iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VIII **Month of publication:** August 2019

DOI: http://doi.org/10.22214/ijraset.2019.8143

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: 7.177
Volume 7 Issue VIII, Aug 2019- Available at www.ijraset.com

A Brief Review on Intrusion Detection System with its Classification Types

Priyanka Tripathi[1], Rajni Ranjan Singh Makwana[2]
[1, 2]*Department of Computer Science and Information Technology, MITS Gwalior (M.P.) 474005, India*

Abstract: Under the Intrusion Detection System (IDS), monitoring the process of various events occurring in a computer system / network and also analyzing them for sign of possible incident which are violations of standard security policies. Here NIDS stands for Network based IDS which is one of the IDS types use to monitors and analyzes the data packets that travel over a network looking for such suspicious activities. In the paper, we represent an analysis of presently available types with their advantages, approaches of IDS, with its attacks on the users systems. In this paper, we also presented our study on various limitations associated with NIDS and also NIDS strengths to enhance the security.
Keywords: Data Mining, Intrusion Detection System, NIDS, HIDS, Spoofing

I. INTRODUCTION

People all over the world use the world wide web to such an extent that the Internet has become a crucial part in their lives. People use the Internet for many purposes such as involvement in social media, currency transactions, exchange of personal information and also storing private data such as passwords, personal media, banking details like credit card credentials. The world wide web has advanced to such an extent that it has developed from a set of markup language sites to a place where performing remote actions on a network from any where in the world is an easy task. Surveys show that network intrusion crimes have increased drastically over the years and lead to personal privacy theft. The data that is stolen as part of personal privacy theft is sold in black markets. Hence there is a need to develop an effective and efficient network intrusion detection system for detecting the type of attacks.[1]
IDS are defined as systems built to monitor and analyse network communication, as a result of monitoring, and hence detect anomalies and intrusions. Current IDS taxonomies focus on a single aspect of the IDS, such as the machine learning algorithms that researchers can potentially use, the characteristics of intrusion detection systems , or the features that should be used by researchers to design an IDS [2].
In general, IDSs contain three main components as depicted in Figure 1.

1) Firstly, there should be a data collection mechanism which tracing the network flows
2) Then, these data need to be used to identify the features, and a feature vector needs to be created.
3) Finally, with the use of this vector, a classification engine is executed, and the traced flow is identified either as normal or as an intrusion according to previous knowledge:

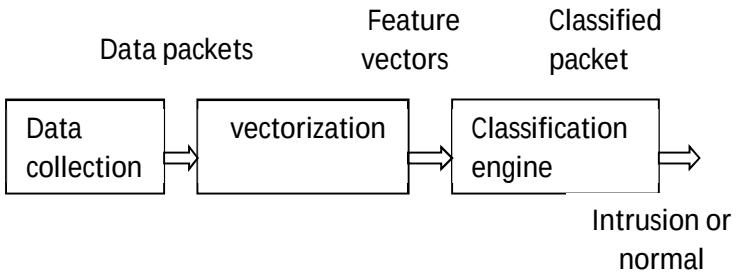


Figure: 1 Main Components of Intrusion Detection System

A. *Intrusion Detection System*

Intrusion: Cyber attack incidents are increasing with the increasing use of internet. Cyber attack is the virtual life of the bullying in normal life. In this attack person encounters such situations as harassment, threats and blackmail. The attack may be in the form of the capture of the persons' passwords or psychological pressure. Intrusion Detection System: Intrusion Detection Systems are very important software or hardware security tools to remove threats that would otherwise occur when carrying information, to prevent unauthorized access or abuse, and to report attacks to those responsible for security [3]. Attack Detection was first introduced in

Computer security threat monitoring and surveillance" survey published in 1980. The reasons for the need for intrusion detection systems; 1) It detects attacks that cannot be prevented by other security mechanisms. 2) It responds to the analysis phase before the attack occurs. 3) It allows attack analysis, system repair and the attacking factors to be corrected. Advantages of intrusion detection systems early detection, detailed information collection, evidence quality. The weaknesses of the intrusion detection systems are as follows; packet fragmentation and timing attacks, mixing of scan sequence, package hijacking. It is difficult to understand that packets arriving on the computer are sent for attack purposes. A packet arriving in the system may be sent for routine communication or an attack. Detecting an attack requires a difficult and intensive calculation. Intrusion detection systems are classified according to several different criteria. IDSs can be classified; the architectural structure, the type of system it protects, and the processing time of the data. According to their location there are two types of intrusion detection systems, Host-Based and Network Based. Also IDSs can be classified according to their techniques; Signature-Based and Anomaly-Based.

1) Host-Based IDS; server tries to detect attacks by listening to the traffic, registration files, and transactions.
2) Network-Based IDS; listening to all the traffic directed to the network, recording the content of each data packet passing through the network, cutting off attacks when necessary and creating reports.
3) Signature-Based IDS; is used to detect known attack types.
4) Anomaly-Based IDS; is used to detect unseen attacks.[3]

II. TYPES OF INTRUSION DETECTION SYSTEMS

There are many types of IDSs, few of them can be summarized as follows and Figure 3 shows the classification of IDS types based on platform that it deployed in it : .

A. Host Based IDS (HIDS)

HIDS was the first developed type of intrusion detection. HIDS monitors and analyzes the internal computing system or system level activities of single host such as: system configuration, application activity, wireless network traffic (only for that host) or network interface, system logs or audit log, running user or application processes, file access and modification.[4]

1) Advantages of Host based Intrusion Detection Systems
a) Verifies success or failure of an attack
b) Monitors System Activities
c) Detects attacks that a network based IDS fail to detect
d) Near real time detection and response
e) Does not require additional hardware
f) Lower entry cost
2) Drawbacks of Host based Intrusion Detection Systems
a) Difficult to analyze the intrusion attempts on multiple computers
b) It can be very difficult to maintain in large networks with different operating systems and configurations
c) It can be disabled by attackers after the system is compromised

B. Network Based IDS (NIDS)

NIDS is used to monitor and analyze network traffic on specific network segment for suspicious activities detection. NIDS used in packet level analysis for all systems in the network segment by check IP, transport-network and application protocol level activities and headers of packet to detect many IP-based DOS attacks like TCP SYN attack, fragment packet attack

1) Advantages of Network based Intrusion Detection Systems
a) Lower Cost of Ownership
b) Easier to deploy
c) Detect network based attacks
d) Retaining evidence
e) Real Time detection and quick response.
f) Detection of failed attacks
2) Disadvantages of Network based Intrusion Detection Systems
a) Cannot analyze encrypted packet
b) Requires access to all traffic to be monitored [5]

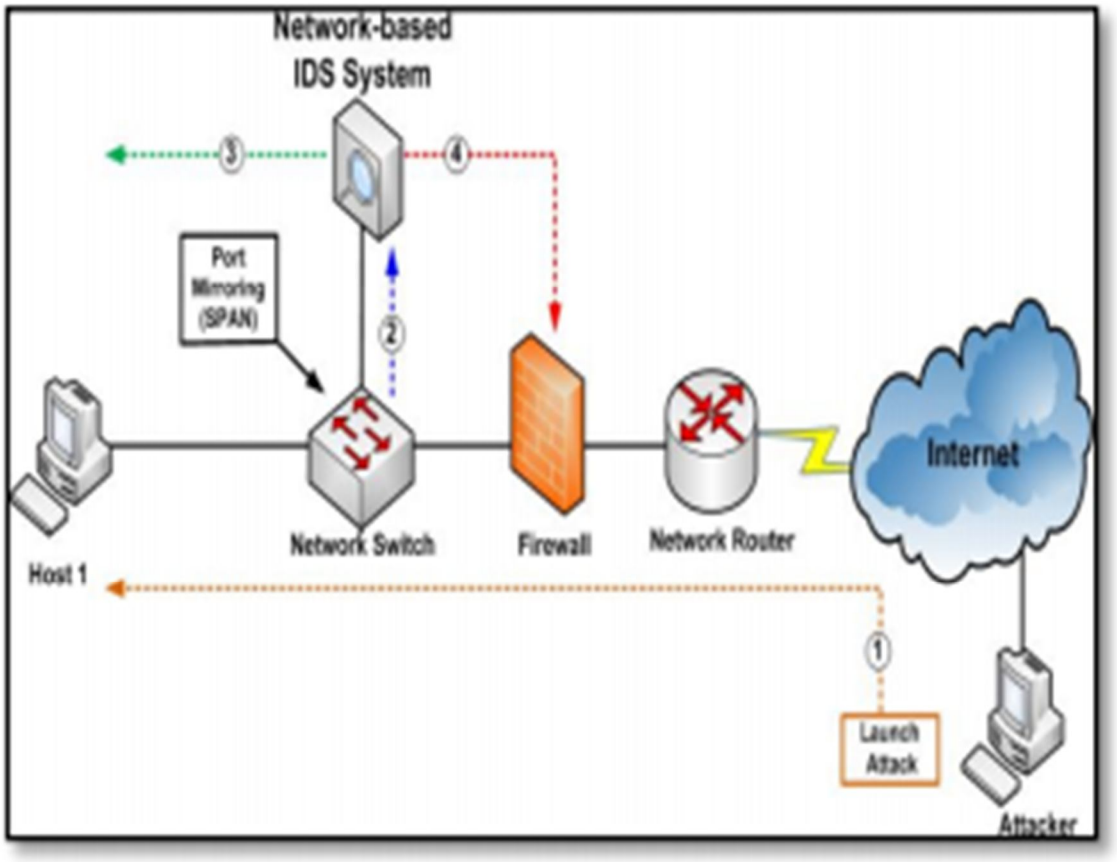


Figure 2: Network-based IDS

i) *Hybrid based IDS or mixed IDS (MIDS):* MIDS Combines two types or more of IDS to achieve the advantages of IDS and complete an accurate detection such as Double Guard that uses host ids and network IDS. However, MIDS takes a long time in analyzing data.

ii) *Protocol-based Intrusion Detection System (PIDS):* PIDS monitors and checks the specific protocol behavior and its state like Hyper Text Transfer Protocol (HTTP) . PIDS can be specialized to monitor application protocol, which is called APIDS . It focuses on actions that happen in some particular application through monitoring and analyzing the application log files or measuring their performance. [6]

iii) *Network Behavior Analysis (NBA):* NBA monitors and checks network traffic to know threats that produce uncommon traffic flows, such as DDOS attacks, malware, and policy violations. The NBA system investigates of network traffic to identify attacks with unexpected traffic flows.

iv) *Wireless IDS (WIDS):* WIDS monitors and analyses wireless traffic to detect any attacks. Wireless traffic is an ad-hoc network, wireless mesh network, and wireless sensor network. There are numerous types of attack in wireless network such as Sinkhole attack, Spoofed altered routing attack, Flood attack and Sybil attack.

v) *Database IDS:* Database IDS monitors and checks attacks toward database. There are several types of database attacks such as SQL injection attack, Direct DB Attack . Several researches addressed SQL injection attack, for instance: Liu A et al. proposed SQL Proxy-based Blocker. In the SQL Prob proposed method harnessed the Genetic Algorithms to dynamically detect and extract users entries for adverse SQL, and used a proxy that integrated with environment presenting protection to frontend web servers and back-end databases.[7]

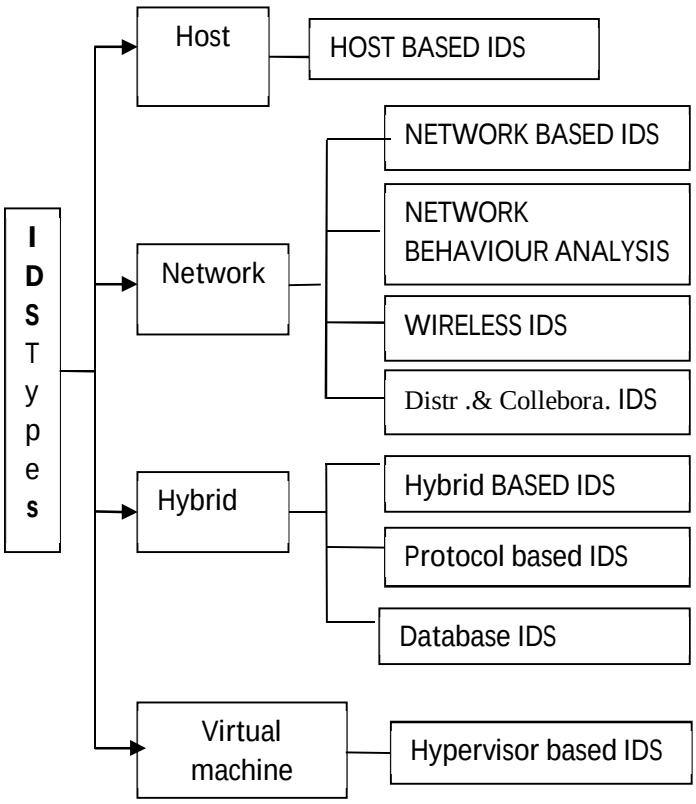


Figure 3: Classification of IDS types. [7]

III. INTRUSION DETECTION APPROACHES

In Intrusion Detection systems; techniques have been developed for modeling the data and create tables by classifying the modeled data . The most used of these techniques are:

1) *Statistical:* The first examples of systems are based on statistical measurements. Using these examples, a statistical model is created by examining user or system behavior. New intrusions are tried to be determined with the created statistical model. Some of the statistical methods used in intrusion detection are Principal Component Analysis, Chi-square distribution, Gaussian Mixture Distribution.
2) *Artificial Neural Networks:* models the given data using graphs of artificial neurons. They associate their vectors with their own algorithms and create new data. It is an approach used to examine and learn the behavior of data in the system [8]. With a enhanced form of ANN some authors prefer the use of Deep Learning for its efficiency
3) *Support Vector Machines:* It is the most preferred method for intrusion detection systems. Used for selection of feature vector. Supper Vector Machines aims to distinguish between data from two classes in a most appropriate way with a feature vector. They used in many classification problems such as face recognition systems, sound analysis.
4) *Data Mining:* it is known as reaching information among large-scale data. Used to extract rules by finding the relationship between data and users. Fuzzy Logic based on fuzzy set theory.
5) *Rule-Based Systems:* It is developed by people who specialize in a specific area. These people examine the system traffic and form rules and attack detection is done in this way.
6) *Fuzzy Logic:* It is based on thinking like human beings and it is aimed to process them by converting them into mathematical functions. [9].

IV. INTRUSION DETECTION ATTACKS

1) *Denial-of-Service (DOS) Attacks:* There are two main types of denial of service (DoS) attacks: flooding and flaw exploitations. Flooding attacks can often simply implement. For example, one can launch a DoS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. If the attacker has access to greater bandwidth than the victim, this will easily and quickly overwhelm the victim. As another example, a SYN flood attack sends a flood of TCP/SYN packets with a forged source address to a victim. This will cause the victim to open half open TCP connections - the

victim will send a TCPSYN/ACK packet and wait for an ACK in response. Since the ACK never comes, the victim eventually will exhaust available resources waiting for ACKs from a nonexistent host.

2) *Eavesdropping Attacks:* It is the scheme of interference in communication by the attacker. This attack can be done over by telephone lines or through email.
3) *Spoofing Attacks:* This attacker portrays as another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker.
4) *Intrusion attacks or User to Root Attack:* (U2R) An intruder tries to access the system or route through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle which leads to loss of data.
5) *Logon Abuse Attacks:* A logon abuse attack would neglect the authentication and access control mechanisms and grant a user with more advantages.
6) *Application-Level Attacks:* The attacker targets the disabilities of application layer. [10]

V. STRENGTHS OF NIDS

NIDS can perform the following functions to enhance the security.

A. Measurements and analysis of typical and atypical user behavior [Estan03]. For example an anomaly based NIDS is capable of detecting high volume traffic flows, flash crowds, load imbalance in the network, sudden changes in demand of a port usage, sudden surge of traffic from/to a specific host, etc.
B. Detection of known worms, viruses, and exploitation of a known security hole. Signature based NIDS can detect these events with fairly high degree of accuracy. An appropriate signature will also ensure a low false positive probability.
C. Some advanced NIDS systems also enable recognitions of patterns of system events that correspond to a known security threa.
D. Enforcement of the security policies in a given network. For example a NIDS can be configured to block all communication between certain sets of IP addresses and or ports. A NIDS can also be used to enforce network wide access controls.
E. Anomaly based NIDS can also recognize, with a certain false positive probability, new attacks and abnormal patterns in the network traffic, whose signatures are not yet generated. This will alert the network administrator early, and potentially reduce the damage caused by the new attack.[11]

VI. LIMITATIONS OF NIDS

1) *A mere Workaround:* A number of researchers have argued that a NIDS is more or a less a workaround for the flaws and weak or missing security mechanisms in an operating system, an application, and/or a protocol .
2) *False Positives:* NIDS comes with a bane, i.e. false positives. A false positive is an event when a NIDS falsely raises a security threat alarm for harmless traffic. Signatures can be tuned precisely to reduce such false positives, however fine signatures create a significant performance bottleneck, which is the next limitation of NIDS. Current Anomaly based algorithms lead to even higher false positives .
3) *Performance Issues:* Current signature based NIDS systems use regular expressions signatures which creates a significant performance bottleneck. In order to reduce false positives long signatures are required which further reduces the performance. The data throughput of current NIDS systems is limited to a few gigabit per second.
4) *Encryption:* The ultimate threat to the very existence of the signature based NIDS systems is the increasing use of data encryption. Everybody dreams to encrypt their data before transmission. Once the packet payloads are encrypted, the existing signatures will become completely useless in identifying the anomalous and harmful traffic .
5) *New and Sophisticated Attacks:* Commercial NIDS which are signature based are unable to detect new attacks whose signatures are not yet devised. Anomaly based NIDS can detect such attacks but due to the limitations of the current anomaly detection algorithms, an intelligent attacker can always develop attacks that remain undetected.
6) *Human Intervention*: Almost all NIDS systems require a constant human supervision, which slows down the detection and the associated actions. Some recent systems such as Network Intrusion Prevention Systems (NIPS) [Cisco] can automatically take pre-programmed actions but these are limited only to the well known attacks.
7) *Evasion of Signatures:* A number of researchers have argued that it is not difficult for an attacker to evade a signature [Varghese06]. Additionally there has been an increase in polymorphic worms which can automatically change their propagation characteristics thereby effectively changing their signatures. Such worms also pose a critical threat to the current NIDS.[11]

VII. LITERATURE REVIEW

Sydney mambwe kasongo et al. [12]introduced an IDS based on Deep Learning (DL) using Feed Forward Deep Neural Networks (FFDNN) coupled with a filter based feature selection algorithm. The FFDNN-IDS is evaluated using the well-known NSL-knowledge discovery and data mining (NSL-KDD) dataset and it is compared to the following existing machine learning methods: Support Vectors Machines (SVM), Decision Tree (DT), KNearest Neighbor (KNN) and Naïve Bayes (NB). The experimental results prove that the FFDNN-IDS achieves an increase in accuracy in comparison to other methods

Sana Ullah Jan et al. [13] developed a lightweight attack detection strategy utilizing a supervised machine learning–based support vector machine (SVM) to detect an adversary attempting to inject unnecessary data into the IoT network. Simulation results show that the proposed SVM-based classifier, aided by a combination of two or three incomplex features, can perform satisfactorily in terms of classification accuracy and detection time

Hiral Vegda et al. [14] this paper shows the secure and flexible implementation about to protect any ad hoc networks. This proposed system design is perfect solution to provide security with flexibility by providing a hybrid system which combines ECC and MAES to detect and prevent Ad hoc network attacks using Intrusion detection system. The complete proposed system designed on NS 2.35 software using Ubuntu (Linux) OS.

Souparnika Jayaprakash et al. [15] This paper proposed a transaction based approach based on naive Bayes classification and octraplet. In comparison with the previous data structures like Hexplet and triplet octraplet can offer more performance and improve detection rate. The Learning Algorithm can effectively detect role violations. Naive Bayes classifier is the simplest classification algorithm that can extract all information available in the log files. This system uses Naive Bayes Classifier which is a supervised Machine Learning method for Detecting anomalous queries. Proposed approach can improve the detection rates as well as performance of the system.

Pratik Satam et al. [16] this paper we present an anomaly-based intrusion detection system for Bluetooth networks; Bluetooth IDS (BIDS). The BIDS use an n-gram based approach to characterize the normal behavior of the Bluetooth protocol. Smoothing techniques like Jelinek-Mercer smoothing was used to improve the machine learning algorithm used for detecting abnormal Bluetooth operations. Machine learning algorithms like C4.5, AdaBoostM1, SVM, Naïve Bayes, RIPPER, Bagging were used to build the behavior models for the Bluetooth protocol.

VIII. CONCLUSION

In this survey paper, we describe about IDS as it is to provide an overview of the necessity as well as utility of the intrusion detection system. This paper gives brief study about types of IDS, various approaches, types of attacks . IDS are becoming essential for everyday security in the corporate world and also for network users. NIDS which is mainly for network based is one among IDS is discussed in this paper with its advantages, drawbacks, strengths and weaknesses. In conclusion, we can say that IDS is essential for various machine learning algorithms for enhancement of system security.

REFERENCES

[1] Suhair Hafez Amer and J Hamilton. 2010. Intrusion detection systems (IDS) taxonomy-a short review. Defense Cyber Security 13, 2 (2010), 23–30.
[2] Tarfa Hamed, Jason B Ernst, and Stefan C Kremer. 2018. A Survey and Taxonomy of Classifiers of Intrusion Detection Systems. In Computer and Network Security Essentials. Springer, 21–39
[3] Gozde Karatas, Onder Demir, Ozgur Koray Sahingoz, “Deep Learning in Intrusion Detection Systems” , International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism ,978-1-7281-0472-0/18/$31.00 ©2018 IEEE.
[4] Vokorokos, L. and A. Baláž. Host-based intrusion detection system. in Intelligent Engineering Systems (INES), 2010 14th International Conference on. 2010. IEEE.
[5] Jayesh Surana, Jagrati Sharma, Ishika Saraf, Nishima Puri, Bhavna Navin, “A Survey On Intrusion Detection System”, International Journal of Engineering Development and Research, © 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.
[6] Zuech, R., T.M. Khoshgoftaar, and R. Wald, Intrusion detection and big heterogeneous data: a survey. Journal of Big Data, 2015. 2(1): p. 3.
[7] Suad Mohammed Othman1 , Nabeel T.Alsohybe2 , Fadl Mutaher Ba-Alwi3 , Ammar Thabit Zahary, “Survey on Intrusion Detection System Types” , international Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 444-462 The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001.
[8] O. Can and O. K. Sahingoz, “An intrusion detection system based on neural network,” in 2015 23nd Signal Processing and Communications Applications Conference (SIU), May 2015, pp. 2302–2305.
[9] G. E. Hinton, P. Dayan, B. J. Frey, and R. M. Neal, “The” wakesleep” algorithm for unsupervised neural networks,” Science, vol. 268, no. 5214, pp. 1158–1161, 1995.
[10] Karthikeyan .K.R and A. Indra- “Intrusion Detection Tools and Techniques a Survey”.
[11] Sailesh Kumar, “Survey of Current Network Intrusion Detection Techniques”,

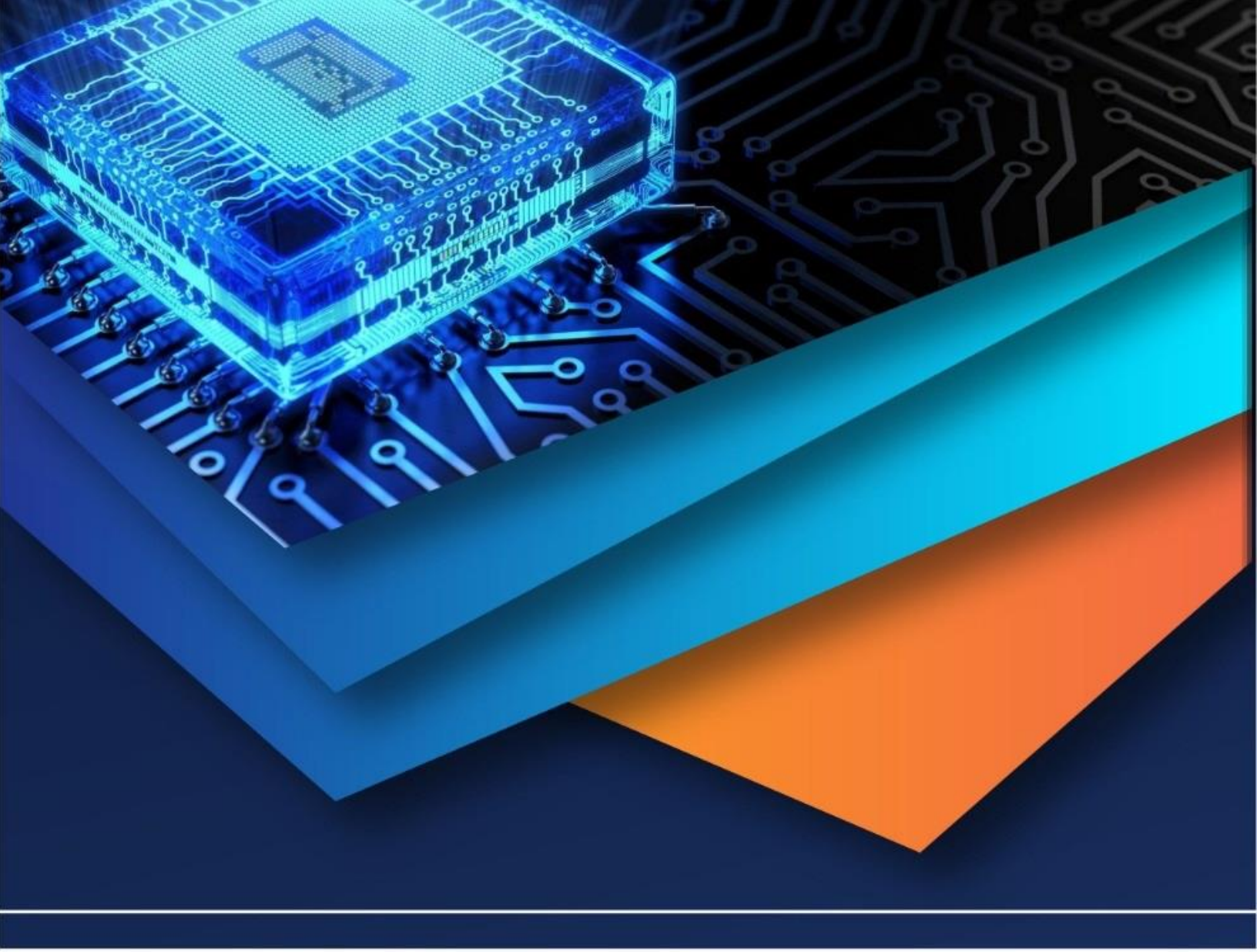
[12] SYDNEY MAMBWE KASONGO, YANXIA SUN, "A Deep Learning Method with Filter Based Feature Engineering for Wireless Intrusion Detection system" , 2169-3536 (c) 2018 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission, 10.1109/ACCESS.2019.DOI.

[13] SANA ULLAH JAN, SAEED AHMED, VLADIMIR SHAKHOV, AND INSOO KOO, "Towards a Lightweight Intrusion Detection System for the Internet of Things" , 2169-3536 (c) 2018 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission, 10.1109/ACCESS.2017.DOI

[14] Hiral Vegda, Dr. Nimesh Modi, "Secure and Efficient Approach to Prevent Ad hoc Network Attacks using Intrusion Detection System" , Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018) IEEE Xplore Compliant Part Number: CFP18K74-ART; ISBN:978-1-5386-2842-3.

[15] Souparnika Jayaprakash, Kamalanathan Kandasamy, "Database Intrusion Detection System Using Octraplet and Machine Learning", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018) IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2.

[16] Pratik Satam, Shalaka Satam, Salim Hariri, "Bluetooth Intrusion Detection System(BIDS)", 978-1-5386-9120-5/18/$31.00 ©2018 IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY