CYBERTHREAT DETECTION BASED ON ARTIFICIAL NEURAL NETWROKS USING EVENT PROFILES

¹D.Sravani, ²Ch.Anusha, ³G.Sathvika, ⁴K.Pranathi, ⁵S.Varsha Reddy,

^{1,2,3,4}U.G.Scholor, Department of IT, Sri Indu College Of Engineering & Technology, Ibrahimpatnam, Hyderabad. ⁵Assistant Professor, Department of IT, Sri Indu College Of Engineering & Technology, Ibrahimpatnam, Hyderabad.

ABSTRACT

One of the major challenges in cyber security is the provision of an automated and effective cyber-threats detection technique. In this paper, we present an AI technique for cyber-threats detection, based on artificial neural networks. The proposed technique converts multitude of collected security events to individual event profiles and use a deep learning-based detection methodforenhancedcyber-threatdetection.For

this work, we developed an AI-SIEM system based on a combination of event profiling for data preprocessing and different artificial neural network methods, including FCNN, CNN, and LSTM. The system focuses on discriminating between true positive and false positive alerts, thus helpingsecurityanalysts to rapidlyrespond to cyber threats.

All experiments in this study are performed by authors using two benchmarkdatasets (NSLKDDandCICIDS2017)andtwodatasets

collected in the real world. To evaluate the performance comparison with existing methods, we conducted experiments using the five conventional machine-learning methods (SVM, k-NN, RF, NB, and DT). Consequently, the experimentalresultsofthisstudyensurethatour

proposed methods are capable of being employed as learning-based models for network intrusion- detection, and show that although it is employed in the real world, the performance outperforms the conventional machine-learning methods.

1. INTRODUCTION

Contrasted with the past, improvements in PC and correspondence innovations have given broad and propelled changes. The use of new innovations gives incredible advantages to people, organizations, and governments, be that as it may, messes some up against them. For instance, the protection of significant data, security of put away information stages, accessibility of information and so forth. Contingent upon these issues, digital fearbased oppression is one of the most significant issues in this day and age. Digital fear, which made a great deal of issues people and establishments, has arrived at a level that could undermine open and nation security by different gatherings, for example, criminal association, proficient people and digital activists. Alongthese lines, Intrusion Detection Systems (IDS) has been created to maintain a strategic distance from digital assaults. Right now, learning the bolster support vector machine (SVM) calculations wereutilized to recognize port sweep endeavors dependent on the new CICIDS2017 dataset with 97.80%, 69.79% precision rates were accomplished individually. Rather than SVMwe can introduce some other algorithms like random forest, CNN, ANN where these algorithms can acquire accuracies like SVM -93.29,CNN-63.52,RandomForest-99.93,

ANN-99.11.

MOTIVATION

The use of new innovations gives incredible people, organizations, advantages to and governments, be that as it may, messes some up against them. For instance, the protection of significant data, security of put away information stages, accessibility of information and so forth. Contingent upon these issues, digital fear-based oppression is one of the most significant issues in this day and age. Digital fear, which made a great deal of issues people and establishments, has arrived at a level that could undermine open and nation security by different gatherings, for example, criminal association, proficient people and digital activists. Along these lines, Intrusion Detection Systems (IDS) has been created to maintain a strategic distance from digital assaults.

OBJECTIVES

Objectiveofthisprojectistodetectcyber-attacks by using machine learning algorithms like

CNN:

A Convolutional Neural Network (CNN) is a type of deep learning neural network that is well-suited for image and video analysis.Random forest: It is the tech industry's definitive destination for sharing compelling, first-person accounts of problem- solving on the road to innovation.

ANN:

ANN algorithm accepts only numeric and structured data. Convolutional Neural Networks (CNN) and Recursive Neural Networks (RNN) are used to accept

unstructured and non-numeric data forms such as Image, Text, and Speech

OUTCOMES:

These predictions can be done by four algorithms like SVM, ANN, RF, CNN thispaper helps to identify which algorithm predicts the best accuracy rates which helps to predict best results to identify the cyber-attacks happened or not.

APPLICATIONS:

This strategy used in Detection of Cyber Attack inNetworkusingMachine LearningTechniques

2. LITERATURESURVEY

Literature Survey Intrusion detection is very important for network situation awareness. While a few methods have been proposed to detect network intrusion, they cannot directly and effectively utilize semi-quantitative information consisting of expert knowledge and quantitative data.

Hence, this paper proposes a new detection model based on a directed acyclic graph (DAG) and a belief rule base (BRB). In the proposed model,calledDAG-BRB,theDAGisemployed

toconstruct amulti-layeredBRBmodelthatcan avoid explosion of combinations of rule number because of a large number of types of intrusion. To obtain the optimal parameters of the DAG-BRB model, an improved constraint covariance matrix adaption evolution strategy (CMA-ES) is developed that can effectively solve the constraint problem in the BRB. A case study was used to test the efficiency of the proposed DAG-BRB.

The results showed that compared with other detection models, the DAG-BRB model has a higher detection rate and can be used in real network.

Nowadays, IT organizations generate colossal amounts of data. Handling these chunks of data itself is critical in the IT world. Hence centralizing the log management system improves security thereby enhances data protection in an organization. Such enterprises require a high profiling tool that helps in managing the information and events data to improve the level of security.

SecurityInformationandEventManagement (SIEM) :

It is a procedure for security analysis that prominence an overview of security in an organization.SIEMtoolscollect,analyze,

normalize and correlates all files and analyze data coming from the various device and give a centralized view of logs. This paper articulates an abstraction of SIEM tools and event correlation engines, furnishing a description of their technical comparative study, focusing on most popular SIEM tools and open source rule- based correlation engines and profiles them.

Distributed computing has become an effective approach to enhance capabilities of aninstitution or organization and minimize requirements for additional resource. In this regard, the distributed computing helps in broadening institutes IT capabilities. One needs to note that distributed computing is now integral part of most expanding IT business sector. It is considered novel and efficientmeans for expanding business. As more organizations and individuals start to use the cloud Literature Survey Intrusion detection is very important for network situation awareness. While a few methods have been proposed to detect network intrusion, they cannot directly and effectively utilize semi-quantitative information consisting of expert knowledge and quantitative data. Hence, this paper proposes a new detection model based on a directed acyclic graph (DAG) and a belief rule

base (BRB). In the proposed model, called DAG-BRB, theDAG is employed to construct a multi-layered BRB model that can avoid explosion of combinations of rule number because of a large number of types of intrusion.

To obtain the optimal parameters of the DAG-BRB model, an improved constraint covariance matrix adaption evolution strategy (CMA-ES) is developed that can effectively solve the constraint problem in the BRB. A case study was used to test the efficiency of the proposed DAG-BRB. The results showed that compared with other detection models, the DAG-BRB model has a higher detection rateand can be used in real network.

Nowadays, IT organizations generate colossal amountsofdata.Handlingthesechunksofdata

itself is critical in the IT world. Hence centralizing the log management system improves security thereby enhances data protection in an organization. Such enterprises require a high profiling tool that helps in managing the information and events data to improve the level of security. Security InformationandEventManagement(SIEM)isa procedure for security analysis that prominence an overview of security in an organization. SIEM tools collect. analvze. normalize and correlatesallfilesandanalyzedatacomingfrom the various device and give a centralized viewof logs.

This paper articulates an abstraction of SIEM tools and event correlation engines, furnishing a description of their technical comparative study, focusing on most popular SIEM tools and open source rule-based correlation engines and profiles them. Distributed computing has become an effective approach to enhance capabilities of an organization minimize institution or and requirements for additional resource. Inthisregard, the distributed computing helps in

broadening institutes IT capabilities. One needs to note that distributed computing is now integral part of most expanding IT business sector. It is considered novel and efficientmeans for expanding business. As more organizations and individuals start to use the cloud to store their data and applications, significant concerns have developed to protect sensitive data from external and internal attacks over internet.

Due to security concern many clients hesitate in relocating their sensitive data on the clouds, despite significant interest in cloud-based computing. Security is a significant issue, since data much of an organizations data provides a tempting target for hackers and those concerns will continue to diminish the development of distributed computing if not addressed. Therefore, this study presents a new test and insight into a honeypot.

It is a device that can be classified into two types:

Handling

1. researchhoneypots.

Handling honeypots are used to mitigate real life dangers:

A research honeypot is utilized as an exploration instrument to study and distinguish the dangers on the internet. Therefore, the primary aim of this research project is to do an intensive network security analysis through a virtualized honeypot for cloud servers to tempt an attacker and provide a new means of monitoring.

2. EXISTINGSYSTEM

EXISTINGAPPROACH:

Blameless Bayes and Principal Component Analysis (PCA) were been used with theKDD99 dataset by Almansob and Lomte. Similarly, PCA, SVM, and KDD99 were used Chithik and Rabbani for IDS. In Aljawarneh et Al's.Consequently, KDD99 is old and doesn't give any data about cutting edge new assault types, example, multi day misuses and so forth.

Drawbacks

- StrictRegulations
- Difficult to work with for non-technical users
- Restrictive to resources
- Constantlyneeds Patching
- Constantlybeing attacked

3. PROPOSEDSYSTEM

ProposedSystem

Important steps of the algorithm are given in below.

- Normalizationofeverydataset.
- Convert that dataset into the testing and training.
- Form IDS models with the help of using RF, ANN, CNN and SVM algorithms.
- Evaluateeverymodel'sperformance

ALGORIT HMS CNN:

AConvolutionalNeuralNetwork(CNN)isatypeof deeplearningneuralnetworkthatiswell-suitedfor imageandvideoanalysis.

Randomforest:

It is the tech industry's definitive destination for sharingcompelling,first-personaccountsofproblemsolvingontheroadtoinnovation.

ANN:

ANNalgorithmacceptsonlynumericandstructured data.ConvolutionalNeuralNetworks(CNN)and RecursiveNeuralNetworks(RNN)areusedtoaccept unstructuredandnon-numericdataformssuchas Image,Text,andSpeech

USECASEDIAGRAM

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Usecase analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The mainpurposeofausecasediagramistoshow what system functions are performed for which actor. Roles of the actors in the system can be depicted.

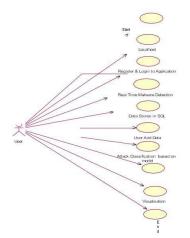


Fig4.1:UseCaseDiagram

CLASSDIAGRAM

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

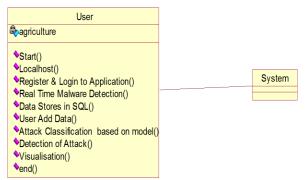


Fig4.2:ClassDiagram

SEQUENCEDIAGRAM

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a constructof a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

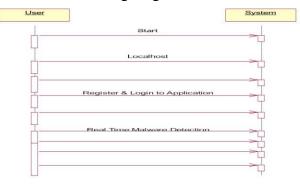


Fig4.3:Sequence Diagram

IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501

Vol.15, Issue No 1, 2025

4 RESULTS

	andas <mark>as</mark> p atplotlib lib inline	pyplot	as pl	t									
nport s nport p nport s nport s rom sta	tertools eaborn as andas_pro tatsmodels tsmodels. sy import	filing s.formu stats.o	utlier			iport va	riance_i	nflation_	facto	r			
ecated.	al/lib/py Use the pandas.u	functio	ns in	the pu						FutureWar	ning: pand	us.util.test	ing is dep
ron skl nport s ron skl ron skl ron skl	earn impo earn.feati klearn.met earn.svm : earn.linea earn.feati earn.feati	ure_sel trics a inport ar_mode ure_sel	ection s metr SVC l inpo ection	rics rt Log inpor	isticReq t Select	tKBest		al_info_c	lassi	f			
	l.read_csv read_csv(
cot-pu.	1600_6341	/ conce	int/ur1			-							
				1	'1g	/.	l:Ir	npu	tL	Jata	l		
: colu	nns=["dura	tion",'	protoc	ol_typ	e","serv	vice","f	lag","sri	t_bytes","	dst_b	iytes", "la	nd",		
: colu "wroi	nns=["dura ng_fragnen	tion",' t","urg	protoc ent","	ol_typ 'hot',"	e","serv num_fail	vice","f led_logi	lag","sri ns","log	t_bytes"," jed_in", "num_file	dst_b	iytes","la	nd",		
"wroi "nun	ng_fragmen compromis	t","urg ed","ro	ient"," iot she	'hot"," ell","s	num_fail u attemp	led_logi oted","n	ns","log um root"	ged_in", "num file	crea	vtes","la itions",	nd",		
"wron "nun "nun "is o	ng_fragmen compromis shells"," puest logi	t" "urg ed", "ro num acc n" "cou	ent" " ot_she ess_fi nt" "s	'hot" " ell" "s eles" " erv cou	num_fail u_attemp num_outb nt","ser	led_logi oted","n ound_cm rror_rat	ns","log um root" ds","is e", "srv	ged_in", "num_file host_login serror_ra	crea	itions",		host count"	."dst host :
"wroi "num "num "is_i "reri "dst	ng_fragnen _compronis _shells"," puest_logi ror_rate", _host_diff	t","urg ed","ro num_acc n","cou "srv_re _srv_ra	ent"," ot_she ess_fi nt","s rror_r rte","d	'hot", " ill", "s iles", " irv_cou rate", " ist_hos	num_fail u_attemp num_outb nt","ser same_srv t_same_s	led_logi oted","n wound_cm ror_rat rate", arc_port	ns","log um root" ds","is e", "srv "diff si rate",	ged_in", "num_file host_login serror_ra rv_rate","	_crea ", te", srv_d	itions", liff_host_	rate","dst	host_count"	,"dst_host_:
"wro "num "is "rer "dst "dst	ng_fragmen compromis shells"," guest logi ror rate", host diff host srv	t" "urg ed", "ro num acc n" "cou "srv_re srv_ra diff ho	ent"," iot she iess fi int","s irror r ite","d ist rat	hot" " ll" "s les" " rv_cou ate" " ist_hos re" "ds	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s	ed logi oted","n oound cm ror_rat ror_rate", orc_port cerror_r	ns","log um root" ds","is e", "srv "diff_si rate", ate","dsi	ged_in", ,"num_file host_login _serror_ra rv_rate"," t host_srv	crea ", te", srv_d serr	itions", liff_host_ or rate",	rate","dst	host_count"	,"dst_host_
"wro "num "is "rer "dst "dst	ng_fragnen _compronis _shells"," puest_logi ror_rate", _host_diff	t" "urg ed", "ro num acc n" "cou "srv_re srv_ra diff ho	ent"," iot she iess fi int","s irror r ite","d ist rat	hot" " ll" "s les" " rv_cou ate" " ist_hos re" "ds	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s	ed logi oted","n oound cm ror_rat ror_rate", orc_port cerror_r	ns","log um root" ds","is e", "srv "diff_si rate", ate","dsi	ged_in", ,"num_file host_login _serror_ra rv_rate"," t host_srv	crea ", te", srv_d serr	itions", liff_host_ or rate",	rate","dst	host_count"	,"dst_host_
"wroi "nun "nun "is_i "dst "dst "dst	ng fragmen compromis shells"," juest logi ror rate", host diff host srv host rerr	t", "urg ed", "ro nun acc n", "cou "srv re srv ra diff ho or rate	ent"," iot_she iess_fi int","s irror_r ite","d ist_rat ist_rat	hot" " ll" "s les" " rv_cou ate" " ist_hos re" "ds	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s	ed logi oted","n oound cm ror_rat ror_rate", orc_port cerror_r	ns","log um root" ds","is e", "srv "diff_si rate", ate","dsi	ged_in", ,"num_file host_login _serror_ra rv_rate"," t host_srv	crea ", te", srv_d serr	itions", liff_host_ or rate",	rate","dst	host_count*	,"dst_host_
"wroi "num "num "is_i "dst "dst () : trai	ng_fragmen compromis shells"," guest logi ror rate", host diff host srv	t", "urg ed", "ro num_acc n", "cou "srv_re srv_ra diff_ho or_rate columns	ent"," iot_she iess_fi int","s irror_r ite","d ist_rat ist_rat	hot" " ll" "s les" " rv_cou ate" " ist_hos re" "ds	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s	ed logi oted","n oound cm ror_rat ror_rate", orc_port cerror_r	ns","log um root" ds","is e", "srv "diff_si rate", ate","dsi	ged_in", ,"num_file host_login _serror_ra rv_rate"," t host_srv	crea ", te", srv_d serr	itions", liff_host_ or rate",	rate","dst	host_count"	,"dst_host_s
"wroi "num "num "is_i "rern "dst "dst "dst : train test	ng fragmen compromis shells"," uuest logi ror rate", host diff host srv_ host rerr n.columns=c	t", "urg ed", "ro num_acc n", "cou "srv_re srv_ra diff_ho or_rate columns	ent"," iot_she iess_fi int","s irror_r ite","d ist_rat ist_rat	hot" " ll" "s les" " rv_cou ate" " ist_hos re" "ds	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s	ed logi oted","n oound cm ror_rat ror_rate", orc_port cerror_r	ns","log um root" ds","is e", "srv "diff_si rate", ate","dsi	ged_in", ,"num_file host_login _serror_ra rv_rate"," t host_srv	crea ", te", srv_d serr	itions", liff_host_ or rate",	rate","dst	host_count*	"dst_host_s
"wroi "num "num "is_i "reri "dst "dst "dst : train test : train	ng_fragmen compromis shells"," juest logi ror_rate", host diff host srv_ host rerr n.columns= .columns=c n.head()	t", "urg ed", "ro num acc n", "cou "srv_re srv_ra diff_ho or_rate columns	ent"," iot_she inst","s intor_r intor into	hot"," ill","s les"," arv_cou rate"," ist_hos e","ds host_	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_same_s t_bost_s srv_rerr	ed_logi nted", "n nound_cm rror_rat /_rate", src_port serror_r ror_rate	ns","log um_root" ds","is_l e", "srv "diff_si rate", ate","dsi ","attacl	ged_in", "num_file lost_login serror_ra rv_rate"," t_host_srv t_host_srv	crea ", te", srv_d flag"	tions", liff_host_ or_rate",]	rate","dst		
<pre>'wror 'num 'num 'num 'bs' 'rern 'dst 'dst 'dst ' 'cst ' 'cst ' 'cs' '' '' '' '' ''' ''''''''''</pre>	ng_fragnen compromis shells"," juest logi ror_rate", host diff host_srv_ host_srv_ n.columns=c n.head() uration proto	t", "urg ed", "ro nun acc n", "cou "srv_re srv_ra diff_ho columns columns	ent", " iot she iess fi int", 's irror r ite", "d ist rat ", "dst service	hot", " ill", "s les", " rry_cou rry_cou rate", " ist_hos ist_hos ist_hos t_host	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s srv_rerr	led_logi oted", "n cound_cm ror_rate rrate", src_port serror_r or_rate	ns","logg um_root", ds","is_l e", "srv "diff_su _rate", "ds" ","attacl ","attacl	ged_in", "num_file lost_login serror_ra rv_rate"," t_host_srv t_host_srv t_host_srv t_host_srv	crea ", te", srv_d serr flag"	tions", liff_host_ or_rate",] hot_num_fa	rate", "dst	iged_in_num_co	mpromised roo
<pre>"wror "num" "num" "num" "dst "dst" "dst" "dst" "dst" "dst" "dst" "dst" " " " " " " " " " " " " " " " " " "</pre>	ng_fragmen comprohis shells"," juest_logi rogr rate", host diff host_srv_ host_rerr n.columns=c n.head() uration proto	t", "urg ed", "ro nun acco ", "cou "srv_re srv_rs srv_rs srv_rate diff ho diff ho columns olumns	ent"," iot_she iess_fi int","s irror_r ite","d st_rat service other	hot", " ill", "s irv_cou ist_hos ist_hos ist_hos ist_hos ist_host_ s sF	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s srv_rerr c_bytes_d 146	ied_logi ted", "n ound_cm rror_rat r_rate", isrc_port ierror_r ror_rate	ns","logg um_root" ds","is_l e", "srv "diff_si rate","dsi ","attacl ate","dsi ","attacl	jed_in", "num file host_togin serror ra rv_rate", t host_srv t host_srv *, "last_ <u>p</u> fragment_u 0	crea ", te", srv_d _serr flag" rgent 0	tions", liff_host_ or_rate",] hot_num_fa	rate", "öst iled_logins log 0	iged_in_mum_co 0	mpromised ro
"wron" "num" "num" "s_j"ren "dst "dst "dst "dst : train test : train 0 1	ng_fragmen comprohis shells"," juest logi, host diff host srv_ host diff host srv_ host rerr n.columns=c n.head() uration proto 0	t", "urg ed", "ro nun acc "srv_re srv_re srv_rate diff_hh or_rate columns columns columns	ent", " iot_she iess_fii int", 's irror_r ite", "d ist_rat ", "dst service other private	hot"," ill","s irv_cou ate"," ist_hos ist_hos ist_host ist_host s s S S S 0	num_fail u_attemp num_outb nt","ser same_srv t_same_s t_host_s t_h	ied_logi ted", "n ror_rat rror_rate", rrc_port ierror_rate ist_bytes 0 0	ns","logi um root" ds", "is l e", "srv "diff si "ate", "dsf ","attacl ","attacl	jed_in", "num file tost_togin serror ra rv_rate"," t host srvv t host srvv t, "last_ 0 0	crea ", te", srv_d serr flag" rgent 0	itions", liff_host_ or_rate",] hot_num_fa 0 0	rate", "dst iled_logins_log 0 0	ged_in_num_co 0 0	mpromised ro 0 0
"wror" "num" "num" "is_i "rer" "dst "dst" "dst i test : train test : train 0 1 2	ng fragmen compronis shells", juest logi ror_rate", host diff host_srv_ host_srv_ host_srv_ n.columns= columns=columns=columns=columns=columns= n.head() uration proto 0 0	t", "urg ed", "ro nun acco "srv_re srv_re srv_ra diff_ho or_rate columns columns columns utp ttp	ent"," iot_she iess_fi int",'s rror_r ite",'d ist_rat st_rat ist_rat service other private http	hot", " ill", "s les", " rry_cou ate", " st_hos ist_hos ist_host_ s s SF so SF	num_fail u_attemp num_outb nt","ser same_srv t_same_st t_host_s srv_rerr 146 0 232	ed_logi ted", "n ror_rat rrar_rate", rcc_port isr.bytes 0 0 8153	ns", *log um root* ef, srnv "diff si ate", "srnv "diff si ste", "ds ate", "d	jed_in", "num file tost_Togin serror rate"," t host srv t host srv t, "last pfragment u 0 0	crea ", te", srv_d _serr flag" rgent 0 0	itions", iff_host_ or_rate",] hot_num_fa 0 0 0	rate", "dst lied_logins_log 0 0 0	ged_in_mum_co 0 0	mpromised roo 0 0 0
"wror" "num,"num, "isj"rer "dst" dst" dst test test train test tast 1 2 3	ng fragmen compromis shells", juest logi ror_rate", host diff host_rrv_ host_rrv n.columns=c n.head() uration proto 0 0 0	t", "urg ed", "ro num acco ", "count "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns up tp tp	ent"," iot_she iess_fi int","s rror r te","d ist_rat ","dst service other private http http	hot"," iles"," irv_cou rate"," ist_hos ist_hos ist_hos ist_hos ist_hos se"," ds ist_hos se"," sf SF SF	num_fail u_attemp num_outh nt","ser same_srv t_same_sr t_same_sr t_same_sr t_same_sr t_host_s srv_rerr c_bytes d 146 0 232 199	ied_logi ted", "n ror_rat rror_rate", rrc_port ierror_rate ist_bytes 0	ns","logi um root" ds", "is l e", "srv "diff si "ate", "dsf ","attacl ","attacl	jed_in", "num file tost_togin serror ra rv_rate"," t host srvv t host srvv t, "last_ 0 0	crea ", te", srv_d serr flag" rgent 0	tions", iiff_host_] hot_num_ta 0 0 0 0	rate", "dst	ged_in_num_co 0 1 1	mpromised roo 0 0 0
"wror" "num" "num" "is_i "rer" "dst "dst" "dst i test : train test : train 0 1 2	ng fragmen compronis shells", juest logi ror_rate", host diff host_srv_ host_srv_ host_srv_ n.columns= columns=columns=columns=columns=columns= n.head() uration proto 0 0	t", "urg ed", "ro num acco ", "count "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns up tp tp	ent"," iot_she iess_fi int",'s rror_r ite",'d ist_rat st_rat ist_rat service other private http	hot"," iles"," irv_cou rate"," ist_hos ist_hos ist_hos ist_hos ist_hos se"," ds ist_hos se"," sf SF SF	num_fail u_attemp num_outb nt","ser same_srv t_same_st t_host_s srv_rerr 146 0 232	ed_logi ted", "n ror_rat rrar_rate", rcc_port isr.bytes 0 0 8153	ns", *log um root* ef, srnv "diff si ate", "srnv "diff si ste", "ds ate", "d	jed_in", "num file tost_Togin serror rate"," t host srv t host srv t, "last pfragment u 0 0	crea ", te", srv_d _serr flag" rgent 0 0	itions", iff_host_ or_rate",] hot_num_fa 0 0 0	rate", "dst lied_logins_log 0 0 0	ged_in_mum_co 0 0	mpromised roo 0 0 0
"wror" "num,"num, "isj"rer "dst" dst" dst test test train test tast 1 2 3	ng fragmen compromis shells", juest logi ror_rate", host diff host_rrv_ host_rrv n.columns=c n.head() uration proto 0 0 0	t", "urg ed", "ro num acco ", "count "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns up tp tp	ent"," iot_she iess_fi int","s rror r te","d ist_rat ","dst service other private http http	hot"," iles"," irv_cou rate"," ist_hos ist_hos ist_hos ist_hos ist_hos se"," ds ist_hos se"," sf SF SF	num_fail u_attemp num_outh nt","ser same_srv t_same_sr t_same_sr t_same_sr t_same_sr t_host_s srv_rerr c_bytes d 146 0 232 199	ed_logi ted", "n ror_rat rrar_rate", rcc_port isr.bytes 0 0 8153	ns", *log um root* ef, srnv "diff si ate", "srnv "diff si ste", "ds ate", "d	jed_in", "num file tost_Togin serror rate"," t host srv t host srv t, "last pfragment u 0 0	crea ", te", srv_d _serr flag" rgent 0 0	tions", iiff_host_] hot_num_ta 0 0 0 0	rate", "dst	ged_in_num_co 0 1 1	mpromised roo 0 0 0
"wror" "num,"num, "isj"rer "dst" dst" dst test test train test tast 1 2 3	Ig_fragmer comprovis puest_logi puest_logi host_srv_ host_srv_ host_rerr n. head() 0 0 0 0 0 0	t", "urg ed", "ro num acco ", "count "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns up tp tp	ent", " iot_she tess_fi_ts rror r rtet, "d st_rat st_rat service other phrate http phrate	hot"," Il","s Iles"," rry_cou ate"," ist_hos ate"," ist_hos ist_host ist_host ist_host ist_host SF SF SF SF REJ	num_fail u_attemp num_outh same_srv t_same_sr t_host_s srv_rerr 0 146 0 232 199 0	ed_logi ted", "m ound_cm ror_rate ror_rate error_r ror_rate ist_bytes 0 0 8153 420 0	ns","log um root" ds", is _ "diff si rate", ate", dst rate", ", 'attack 0 0 0 0 0 0	red in', "run file serror ra v_rate", " t_host_sarror ra t_host_sarror ra t_host_sarror t_ t_host_sarror t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_	crea ", srv_d _serr flag" 0 0 0 0	tions", iiff_host_ or_rate",] hot num_fa 0 0 0 0 0 0 0 0	ited logins for 0 0 0 0	ged_in_num_co 0 1 1	mpromised roo 0 0 0
"wroi" "num" "num" "ser" "dst" "dst" "dst" "dst" test test test test 1 2 3 4	Ig_fragmer comprovis puest_logi puest_logi host_srv_ host_srv_ host_rerr n. head() 0 0 0 0 0 0	t", "urg ed", "ro num acco ", "count "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns up tp tp	ent", " iot_she eess_fi_ts rror r rtet, "d st_rat st_rat service other phrate http phrate	hot"," Il","s Iles"," rry_cou ate"," ist_hos ate"," ist_hos ist_host ist_host ist_host ist_host SF SF SF SF REJ	num_fail u_attemp num_outh same_srv t_same_sr t_host_s srv_rerr 0 146 0 232 199 0	ed_logi ted", "m ound_cm ror_rate ror_rate error_r ror_rate ist_bytes 0 0 8153 420 0	ns","log um root" ds", is _ "diff si rate", ate", dst rate", ", 'attack 0 0 0 0 0 0	red in', "run file serror ra v_rate", " t_host_sarror ra t_host_sarror ra t_host_sarror t_ t_host_sarror t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_	crea ", srv_d _serr flag" 0 0 0 0	tions", iiff_host_ or_rate",] hot num_fa 0 0 0 0 0 0 0 0	ited logins for 0 0 0 0	ged_in_num_co 0 1 1	mpromised roo 0 0 0
"wroi" "num" "num" "ser" "dst" "dst" "dst" "dst" test test test test 1 2 3 4	Ig_fragmer comprovis puest_logi puest_logi host_srv_ host_srv_ host_rerr n. head() 0 0 0 0 0 0	t", "urg ed", "ro num acco ", "count "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns up tp tp	ent", " iot_she eess_fi_ts rror r rtet, "d st_rat st_rat service other phrate http phrate	hot"," Il","s Iles"," rry_cou ate"," ist_hos ate"," ist_hos ist_host ist_host ist_host ist_host SF SF SF SF REJ	num_fail u_attemp num_outh same_srv t_same_sr t_host_s srv_rerr 0 146 0 232 199 0	ed_logi ted", "m ound_cm ror_rate ror_rate error_r ror_rate ist_bytes 0 0 8153 420 0	ns","log um root" ds", is _ "diff si rate", ate", dst rate", ", 'attack 0 0 0 0 0 0	red in', "run file serror ra v_rate", " t_host_sarror ra t_host_sarror ra t_host_sarror t_ t_host_sarror t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_	crea ", srv_d _serr flag" 0 0 0 0	tions", iiff_host_ or_rate",] hot num_fa 0 0 0 0 0 0 0 0	rate", "dst	ged_in_num_co 0 1 1	mpromised roo 0 0 0
"wroi" "num" "num" "ser" "dst" "dst" "dst" "dst" test test test test 1 2 3 4	Ig_fragmer comprovis puest_logi puest_logi host_srv_ host_srv_ host_rerr n. head() 0 0 0 0 0 0	t", "urg ed", "ro num acco ", "count "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns up tp tp	ent", " iot_she eess_fi_ts rror r rtet, "d st_rat st_rat service other phrate http phrate	hot"," Il","s Iles"," rry_cou ate"," ist_hos ate"," ist_hos ist_host ist_host ist_host ist_host SF SF SF SF REJ	num_fail u_attemp num_outh same_srv t_same_sr t_host_s srv_rerr 0 146 0 232 199 0	ed_logi ted", "m ound_cm ror_rate ror_rate error_r ror_rate ist_bytes 0 0 8153 420 0	ns","log um root" ds", is _ "diff si rate", ate", dst rate", ", 'attack 0 0 0 0 0 0	red in', "run file serror ra v_rate", " t_host_sarror ra t_host_sarror ra t_host_sarror t_ t_host_sarror t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_	crea ", srv_d _serr flag" 0 0 0 0	tions", iiff_host_ or_rate",] hot num_fa 0 0 0 0 0 0 0 0	ited logins for 0 0 0 0	ged_in_num_co 0 1 1	mpromised roo 0 0 0
"wron "num "num "is_j"rer "dst "dst" "dst "dst" "dst " test " ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' '	ng fragmen comprosis skells*,*, host skells*,*, host diff host srv_v n. columns=c n. columns=c n. head() 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	t", "urg ed", "ro "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns udp top top top top	ent"," ot she less fi int","s irror r ist_rat service other private http private F ist_rat	hot"," ill","s", iles","y cou ate","st hos e","dst ist hos sr sr sr sr sr sr sr sr sr sr sr sr sr	nun fail u_attenp nt teap sane srv t_sane sr t_hast s srv_rerr 146 0 232 199 0	ed_logi ted", "m ound_cm ror_rate ror_rate error_r ror_rate ist_bytes 0 0 8153 420 0	ns","log um root" ds", is _ "diff si rate", ate", dst rate", ", 'attack 0 0 0 0 0 0	red in', "run file serror ra v_rate", " t_host_sarror ra t_host_sarror ra t_host_sarror t_ t_host_sarror t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_ t_	crea ", srv_d _serr flag" 0 0 0 0	tions", iiff_host_ or_rate",] hot num_fa 0 0 0 0 0 0 0 0	ited logins for 0 0 0 0	ged_in_num_co 0 1 1	mpromised roo 0 0 0
"wron "num "num" "is_j"rerr "dst "dst" "dst" "dst "dst" (dst") "dst" "dst" "dst" "dst" "dst" "solution" "solut	ng fragmen shells"," huest logis host stuff host stuff host stuff n. columns=c columns=c columns=c n. head() 0 0 0 0 0	t", "urg ed", "ru ", "cou "srv_re srv_re srv_re srv_re diff_ho or_rate columns columns columns columns columns columns columns columns tp tp tp tp tp tp	ent"," ot_shei less_fi less_fi service service other http: private http: private less_fi	hot"," ill","s", iles","s iles","s ist hos ist host ist host fing sr sr sr sr sr sr sr sr sr sr sr sr butiu (8))	num fail u_attemp num fail t same s same s t host s srv_rerr	led logi tred", 'n ror rate", rate", rc port serror_rate ist bytes 0 0 8153 420 0 *:D	ns", 'log dir", 'is ' "dir", 's ru "dir", 's ru "ate", 'dsr ate", 'dsr a	rim file iost_login serror rate", " thost_order", the thost_order", the thost_order"	crea ", srv_d _serr flag" 0 0 0 0	tions", iiff_host_ or_rate",] hot num_fa 0 0 0 0 0 0 0 0	ited logins for 0 0 0 0	ged_in_num_co 0 1 1	mpromised roo 0 0 0



	Model Building
	train X-train new(ols] train y-train new(ols] test X-test new(ols] test y-test new(ols]
	Fig7.4:ModelBuilding
Log	istic Regression
log	<pre>building Hodels m sklearn.linear_model import LogisticRegression rrg = LogisticRegression(random_state=0,solver='lbfgs',multi_class='multinomial') rrg.fit(train X, train y) rrg.predict(train_X) #by default, it use cut-off as 0.5</pre>
lis	<pre>st(zip(cols, logreg.coef_[0]))</pre>
log	reg.intercept_
log	<pre>score(train_X,train_y)</pre>
	Fig7.5: LogisticRegression
	Decision Trees
	train_X.shape
	param_grid = { 'max_depth': np.arange[2, 12), 'max_features': np.arange[10,15]}
	train_y.shape
	<pre>from sklearn.model selection import GridSearchCV from sklearn.tree import DecisionTreeClassifier, export graphviz, export tree = GridSearchCV(DecisionTreeClassifier(), param grid, cv = 10,verbose=1,n_jobs=-1) tree.fit(train_X, train_y)</pre>
	tree.best_score_
	tree.best_parans_
	train mred = tree predict(train X)

print(metrics.classification_report(train_y, train_pred))

test ored = tree.oredict(test X)

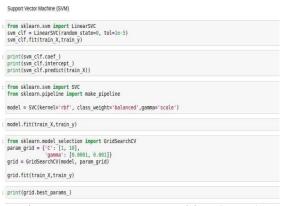
Fig7.6:DecisionTrees

	Random Forest
	<pre>from sklearn.ensemble import RandomForestClassifier pargrid_rf = { 'n_estimators': [50,60,70,80,90,100],</pre>
	<pre>from sklearm.model_selection import GridSearchCV gscv_rf = GridSearchCV(estimator=RandomForestClassifier(),</pre>
	gscv_results.best_params_
100	gscv_rf.best_score_
	<pre>radm_clf = RandomForestClassifier(oob_score=True,n_estimators=80, max_features=5, n_jobs=-1) radm_clf.fit(train_X, train_y)</pre>

Fig7.7:Random forest

IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501

Vol.15, Issue No 1, 2025



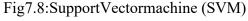




Fig7.9:LocalHostincmdpython app.py

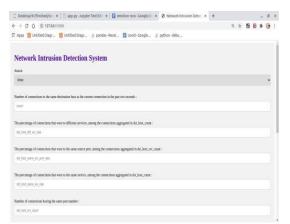


Fig7.10:NetworkIntrusionDetection System

🗘 Desktop/Hijfnished/se: x 🗅 app.pr-Jupyter Text Edi x 🖥 emotion reco-Google D: x 🛛 Network intrusion Detect x 🕴					-	9 :
· → C △ © 127.00.15100	ą	Ŕ	58	0	* () :
🛿 Apps 🔢 Unitled Diegr 🔢 Unitled Diegr 🧋 pandas-Recei 📓 covid-Coogle 🐒 python-debu						
States of the connection-Normal or Erwe:						
Ober						v
LasFeg:						
3						
l Fransshily leggt it Unbersite :						
5						
The presenting of connections that were no the same service, among the connections appropriate in coart :						
5						
The percentage of connections that have activated the Eng (4) of , c) are 3, among the connections aggregated in count:						
\$						
Destantion notwork service used http or tox :						
						ġ
k						

Fig7.11: Entering the input data

Predict	

Attack Class should be DOS

Fig7.12:Predict attack

4. CONCLUSIONANDFUTURESCOPE

CONCLUSION

Right now, estimations of help vector machine, ANN, CNN, Random Forest and profound learning calculations dependent on modern CICIDS2017 dataset were introduced relatively. Results show that the profound learning calculation performed fundamentally preferable outcomes over SVM, ANN, RF and CNN. We aregoingtoutilizeportsweependeavorsaswell as other assault types with AI and profound learning calculations, Apache Hadoop and sparkle innovations together dependent on this dataset later on.

All these calculation helps us to detect the cyberattack in network. It happens in the way that when we consider long back years there maybesomanyattackshappened sowhen these attacks are recognized then the features at which values these attacks are happening will be stored insome datasets. So by using these datasets we

are going to predict whether cyber-attack isdone or not. These predictions can be done by four algorithms like SVM, ANN, RF, CNN this paper helps to identify which algorithm predicts the best accuracy rates which helps to predict best results to identify the cyber-attacks happened or not.

5.2FUTURESCOPE

The future scope of cyber threat detection using ANNs based on event profiles is promising, with potential benefits in terms of detection accuracy, real-time monitoring, adaptive learning, and scalability. However, organizations need to consider the challenges and invest in the necessary resources to implementandmaintain these advanced systems effectively.

REFERENCES

[1] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.

[2] R. Christopher, "Port scanning techniques and the defense against them,"SANS Institute, 2001.

[3] M. Baykara, R. Das, and I. Karadogan, "Bilgig"uvenli gisistemlerindekullanilanarac,

larinincelenmesi," in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013,pp. 231–239.

[4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.

[5] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in DARPA Information Survivability Conference and Exposition, 2003.Proceedings, vol. 1. IEEE, 2003, pp. 130–138.

[6] K. Ibrahimi and M. Ouaddane, "Management of intrusion detection systems based-kdd99: Analysis with Ida and pca," in Wireless Networks and MobileCommunications

(WINCOM),2017

InternationalConferenceon. IEEE,2017,pp.1–6. [7] N. Moustafa and J. Slay, "Thesignificant features of the unsw-nb15 and the kdd99 data sets for network intrusion detection systems," in Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2015 4th International Workshop on. IEEE, 2015, pp. 25–31.

[8] L.Sun, T.Anthony, H.Z.Xia, J.Chen,

X. Huang, and Y. Zhang, "Detection and classification of malicious patterns in network traffic using Binford's law," in Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864–872.

[9] S. M. Almansob and S. S. Lomte, "Addressing challenges for intrusion detection system usingnaive bayes and pca algorithm," in Convergence in Technology (I2CT), 2017 2nd International Conference for. IEEE, 2017, pp. 565–568.

[10] M. C. Raja and M. M. A. Rabbani, "Combined analysis of support vector machine and principle component analysis for ids," in IEEE International Conference on CommunicationandElectronicsSystems,2016, pp. 1–5.

[11] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," Journal of ComputationalScience,vol.25,pp.152–160, 2018.

[12] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization."inICISSP,2018,pp.108–116.

[13] D.Aksu,S.Ustebay,M.A.Aydin,and

T. Atmaca, "Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm," in International Symposium on Computer and Information Sciences. Springer, 2018, pp. 141–149.

IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501

Vol.15, Issue No 1, 2025

[14] N.Marir,H.Wang,G.Feng,B.Li,and

M. Jia, "Distributed abnormal behaviordetection approach based on deep beliefnetwork and ensemble svm using spark," IEEE Access, 2018. [15] P. A. A. Resende and A. C. Drummond, "Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling," Securityand Privacy, vol. 1, no. 4, p. e36, 2018. [16] C. Cortes and V. Vapnik, "Supportvectornetworks,"Machinelearning,vol.20,no. 3,pp. 273–297, 1995.

[17] R. Shouval, O. Bondi, H. Mishan, A. Shimoni, R. Unger, and A. Nagler, "Application of machine learning algorithms for clinical predictive modeling: a data-mining approach in sct," Bone marrow transplantation, vol. 49, no. 3, p. 332, 2014.