iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.40072

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: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

The Review of Artificial Intelligence in Cyber Security

Sivasankar G. A.
Department of Aeronautical Engineering, KIT-Kalaignarkarunanidhi Institute of Technology, Anna University, Coimbatore, Tamilnadu, India

Abstract: ***In today's world, cyber security and artificial intelligence (AI) are two growing technologies. AI is built on the foundation of machine learning (ML) models. Everywhere AI plays a significant role is in access control, user authentication and behaviour analysis, spam, malware, and botnet identification. On the contrary, today's security challenges are numerous. Cloud computing, social media, smart phones, and the widespread usage of numerous programmes such as WhatsApp and Viber have all posed significant security risks to users. This research looks at seven machine learning algorithms: MLP, LSTM, GRU, Decision Tree, SGD, KNN, and CNN. This study uses a two-step efficiency test called AI in Cyber Security. KDD'99 is used in the first step to train the models as well as for testing. Following the NSL-KDD data sets, train models go straight to testing. Following the examination of many cyber-attacks, the research continues on to deep analysis. The effectiveness of all seven AI models is examined, and the outcomes of cyber-attacks are discovered. All of the results have demonstrated the efficacy of using various AI models to perform cyber security.***

Keywords: Cyber Security, Artificial Intelligence (AI), Machine Learning (ML), KDD'99, NSL-KDD

I. INTRODUCTION

In today's world, cyber security and artificial intelligence (AI) are two growing technologies. Network and communication infrastructures, as well as human actors who interact with computer networks and communication infrastructures, are all covered under cyber security [1]. This is an interactive domain for global digital networks. The field of cyber security covers a vast array of risks and domains. Malware analysis, intrusion detection, web application security, social network security, and so on are just a few of them [2]. AI is characterised as a machine-driven decision-making process capable of approaching human intellect. Furthermore, statistical learning algorithms, which are at the heart of AI, are referred to as machine learning [3]. A two-step efficiency test of AI in the field of Cyber Security was undertaken in this study paper. A two-step efficiency test of AI in the field of Cyber Security was undertaken in this study paper. The KDD'99 data collection is used to train and test a total of seven AI models. The trained model is then tested on the NSL-KDD dataset in the second step. In the first step, AI models have an average accuracy of 96 percent. Furthermore, the efficiency rate in the second stage is 87 percent. Following that, a thorough investigation is carried out, with several AI models detecting multiple cyber-attacks such as DOS, R2L, U2R, and Probe. The application of artificial intelligence in cyber security is demonstrated by the modelling of artificial intelligence using seven machine learning methods, identification of normal and attack instances, and detection of numerous cyber-attacks.

A. Research Contributions

This paper helps in the following areas:

Multiple AI models are put into practise employing novel training and testing methodologies in a cutting-edge data analysis environment.

An in-depth examination of the performance of various AI models in detecting various sorts of cyber-attacks.

II. LITERATURE REVIEW

A. Overview

Though a lot of research works have already been reported and published were carried out using various machine learning and deep learning methods, however, nothing worth standing have been reported in the IDS field. The gap found in the field of IDS was studied with available resources till today. The unique idea of applying the machine learning methods in the IDS was also a new theme in the contemporary research arena.

B. Literature Review Regarding Dataset

The most significant challenge in assault identification framework is whether to produce genuine system traffic or to utilize the accessible benchmark datasets. There is criticism about the use of datasets acquired from genuine system traffic as it makes greater uncertainty and there is no such methodology that obviously discloses how to precisely separate between ordinary system traffic and attack traffic.[4].This is the explanation behind utilizing the benchmark datasets for executing different attack discovery framework of this paper. The available attack datasets[5][6][7][8]are DARPA 1998, KDD Cup99, NSL KDD, UNSW NB15, etc.The DARPA 1998, KDD Cup99, and NSL KDD consists of 42 attributes including the class label. The UNSW NB15 dataset consists of 48 attributes including the class label.

C. Review Regarding Detection

Multiple detection methods have been carried out in various literatures. It includes traditional detection, ML-based and DL Neural-network based detection. In few research hybrid method is also used.Various detection techniques are analyzed in the following discussion.

1) *Traditional Detection:* A sandbox, in computer security, is a security component wherein a different, confined condition is made and in which several functions are restricted. A sandbox is regularly utilized when untested code or entrusted programs from outsider sources are being utilized. Sandbox also has few constrain. Some sandbox apparatuses just deal with explicit sorts of PDF assaults like MD Scan for Java Script, [9],Nozzle for heap spraying[10],or it only records dynamic behavior of a system and still requires manual analysis to detect as in the case of CW Sandbox[11]. Huaibin Wang, HaiyunZhou, ChundongWanghas discussed about VM-based different IDSs[12].They have recommended to deploy VM-based numerous IDSs in each layer to observe specific virtual component. Additionally, they have also proposed the cloud alliance view, by the communication agents exchanging shared cautions commonly to withstand Denial of Service (DoS) and Distributed Denial-of-Service (DDoS). On this premise, they have accomplished an identity authentication of the communication agents, to improve the unwavering quality of the alarms. Through the evaluation of simulation results, the proposed device framework had a benefit for observing VMs on the detection.
2) *Artificial Intelligence (AI) Based Detection:* Machine learning algorithm learns from data[14]. Tom Mitchell precisely defines it as a computer program which learns from experience in respect to task and final outcome is the performance [15]. Vipin Kumar [16] used k mean clustering approach on NSLKDD dataset to perceive the accuracy for intrusion detection. Shilpaet.Al [17].used fundamental element evaluation on NSLKDD dataset for feature selection and dimension pruning approach for evaluation on anomaly detection. In general, network intrusion detection has been broadly improved by applying data mining and machine learning technique, which has largely utilized individual conduct patterns from the community site visitors' data. Support Vector Machine (SVM) is used, as a method in a study, to evaluate IDS [18].Among various approaches of IDS, SVM acts as a classifier with false alarm and detection rate as a measure of performance.Authors in a study [19]used Markov Chain implementation as classifier and Apriori algorithm to remove isolated data from the database and also used to judge the performance of NIDS. K-Means, an unsupervised algorithm, is used for classification, defines an unlabeled class to which the clustering is performed. Snort is the most popularly used software for network intrusion detection because of its numerous advantages[20]. Zhimin Zhang [21] surveys 54 papers published between 2016 to 2020 on the practical application of AI in the field of access authentication, network security, behavior anomalies and unusual traffic analysis. T.C Truong [22] theoretically reviewed AI in Cyber security and its validity in past, present and future. Priyanka Dixit [23] reviewed 80 papers from 2014 to 2019 related to Deep Learning algorithms for Cyber security applications. Sherali Zeadally [24] has tried to articulate a theoretical approach various Cyber security threats and AI techniques. Murat Kuzlu [25]has developed a review paper compiling topics regarding IOT, AI and Cyber Attacks. Thanh Cong (T.C) Truong [26] has written a survey paper on AI and its uses in Cyber security in offense and defense. SAGAR SAMTANI [27] has developed a theoretical approach for AI in Cyber security. Xianwei Gao [28] has propose an ensemble method of Machine Learning and shown that data features 15 an important factor for intrusion detection.

III. THEORETICAL STUDY REGARDING CYBER SECURITY & ARTIFICIAL INTELLIGENCE

A. Cyber Attack

Cyber Attack means to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber-attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

1) *Cyber-Attack lifecycle:* An attacker conducts exhaustive recce to find out the weak points of the network. The vulnerable points may be less secure computer, cell phones, any IOT device or even any network device like router, etc. The attacker exploits malicious codes or applications through those weak points by cyber engineering, phishing E-mail etc. Once the initial compromise is done, the attacker maintains control over that [29]. The attacker installs backdoor or downloads malware to the compromised system to establish permanent foothold. The attacker never leaves the environment rather he ensures continuous presence. Hence, attacker complete miss ion and continue silent presence until a new mission is directed.
2) *Types of Cyber attack*

a) *DOS:* Denial of service attack is an attack against an internet operated network where legitimate users are restricted to access information system devices or network resources. Example: Lock, Land, Neptune, pod, smurf, teardrop.
b) *R2L:* Remote to local attack (R2L) is launched by an attacker to gain unauthorized access to a victim machine in the entire network [31]. Example: ftp-write, guess-password, imap, multihop.
c) *U2R:* User to root attack (u2r) is usually launched for illegally obtaining the root's privileges when legally accessing a local machine [32]. Example: buffer-overflow, load module, perl, rootkit, ps, sqlattack, x term.
d) *Probe:* A probe is a program or other device inserted at a key juncture in a network for the purpose of monitoring or collecting data about network activity [33]. Example: ipsweep, nmap, portsweep, Satan.

B. *Cyber Defense*

Cyber Defense means the early prediction of adverserial cyber activity and to take measure to counter intrusions. It also refers to prevent, disrupt and counter cyber threats [34].

C. *Machine Learning*

Machine learning refers to processes and algorithms that generalize data and experiences from the past. It predicts probable future results in this process. Machine learning is therefore a set of mathematical techniques implemented on computer systems that allow information mining, pattern discovery, and data inferences to be drawn.

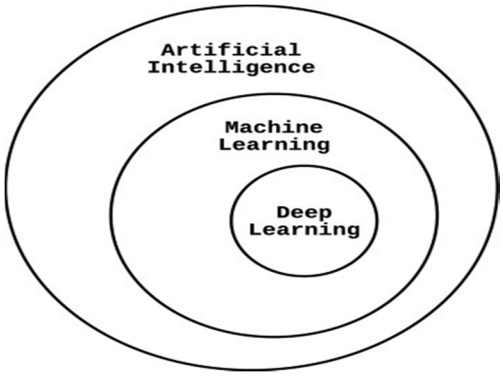


Fig.2. Artificial intelligence as it relates to machine learning and deep learning[35]

Artificial intelligence (AI)indicates algorithmic solutions to complex problems. Machine learning is a fundamental building block for AI. AI decision engine that are hardcoded into rule engines, and that would not be considered machine learning[36].

D. *MLP (Multi-Layer Perceptron)*

A feedforward artificial neural network called a multilayer perceptron (MLP) is a type of feedforward artificial neural network (ANN). The name MLP is ambiguous; it can be used to refer to any feedforward ANN, or it can refer to networks made up of many layers of perceptrons (with threshold activation) Multilayer perceptrons, especially those with a single hidden layer, are commonly referred to as "vanilla" neural networks.

There are at least three levels of nodes in an MLP: an input layer, a hidden layer, and an output layer. Each node, with the exception of the input nodes, is a neuron with a nonlinear activation function. Backpropagation is a supervised learning technique used by MLP during training. MLP is distinguished from a linear perceptron by its numerous layers and non-linear activation. It can tell the difference between data that isn't linear and data that isn't.

Weight is updated to minimize the error. Weight update equation is narrated below:
weight = weight + learning rate * (expected - predicted) * x[38].

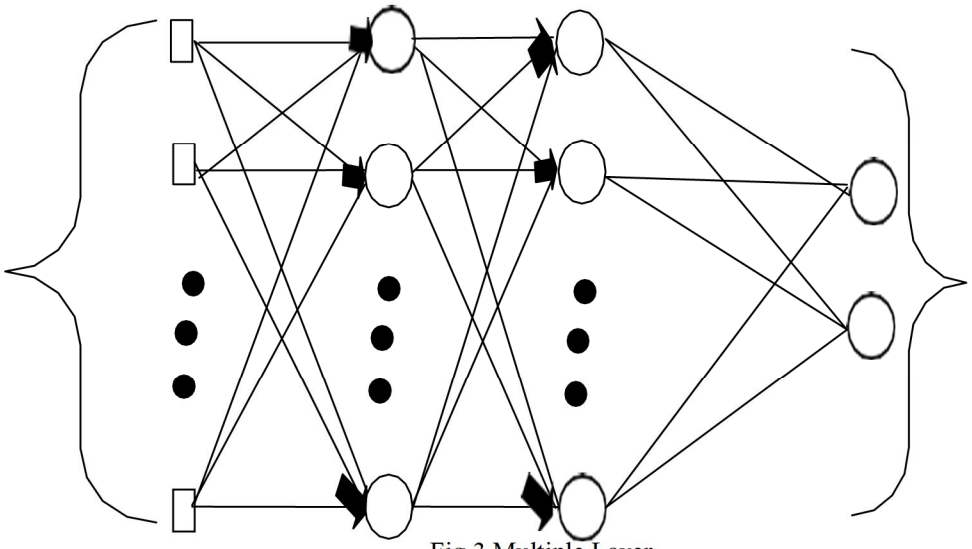


Fig 3 Multiple Layer

1) *LSTM:* Long Short-Term Memory (LSTM) networks are type of recurrent neural network. It is capable of learning order dependence is sequence prediction problem [40].
2) *GRU:* Gated Recurrent units (GRU) are a gating mechanism in recurrent neural networks. They are quite similar to LSTM because they also use gates to control the flow of information. It is comparatively newer technique introduced in the year of 2014 [41].
3) *CNN:* Convolution neural network (CNN) are specialized type neural network. It acts like traditional neural network, multiplication of a set of weights with the input [42].
4) *Decision Tree:* Decision tree is the algorithm which is used for classification or regression predictive modeling problem. To createthis model, it predicts the target variable value. It uses the tree presentation to solve the problem [43].
5) *KNN:* K-Nearest neighbor is a type of supervised machine learning algorithm. It can be used for both classification and regression predictive problems. It considers K Nearest Neighbors (Data points) to predict the class or new data points [44].
6) *SGD:* Stochastic Gradient Descent (SGD) is a quick and easy way to fit linear classifiers and regressors to convex loss functions like (linear) Support Vector Machines and Logistic Regression.

E. Survey Of Cyber Security Data SetKdd'99

The 1998 DARPA Data set was used as the basis to derive the KDD Cup 99 data set. The data set been used in Third International Knowledge Discovery and Data Mining Tools Competition (KDD.1999). Despite various limitations at present day cyber-attack scenario, it remains as a bench mark within cyber-attack research community.

1) *CAIDA:* This data collection was obtained in 2007 and contains network traffic traces from Distributed Denial-of-Service-Attacks. This data collection is missing features from the entire network, as well as diversity of attacks. As a result, it's impossible to tell the difference between typical and abnormal traffic flows.
2) *NSL-KDD:* This is the upper version of KDD'99 data set where the redundant records of KDD'99 are eliminated and updated to NSL-KDD.
3) *ISCX 2012:* From genuine HTTP, SMTP, SSH, IMAP, POP3, and FTP traffic, real network traffic traces were studied to discovernormal behavior for computers.
4) *ADFA-LD and ADRA-WD:* Researchers at the Australian Defense Force Academy developed two public data sets (ADRA-LD and ADFA-WD)that demonstrate the structure and technique of modern attacks.
5) *CICIDS 2017:* The CICIDS 2017 data set includes information on both benign behavior and emerging malware threats such as BruteForce FTP. SSH, DOS, Heart bleed, Web Attack, Infiltration, Botnet, and DDOS.

F. Data Analysis Platform

1) *Jupyter Notebook:* Python jupyter notebook is highly portable, contains a big library and has the capacity of analyzing big data. It alsohas the capability of advance analysis process through machine learning.
2) *Google Colab in Python:* Colab is a Python development environment that runs in the browser using Google cloud.
3) *Matlab:* Matlab provides interactive tools. These tools can perform a variety of machine learning task, including connecting to and importing data.
4) *WEKA:* Weka is a collection of machine learning algorithms for data mining tasks. It contains tools for data preparation, regression, clustering, classification, visualization and association rules mining.

IV. RESEARCH METHODOLOGY

A. Cyber Attack Data Set

Corrected. CSV of KDD'99 and KDD Test + .TXT of NSL-KDD has been used to perform the two-step suitability test. Noof instances and features are described below.

Table 1. Data Set Description

Ser	Class Name	Record No	No of Record as per Subclass
1.	Normal	64,954	
2.	DOS	2,29,855	Neptune-58,001Smart-1,64,091 Snmpget-7,741attack-back-1,098 process table-794pad-759 tear drop-12
3.	R2L	11,978	Guess-password-4,367 snmpguess-2,406 warezmaster-1,602 multihop-18 named-17 sendmail-17xclock-9 xsnoop-4 ftp-write-3 phf-02 Worm-02 imap-01
4.	U2R	70	httptunnel-158 buffer-Overflow-22 PS-16 rootkit-13xterm-13 pearl-02 loadmodule-02Sqlattack-02
5.	Probe	4,166	Saton-1,633 Mscan-1,053 saint-736 portsweop-354Ipsweop-306 Nmap-84
6.	Total	3,11,028	

Table 2. List of all 41 Features and list of selective 15 features

	41 Features
duration, protocol type, service, flag, src bytes, dst bytes, land, wrong fragment, urgent, hot, num failed logins, logged in, num compromised, root shell, su attempted, num root, rerror rate, srv rerror rate, same srv_rate,diff srv rate,	srv diff host rate, dst host count, dst host srvcount, dst host same srv rate, dst host diff srv rate, dst host same src port rate, dst host srv diff host rate, dst host serror rate, dst host srv serror rate, dst host rerror rate, dst host srv rerror rate num file creations, num shells, num access files, num outbound cmds, is host login, is guest login, count, srv count, serror rate, srv serror rate,

B. Data Set Preprocessing

Corrected.CSV of KDD'99 and KDD Test + .TXT of NSL-KDD have been used to perform the 1st step Efficiency test of AI in Cyber Security.Corrected.CSV of KDD'99 data set has been used while conducting the deep analysis part of this research. There are total forty-one features in this data set. The column forty-two signifies the exact type of attacks in that particular instance. Total 3.11, 028 instances are taken in this data set. In the initial coding total 37 types of attacks are grouped in major four types of attacks, DOS, R2L, U2R and Probe.

1) Conversion Of Data Set: Corrected Text Data Set of KDD'99 & KDD Test+. TXT of NSL-KDD has been converted to corrrected. CSV KDD.+CSV file type. Therefore the initial data preprocessing has been started.

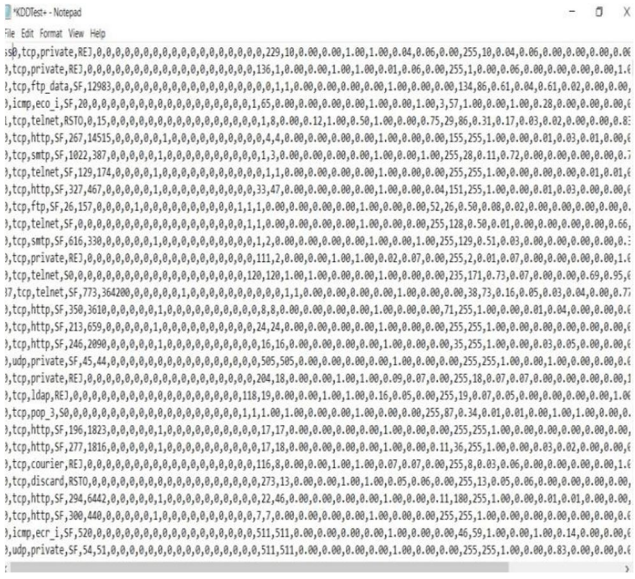


Fig.4.Data Set before Conversion

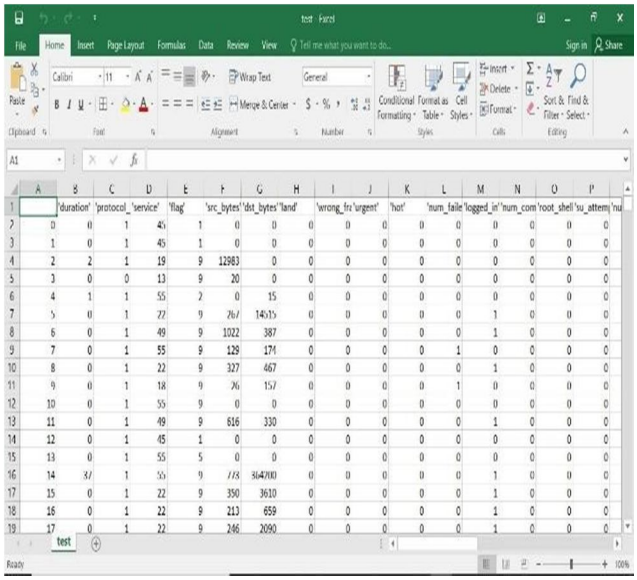
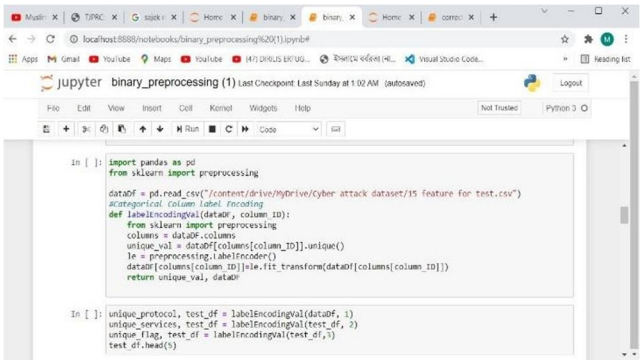
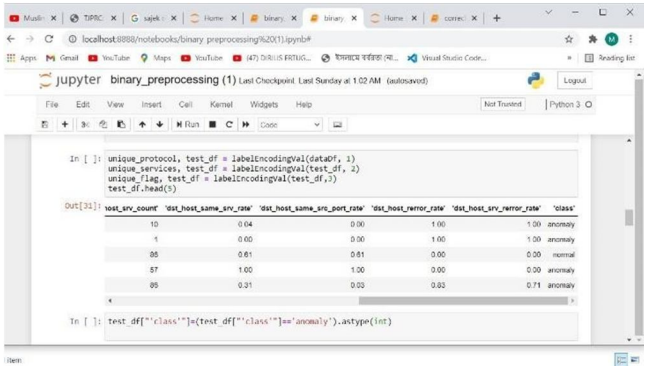


Fig.5. Data Set after Conversion

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

2) Label Encoding: While conducting the efficiency test normal instance are converted to zero and attack instances are converted to 1. Through label binarize and one hot encoding the main normal data and four types of attacks are converted to binary 0, 1, 2, 3, 4 in the deep analysis part of this research.Through label binarize, attacks are given the unique identificationFig.6.





V. RESULTS AND ANALYSIS

A. *Experimental Results and Analytical Review using all Features of KDD'99 Dataset*

Seven model is analyzed through KDD'99 data set**.** These are MLP, LSTM, GRU, CNN, Decision Tree, KNN, and SGD**.** Detection rate of attack and normal flow of data are found out in three separate segments**.** Firstly, accuracy, and then sensitivity and FPR**.** In this segment of analysis, all 41 features of dataset are utilized**.** Higher the accuracy and sensitivity and lower FPR makes the models very effective and efficient**.** Here all the model**'**s accuracy is more than 90**%** and sensitivity is more than 85**%** and also the FPR is less than 10**%** excluding the case of CNN and SGD and partially GRU**.** Therefore, the models are quite effective in detecting attacks and normal flow of data**.**The average accuracy and sensitivity results of AI models using 41 features, in the 1st step, are more than 90% which is a very effective result. Furthermore, the average result of FPR is almost less than 10% that makes the AI models efficient. Once the trained ML models are tested in a new dataset NSL-KDD, still ML models using 41 features provides good outputs, almost more than 85% and FPR is less than 15%. Therefore, in the anomaly detection AI models acts efficiently.

Table 5. Comparison among the Steps of Efficiency Test

S.no	Class Name	Average Accuracy %	Average Sensitivity%	Average FPR%
1.	AI Model using 41 Features of KDD'99	96%	93.44%	10.72%
2.	AI Model using 41 Features of NSL-KDD	87%	84.16%	14.21%

VI. CONCLUSION

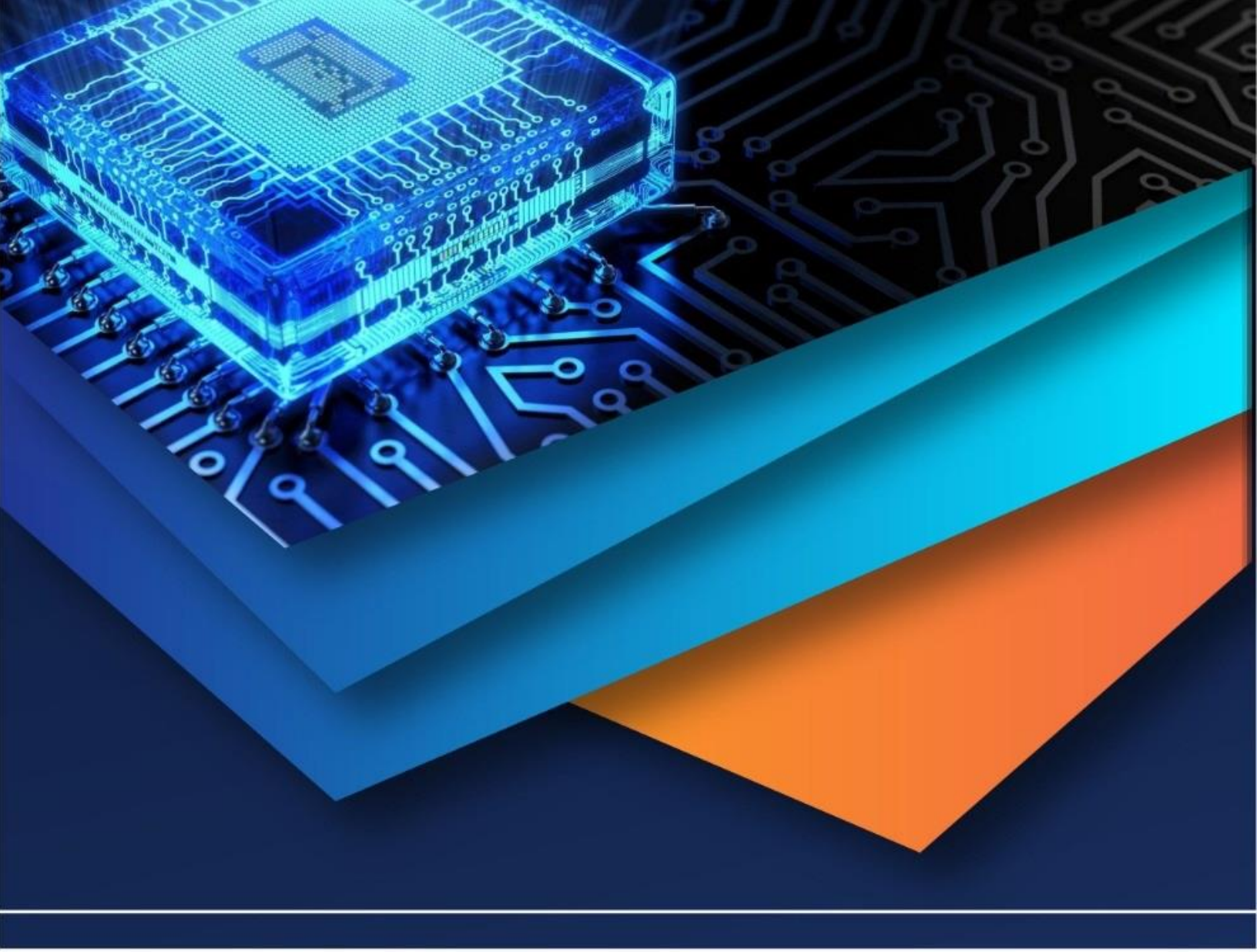
Every learning algorithm has its own merits and demerits. Total seven AI models analyzed in this study has brought versatility to the research. Most of the models performed effectively less SGD and more or less CNN. The AI model's suitability in cyber security was tested in two steps. Both the steps provided the AI model's prudency in cyber security. Use of two separate data sets, KDD'99 and NSL-KDD, in two steps and training and testing methodologies also brought uniqueness in the study. In addition, deep analysis through multiple cyber-attack detection by the AI models have further authenticate the credibility of AIin cyber security.

A true aggressive model is consisting of higher accuracy and sensitivity and lower FPR. In most cases, all AI models ensure this principle. Final average accuracy, sensitivity and FPR results are also the testimonies of suitability of AI in the field of cyber security. Hence, it is concluded saying. "AI based cyber security is the prudent and time-worthy solution."

The two-emerging technology, cyber security and AI, has been blended in this research work. Attackers always choose to attack the defender, by achieving surprise. Therefore, use of modern technology's the best arsenal to achieve surprise. Hence, it is expected to bring enormous success through this process of cyber defense.

REFERENCES

[1] Brij B. Gupta and Michael Sheng, "Machine Learning for Computer and Cyber Security," CRC Press. A Bio-inspired Approach to Cyber Security, P-75.
[2] Clarence Chio & David Freeman, "Machine Learning & Security," O'REILLY.P-1.
[3] https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/.Accessed on 01 August 2021.
[4] F. Iglesias, T. Zseby, Analysis of network traffic features for anomaly detection, Machine Learning 101 (1-3) (2015) 59–84. doi:10.1007/525 s10994-014-5473.
[5] N. Moustafa, J. Slay, The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set, Information Security Journal: A Global Perspective 25 (1-3) (2016) 18–31. doi:10.1080/19393555.2015.1125974.
[6] M. Tavallaee, E. Bagheri, W. Lu, A. A. Ghorbani, A detailed analysis of the kdd cup 99 data set, in: Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on, IEEE,2009, pp. 1–6. doi:10.1109/CISDA.2009.5356528.
[7] J. McHugh, testing intrusion detection systems: a critique of the 1998 535 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory, ACM Transactions on Information and System Security(TISSEC) 3 (4) (2000) 262–294. doi:10.1145/382912.382923.
[8] Z. Tzermias, G. Sykiotakis, M. Polychronakis, and E.P. Markatos, "Combining Static and Dynamic Analysis for the Detection of Malicious Documents," in Proceeding sof the fourth Workshop on European Workshop on System Security, (Salzburg,Austria), 2011.
[9] P.Ratanaworabhan, B.Livshits,andB.Zorn, "NOZZLE: A Defense Against Heap spraying Code Injection Attacks," inSSYM'09 Proceeding sof the 18th conference on USENIX security symposium, (Berkeley, CAUSA), 2009.
[10] C.Willems,T.Holz,andF.Freiling,"TowardAutomatedDynamic Malware Analysis Using CW Sandbox,"
[11] Huaibin Wang, Haiyun Zhou, ChundongWang "Virtual Machine-based Intrusion Detection System Framework in Cloud Computing Environment" JCP 2012 Vol.7(10): 2397-2403 ISSN: 1796-203Xdoi: 10.4304/jcp.7.10.2397-2403.
[12] Good fellow,Y.Bengio,andA. Courville, "Deep Learning," The MIT Press, 2016.
[13] T.Mitchell, "MachineLearning," McGrawHill,1997.
[14] VipinKumar, HimadriChauhan, DheerajPanwar, "K-Means Clustering Approach to Analyze NSL-KDD Intrusion Detection Dataset" International Journal of Soft Computing and Engineering (IJSCE)ISSN:2231-2307,Volume-3,Issue-4,September2013.
[15] Shilpalakhina, Sini Joseph and Bhupendraverma, "Feature Reduction using Principal Component Analysis for Effective Anomaly–Based Intrusion Detection on NSL-KDD", International Journal of Engineering Science and Technology, Vol.2(6),2010,1790-1799.
[16] MohammadpourL, HussainM, Aryanfar A, Raee VM, SattarF. "Evaluating performance of intrusion detection system using support vector machines," International Journal of Security and Its Applications. 2015 Sep;9(9):225−34. Cross ref
[17] BrindasriS, SaravananK. "Evaluation of network intrusion detection using Markov chain, "International Journal on Cybernetics and Informatics (IJCI).2014Apr;3(2):11−20.Crossref
[18] What is Snort? Date accessed:04/01/2018.https://www.snort.org/faq/what-is-snort.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY