Detection of Cyber Attacks in Network Using Machine Learning Techniques

[1]N.Vivek, [2]N.Prashanth, [3]K.Nithin kumar reddy, [4]K.veeresh, [5]P.Ramesh,

[1,2,3,4] U.G.Scholor, Department of ECE, Sri Indu College Of Engineering & Technology, Ibrahimpatnam, Hyderabad.

[5]Professor, Department of ECE, Sri Indu College Of Engineering & Technology, Ibrahimpatnam, Hyderabad.

ABSTRACT

Cyber-crime is proliferating everywhere exploiting every kind of vulnerability to the computing environment. Ethical Hackers pay more attention towards assessing vulnerabilities and recommending mitigation methodologies. The development of effective techniques has been an urgent demand in the field of the cyber security community. Most techniques used in today'sIDSarenotabletodealwiththedynamic andcomplexnatureofcyber-attacksoncomputer networks. Machine learning for cyber security hasbecomeanissueofgreatimportancerecently due to the effectiveness of machine learning in cyber security issues. Machine learning techniques have been applied for major challenges in cyber security issues like intrusion detection, malware classification and detection, spamdetectionandphishingdetection.Although machine learning cannot automate a complete cyber security system, it helps to identify cyber security threats more efficiently than other software-oriented methodologies, and thus reduces the burden on security analysts. Hence, efficient adaptive methods like various techniques of machine learning can result in higherdetectionrates,lowerfalsealarmratesand reasonable computation and communication costs. Our main goal is that the task of finding attacks is fundamentally different from these other applications,making itsignificantlyharder for the intrusion detectioncommunity to employ machine learning effectively.

Keywords: Cyber-crime, Machine learning, Cyber-security, Intrusion detection system.

I. INTRODUCTION

Today, political and commercial entities are increasingly engaging in sophisticated cyber-warfaretodamage,disrupt,orcensorinformation content in computer networks. In designing network protocols, there is a need to ensure reliabilityagainstintrusionsofpowerfulattackers that can even control a fraction of parties in the network. The controlled parties can launch both passive (e.g., eavesdropping, nonparticipation) and active attacks (e.g., jamming, message dropping, corruption, and forging). Intrusion detection is the process of dynamically monitoring events occurring in a computer system or network, analysing them for signs of possible incidents and often interdicting the unauthorized access. This is typically accomplished by automatically collecting information from a variety of systems and network sources, and then analysing the information for possible security problems. Traditional intrusion detection and prevention techniques, like firewalls, access control mechanisms, and encryptions, have several limitations in fully protecting networks and systems from increasingly sophisticated attacks like denial of service. Moreover, most systems built based on such techniques suffer from high false positive and false negative detection rates andthelackofcontinuouslyadaptingtochanging malicious behaviours. In the past decade, however, several Machine Learning (ML) techniques have been applied to the problem of intrusion detection with the hope of improving detectionratesandadaptability.Thesetechniques areoftenusedtokeeptheattackknowledgebases up-to-date and comprehensive. In recent days, cyber-security and protection against numerous cyber-attacks are becoming a burning question. The main reason behind that is the tremendous growth of computer networks and the vast number of relevant applications used by individuals or groups for either personal or commercial use, especially after the acceptance oftheInternetofThings(IoT).Thecyber-attacks

cause severe damage and severe financial losses in large-scale networks. The existing solutions like hardware and software firewalls, user's authentication, and data encryption methods are not sufficient to meet the challenge of upcoming demand,andunfortunately,notabletoprotectthe computer network'sseveral cyber-threats.These conventionalsecuritystructuresarenotsufficient as safeguard due to the faster rigorous evolution ofintrusionsystems.Firewallonlycontrolsevery access from network to network, which means preventaccessbetweennetworks.Butitdoesnot provide any signal in case of an internal attack. So, it is obvious to develop accurate defense techniques such as machine learning-based intrusiondetectionsystem(IDS)forthesystem's securityIngeneral,anintrusiondetectionsystem (IDS) is a system or software that detects infectious activities and violations of policy in a network or system. An IDS identifies the inconsistencies and abnormal behavior on a networkduringthefunctioningofdailyactivities in a network or system used to detect risks or attacksrelatedtonetworksecurity,likedenial-of-service(Dos).Anintrusiondetectionsystemalso helps to locate, decide, and control unauthorized systembehavioursuchasunauthorizedaccess,or modification and destruction.Therearedifferent typesofintrusiondetectionsystemsbasedonthe user perspective. For instance, they are host-based and network-based IDS.

II.   LITERATURESURVEY

AnIDSgenerallyhastodealwithproblemssuch as large network traffic volumes, highly uneven datadistribution,theResearchArticleVolume11 Issue No.06 IJESC, June 2021 28154 http://ijesc.org/difficultytorealizedecisionboundaries between normal and abnormal behaviour, and a requirement for continuous adaptation to a constantlychangingenvironment.Ingeneral,the challenge is to efficiently capture and classify various behaviours in a computer network. Strategies for classification of network behaviours are typically divided into two categories: misuse detection and anomaly detection. Misuse detection techniques examine both network and system activity for known instances of misuse using signature matching algorithms.Thistechniqueiseffectiveat

detecting attacks that are already known. However, novel attacks are often missed giving rise to false negatives. Alerts may be generated bytheIDS,butreactiontoeveryalertwastestime andresourcesleadingtoinstabilityofthesystem. To overcome this problem, IDS should not start elimination procedure as soon as the first symptomhasbeendetectedbutratheritshouldbe patient enough to collect alerts and decide based on the correlation of them. Some research statistics with regards to the impact of cyber security to businesses, organizations, and individuals include:

In recent years, cybercrime has been responsible for more than $400 billion in funds stolen and coststomitigatedamagescausedbycrimes.Ithas beenpredictedthatashortageofover1.8million cybersecurity workers will be experienced by 2022. It's been predicted that organizations globallywillspendatleast$100billionannually on cyber security protection. Attackers currently make over $1 billion in annual revenue from Ransomware attacks, such as Wannacry and Crypto Wall attacks

III.   EXISTINGSYSTEM

Within the ever-growing and quickly increasing field of cyber security, it is nearly impossible to quantify or justify the explanations why cyber security has such an outsized impact. Permitting malicious threats to run anyplace, at anytime or in any context is a long way from being acceptable, and may cause forceful injury. It particularly applies to the Byzantine web of consumers and using the net and company informationthatcybersecuritygroupsarefinding it hardtoshieldandcontain. Cyber securitymay be a necessary thought for people and families alike, also for businesses, governments, and academic establishments that operate inside the compass of the world network or net. With the facilityofMachineLearning,wewilladvancethe cyber security landscape. Today's high-tech infrastructure, that has network and cyber security systems, is gathering tremendous amounts of data and analytics on almost all the keyaspectsofmission-criticalsystems.Whereas peoplestillgivethekeyoperationaloversightand intelligent insights into today's infrastructure. Mostintrusiondetectionsystemsarefocusedon

the perimeterattacksurfacethreats,startingwith your firewall. That offers protection of your network's northsouth traffic, but what it doesn't take intoaccountis the lateral spread (east-west) that many network threats today take advantage of as they infiltrate your organization's network and remain there unseen. We know this is true because research has shown that only 20% of discovered threats come from northsouth monitoring. When an IDS detects suspicious activity, the violation is typically reported to a security information and event management (SIEM) system where real threats are ultimately determined amid benign traffic abnormalities or otherfalsealarms.However,thelongerittakesto distinguish a threat, the more damage can be done. An IDS is immensely helpful for monitoring the network, but their usefulness all dependsonwhatyoudowiththeinformationthat they give you. Because detection tools don't block or resolve potential issues, they are ineffective at adding a layer of security unless you have the right personnel and policy to administer them and act on any threats. An IDS cannot see into encrypted packets, so intruders canusethemtoslipintothenetwork.AnIDSwill not register theseintrusionsuntil theyare deeper into the network, which leaves your systems vulnerable until the intrusion is discovered. This isahugeconcernasencryptionisbecomingmore prevalenttokeepourdatasecure.Onesignificant

issue with an IDS is that they regularly alert you to false positives. In many cases false positives aremorefrequentthanactualthreats.AnIDScan be tuned to reduce the number offalse positives; however, your engineers will still have to spend time responding to them. If they don't take care tomonitorthefalsepositives,realattackscanslip through or be ignored.

PROPOSEDSYSTEM

MachineLearningalgorithmscanbeusedtotrain and detect if there has been a cyber attack. As soon as the attack is detected, an email notification can be sent to the security engineers orusers.Anyclassificationalgorithmcanbeused to categorize if it is a DoS/DDoS attack or not. One example of a classification algorithm is Support Vector Machine (SVM) which is a supervised learning method that analyses data andrecognizespatterns.Sincewecannotcontrol when,whereorhowanattackmaycomeourway, and absolute prevention against these cannot be guaranteed yet, our best shot for now is early detection which will help mitigate the risk of irreparable damage such incidents can cause. Organizationscanuseexistingsolutions orbuild their own to detect cyber attacks at a very early stage to minimize the impact. Any system that requires minimal human intervention would be ideal.

SYSTEMARCHITECTURE
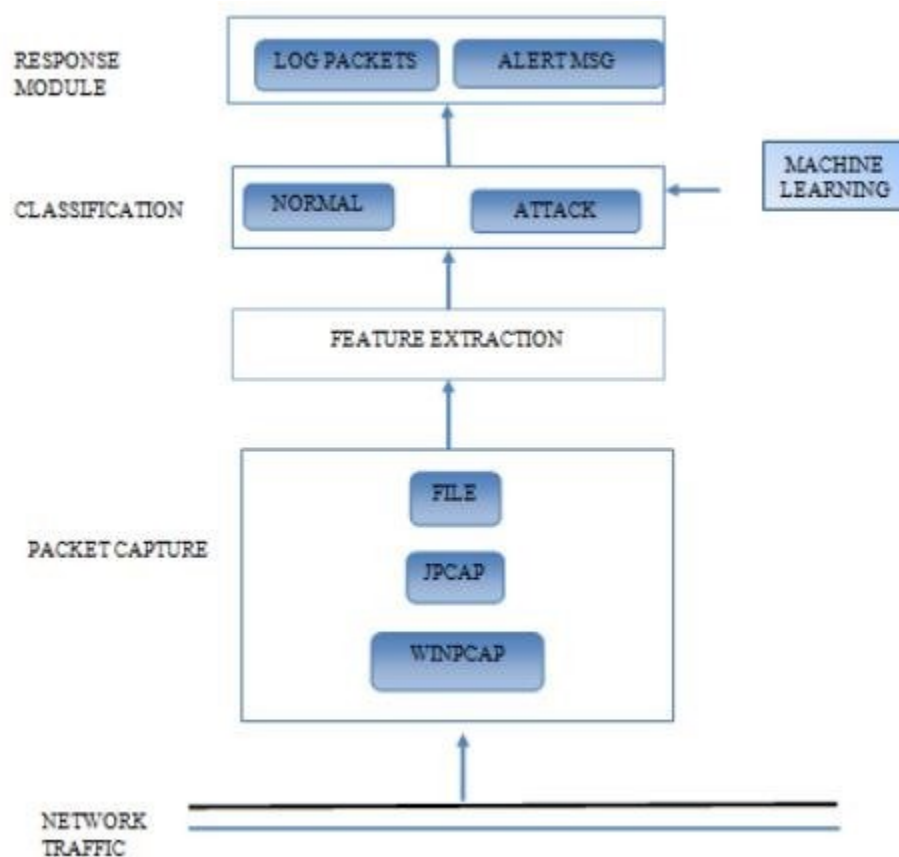
IV. IMPLEMENTATION

1.Systemlevel:

CumulativeandperuserCPUusageUsageofreal and virtual memory Amount of swap space currently available Amount of free memory I/O and disk usage

User level:

Type of user and user privileges Login/Logout period and location Access of resources and directories Type of software/programs use Key stroke pattern (usein future) Average number of packets sent and received Duration of the connection

Processlevel

The number of processes and their types Relationship among processes

Packetlevel

Averagenumberofpacketssentandreceived

V. CONCLUSION

Tolocateapplicationlayerattacksusingartificial intelligence (AI) was suggested in this article. Graph-based division method and dynamic programmingareusedtoobtainexamples(inthe form of PCRE standard articulations) for the model. In order to show the actual behaviour of the apps and to detect digital attacks, the usual articulationsareusedasaguide.Additionally,we presentedtheresultsthatshowhowthesuggested computation may effectively be used to locate application layer attacks.

REFERENCES

[1]. DipankarDasgupta. Immunity-based intrusion detection system: A general frame-work.InProceedingsofthe22ndNational

Information Systems Security Confer-ence (NISSC). Arlington, Virginia, USA, 1999.

[2]. Jonatan Gomez and DipankarDasgupta. Evolvingfuzzyclassi_ersforintrusiondetection. In Proceedings of the 2002 IEEE Workshop on Information Assurance,West Point, NY, USA, 2002.

[3]. Steven A. Hofmeyr, Stephanie Forrest, and Anil Somayaji. Intrusion detection using sequences of system calls. Journal of Computer Security, 6(3):151{180, August 1998.

[4]. Peter Mell Karen Scarfone. Guide to intrusiondetectionandpreventionsystems(idps). National Institute of Standards and Technology, NIST SP - 800-94, 2007.

[5]. Jungwon Kim, Peter J. Bentley, Uwe Aickelin,Julie Greensmith,GianniTedesco,and Jamie Twycross. Immune system approaches to intrusion detection { a review. Natural Computing, 6(4):413{466, December 2007.

[6] A. Shabtai, E. Menahem and Y. Elovici. F-Sign: automatic, function-based signature generation for malware, systems, man, and cybernetics, Part C: applications and reviews. Transactions on IEEE, 41, 494–508, 2011.

[7] D. Kong, J. Gong, S. Zhu, P. Liu and H. Xi. SAS: semantics aware signature generation for polymorphic worm detection. International Journal of Information Security, 50, 1–19, 2011.

[8] M. Sharma and D. Toshniwal. Pre-clustering algorithm for anomaly detection and clustering that uses variable size buckets. RecentAdvances in Information Technology, 515–519, 2012.