for pernicious exercises and unapproved access to gadgets. The objective of designing NIDS is to ensure the information's secrecy and respectability. Creators venture concentrates on these issues with the assistance of Data Mining. The examination paper

incorporates the usage of various information mining algorithms including linear regression and K-Means Clustering to automatically produce the tenets for arrange network activities. A near investigation of these procedures to distinguish intrusions has likewise been made. To learn the patterns of the attacks, NSL-KDD dataset has been utilized.

Z. Yanbin et al. [9], the most intense issue for abuse identification strategy is its inability to distinguish new sorts of attacks. A superior identification technique, which utilizes another learning system, is proposed to take care of this issue. A Concept Hierarchy Generation for attack Labels (CHGL) applying pertinent component subset codes clustering, makes basic machine learning algorithms learn attack profiles on high idea levels. Furthermore, that will empower the framework to identify more attack cases. Exploratory outcomes demonstrate the upside of this new strategy. To recognize more attack cases including those having a place with new attack types with the assistance of an information arranged characterization, which yields a concept hierarchy. Trial comes about have demonstrated the change of the framework execution. Another favorable position of this strategy is that attack writes are naturally grouped by PC, not by human.

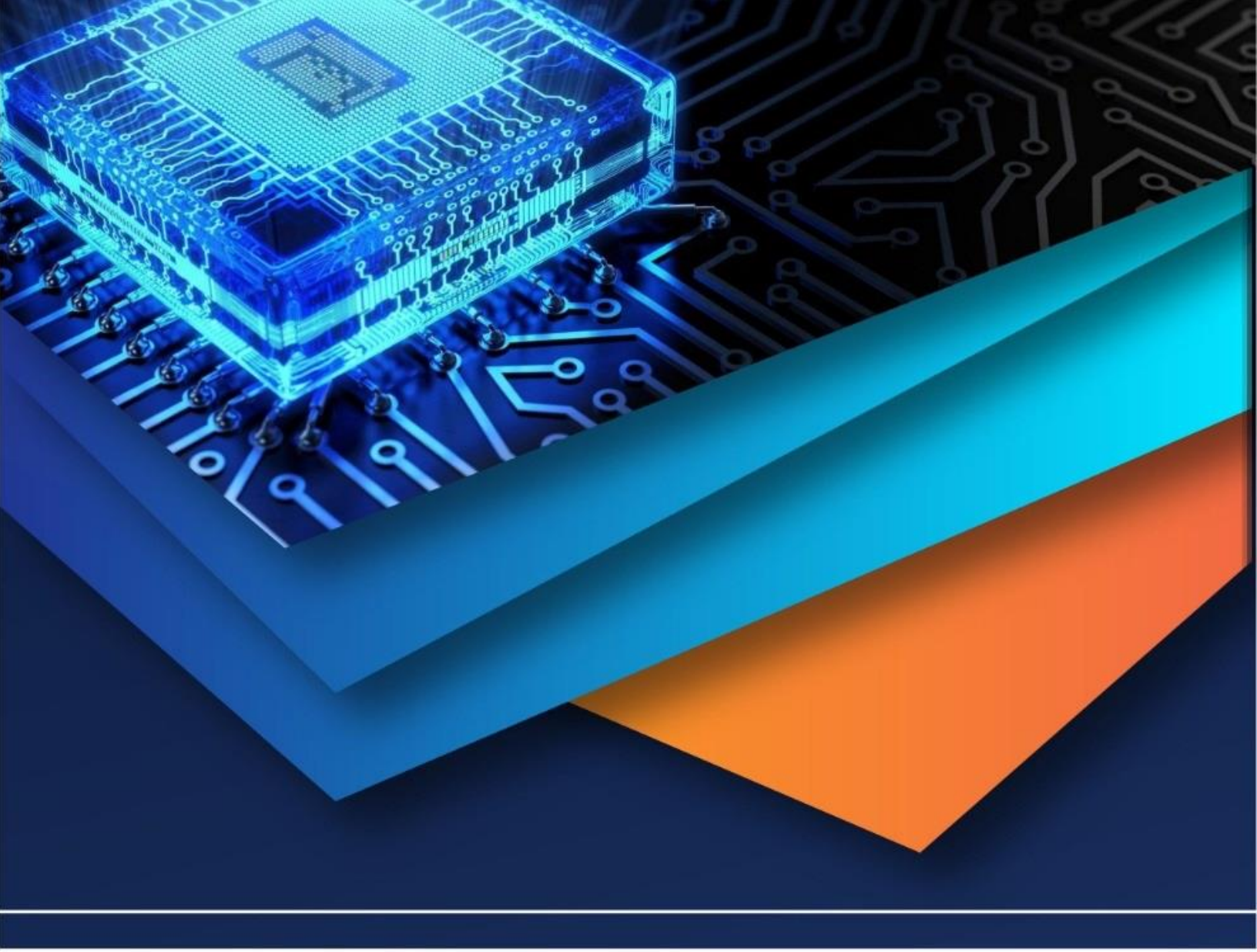
T. Zou et al. [10], Intrusion Detection Systems (IDS) assume an essential part in organize security. The fundamental test is the way to find occurrences of examples characterized in the administer set which portray the mark of malicious exercises. In this paper, authors proposed a productive correct example coordinating algorithm in light of the bit parallel approach. Exploratory outcomes demonstrate that our algorithm beats the conventional Aho-Corasick machine at the cost of few false positives. They demonstrated somewhat parallel separating algorithm for IDS. It runs speedier than the conventional Aho-Corasick automata. Despite the fact that it yields few false positive answers, it can be endured as we do customary articulation coordinating a short time later.

VIII.CONCLUSION

The developing danger of intrusion detection is devastating the networking group and different association. The paper has talked about and examined a portion of the best strategies as proposed by the different scientists in this field. This examination has truly helped in proposing in my own particular research work and turn out with something remarkable.

REFERENCES

[1]. M. E. L. Ajjouri, “New Model of Intrusion Detection Based On Multi Agent Systems and CBR Paradigm,” pp. 133–138, 2016.
[2]. L. M. L. de Campos, R. C. L. de Oliveira, and M. Roisenberg, “Network Intrusion Detection System Using Data Mining,” vol. 311, pp. 104–113, 2012.
[3]. S. Dhivya, D. Dhakchianandan, A. Gowtham, P. K. Sujatha, and A. Kannan, “Memory efficacious pattern matching intrusion detection system,” 2013 Int. Conf. Recent Trends Inf. Technol. ICRTIT 2013, pp. 652–656, 2013.
[4]. Y. Gao, J. Z. Huang, D. Gu, and H. Rong, “Learning Classifier System Ensemble for Data Mining,” Gecco’05, pp. 63–66, 2005.
[5]. Sung-Il Oh, Inbok Lee and Min Sik Kim, "Fast filtering for intrusion detection systems with the shift-or algorithm," 2012 18th Asia-Pacific Conference on Communications (APCC), Jeju Island, 2012 IEEE, pp. 869-870.
[6]. Divyatmika and M. Sreekesh, "A two-tier network based intrusion detection system architecture using machine learning approach," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016 IEEE, pp. 42-47.
[7]. N. Sharma and S. Mukherjee, “Layered approach for intrusion detection using naïve Bayes classifier,” Proc. Int. Conf. Adv. Comput. Commun. Informatics – ICACCI ’12, p. 639, 2012.
[8]. N. Sheikh, K. Mustafi and I. Mukhopadhyay, "A unique approach to design an intrusion detection system using an innovative string searching algorithm and DNA sequence," 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, 2016, pp. 1-9.
[9]. Z. Yanbin, “Network Intrusion Detection System Model Based On Artificial Immune,” vol. 9, no. 9, pp. 359–370, 2015.
[10]. T. Zou, Y. Cui, M. Huang, and C. Zhang, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176.
[11]. Ghorbani, AA, Lu, W, Travallaee, M, “Network Intrusion Detection and prevention Concepts and Techniques “Springer 2010, hardcover, ISBN:978-0-387-88770-8
[12]. Sharddha Surna “Intrusion Detection using Fuzzy Clustering and Artificial Neural Network”, Advances in Neural Networks, Fuzzy Systems and Artificial Intelligence, pp 209-217.
[13]. Y. Ke and J. M. Zhu, "Research of Hybrid Intrusion Detection and Prevention System for IPv6 Network," 2011 International Conference on Internet Technology and Applications, Wuhan, 2011, pp. 1-3.
[14]. Shaik Akbar, Dr.K.Nageswara Rao, Dr.J.A.Chandula “Intrusion Detection System Methodologies Based on Data Analysis”, international Jouranal of Computer Application (0975-8887) Volume 5-no.2, August 2010,” in Proc. Symp. Usable Privacy Security, 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY