Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

ANALYSIS AND DETECTION OF DDOS ATTACKS ON CLOUD COMPUTING

Mrs. Bonagiri Rajitha *Assistant professor CSE, Vaagdevi College of Engineering(Autonomous),India*
Pavuluri Sravani,*UG Student,CSE,Vaagdevi College of Engineering(Autonomous),India*
Guguloth Kalyan,*UG Student,CSE,Vaagdevi College of Engineering(Autonomous),India*
Kuruchapally Abhishek ,*UG Student,CSE,Vaagdevi College of Engineering(Autonomous),India*
Nagishetty Harshini,*UG Student,CSE,Vaagdevi College of Engineering(Autonomous),India*

ABSTRACT

Cloud service availability has been one of the major concerns of cloud service providers (CSP), while hosting different cloud-based information technology services by managing different resources on the internet. The vulnerability of internet, the distribute nature of cloud computing, various security issues related to cloud computing service models, and cloud's main attributes contribute to its susceptibility of security threats associated with cloud service availability. One of the major sophisticated threats that happen to be very difficult and challenging to counter due to its distributed nature and resulted in cloud service disruption is Distributed Denial of Service (DDoS) attacks. Even though there are number of intrusion detection solutions proposed by different research groups, and cloud service providers (CSP) are currently using different detection solutions by promising that their product is well secured, there is no such a perfect solution that prevents the DDoS attack. The characteristics of DDoS attack, i.e., having different appearance with different scenarios, make it difficult to detect. This paper will review and analyze different existing DDoS detecting techniques against different parameters, discusses their advantage and disadvantages, and propose a hybrid statistical model that could significantly mitigate these attacks and be a better alternative solution for current detection problems.

1. INTRODUCTION

A Distributed Denial of Service (DDoS) attack is a distributed, coordinated attack on the availability of services of a host server (application server, storage, database Server, or DNS server) or network resource, launched indirectly through many compromised systems called botnets on the Internet.

Since its inception, distributed denial-of-service (DDoS) attacks have evolved over the years. As mentioned above, DDoS attacks have been a major challenge to the researchers and big security issue to the cloud computing environment. In modern very sophisticated approaches, by assuming multiple targets on the cloud resources, applications or network, hackers use multiple vectors and do not take any risk of missing their target cloud resources in a single attack campaign. DDoS attacks can range from simple network attacks to all cloud resources attacks. They can be volumetric, designed to disrupt a host service and make it unreachable, or attack application layers, targeting a specific service on the host. DDoS use of multiple botnet machines to amplify attacks could make it very challenging to stop it or to trace back the hackers

2. LITERATURE SURVEY

TITLE: "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques"
AUTHORS: Abdul Raoof Wani; Q. P. Rana; U. Saxena; Nitin Pandey
ABSTRACT: The primary benefit of the cloud is that it elastically scales to meet variable demand and it provides the environment which scales up and scales down instantly according to the demand, so it needs great protection from DDoS attacks to tackle downtime effects of DDoS Attacks. Distribute Denial of Service attacks fall on the category of critical attacks that compromise the availability of the network. These attacks have become sophisticated and continue to grow at a rapid pace so to detect

and counter these attacks have become a challenging task. This work was carried out on the owncloud environment using Tor Hammer as an attacking tool and a new dataset was generated with Intrusion Detection System. This work incorporates various machine learning algorithms: Support Vector Machine, Naive Bayes, and Random Forest for classification and overall accuracy was 99.7%, 97.6% and 98.0% of Support Vector Machine, Random Forest and Naive Bayes respectively.

TITLE: "Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment"

AUTHORS: AntenehGirma; Moses Garuba; Jiang Li; Chunmei Liu

ABSTRACT: Cloud service availability has been one of the major concerns of cloud service providers (CSP), while hosting different cloud based information technology services by managing different resources on the internet. The vulnerability of internet, the distribute nature of cloud computing, various security issues related to cloud computing service models, and cloud's main attributes contribute to its susceptibility of security threats associated with cloud service availability. One of the major sophisticated threats that happen to be very difficult and challenging to counter due to its distributed nature and resulted in cloud service disruption is Distributed Denial of Service (DDoS) attacks. Even though there are number of intrusion detection solutions proposed by different research groups, and cloud service providers (CSP) are currently using different detection solutions by promising that their product is well secured, there is no such a perfect solution that prevents the DDoS attack. The characteristics of DDoS attack, i.e., Having different appearance with different scenarios, make it difficult to detect. This paper will review and analyze different existing DDoS detecting techniques against different parameters, discusses their advantage and disadvantages, and propose a hybrid statistical model that could significantly mitigate these attacks and be a better alternative solution for current detection problems.

TITLE: "A Comprehensive Analysis of DDoS attacks based on DNS"

AUTHORS: Lei Fang1*, Hongbin Wu1*, Kexiang Qian1 , Wenhui Wang and Longxi Han1

ABSTRACT: Domain Name System (DNS) is a basic and important services on the Internet. However, Distributed Denial of Service (DDoS) has been a threat to the security and stability of DNS for a long time. In this paper, we take a review of DDoS attacks based on NS aiming to make a better understanding of it. Firstly, we analyse the security vulnerabilities of DNS related to denial-of-service attack. Then we discuss the classification of DNS DDoS attacks, and divide them into four categories according to the attack mode. Finally, we summarize the existing defense methods of two aspects. We aim to get a better understanding of the DDoS attacks based on DNS andexpand the understanding of DDoS attacks

TITLE: "Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic "

AUTHORS: Rami J. Alzahrani,Ahmed Alzahrani.

ABSTRACT: The recent advance in information technology has created a new era named the Internet of Things (IoT). This new technology allows objects (things) to be connected to the Internet, such as smart TVs, printers, cameras, smartphones, smartwatches, etc. This trend provides new services and applications for many users and enhances their lifestyle. The rapid growth of the IoT makes the incorporation and connection of several devices a predominant procedure. Although there are many advantages of IoT devices, there are different challenges that come as network anomalies. In this research, the current studies in the use of deep learning (DL) in DDoS intrusion detection have been presented. This research aims to implement different Machine Learning (ML) algorithms in WEKA tools to analyze the detection performance for DDoS attacks using the most recent CICDDoS2019 datasets. CICDDoS2019 was found to be the model with best results. This research has used six different types of ML algorithms which are K_Nearest_Neighbors (K-NN), super vector machine (SVM), naïve bayes (NB), decision tree (DT), random forest (RF) and logistic regression (LR). The best accuracy result in the presented evaluation was achieved when utilizing the Decision Tree (DT) and Random Forest (RF) algorithms, 99% and 99%, respectively. However, the DT is better than RF

because it has a shorter computation time, 4.53 s and 84.2 s, respectively. Finally, open issues for further research in future work are presented.

3. PROBLEM STATEMENT

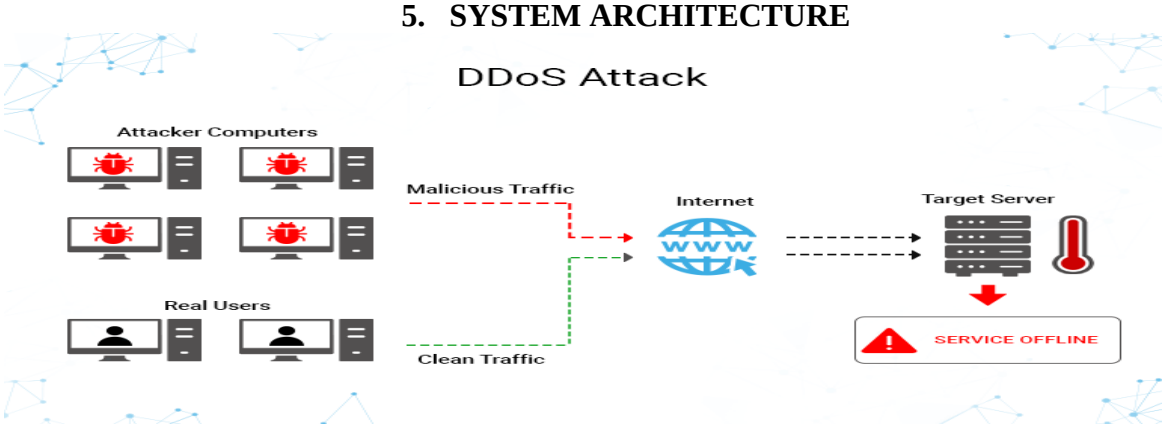
Considering how hackers are using very sophisticated attacking tools and methods to intrude and disrupt systems, the road ahead for the next generation of intrusion detection system is very challenging and need a collective effort. Besides preventing these attacks, it should also be realized that any intended detection scheme should take into consideration of the advancement of the networking technology and major changes in systems like cloud computing environment. The main challenge in detecting such attacks efficiently is the reduction of the false alarm rate.

Different types of DDoS detection methods have been proposed based on different architectures namely, victim-end, source-end, and in-network [29]. These methods includes statistical methods, soft computing methods, knowledge based methods, and data mining and machine learning methods. While the important aspect of these detection schemes is to defend itself from attacks, those traditional intrusion detection systems have not adapted to new technological paradigms like mobile and wireless networks [22]. Different schemes have been used with these detection mechanisms. The following table discusses the advantages and disadvantages of different detection schemes.

4. PROPOSED SYSTEM

We propose a hybrid model by noticing that two approaches the covariance matrix based and the entropy-based system – are heuristically similar in that both classify a DDoS attack via measuring heightened dependency in the data.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

6.1 ADMIN

In this application admin is the module, here admin can login directly with the application and after login successful admin can perform operations such as Classify and detectDDos add viewgraph and logout.

6. 2 Owner

In this application owner is a module, here owner should register with the application then only the owner can access his home page after successful login he can perform some operations such as uploadFile, viewUploads, ViewRequest and Accept/Reject and logout

6.3 User

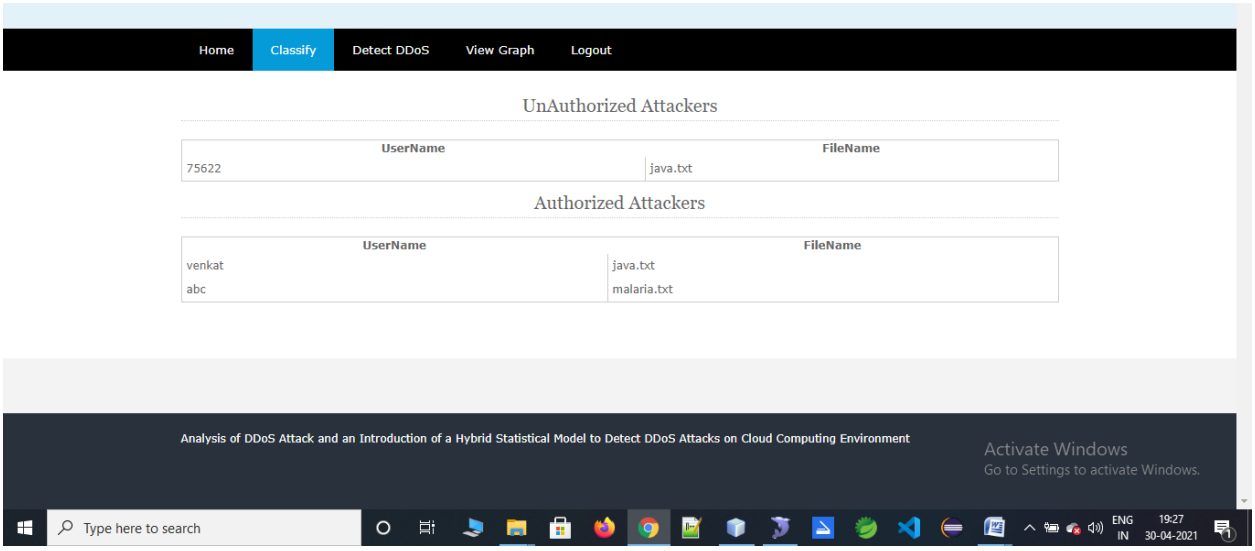
In this application user is a module, here user should register with the application then only the user can access his home page after successful login he can perform some operations such as viewProfile, viewUploads, searchFile And requestStatus and logout

6.4 Cloud

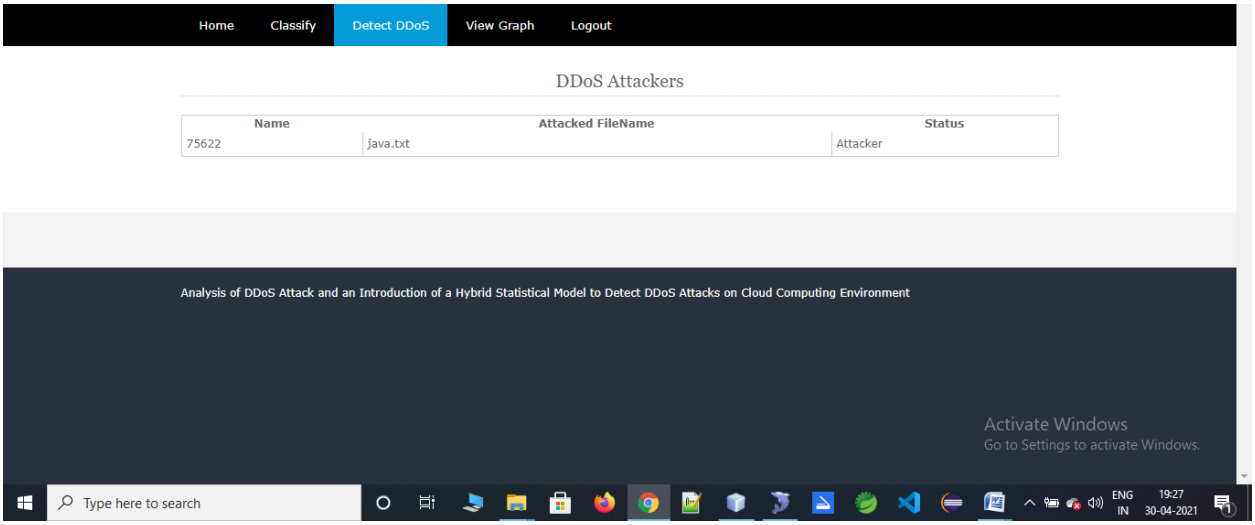
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

In this application cloud is the module, here cloud can login directly with the application and after login successful cloud can perform operations such as view All Uploaded Files and logout.

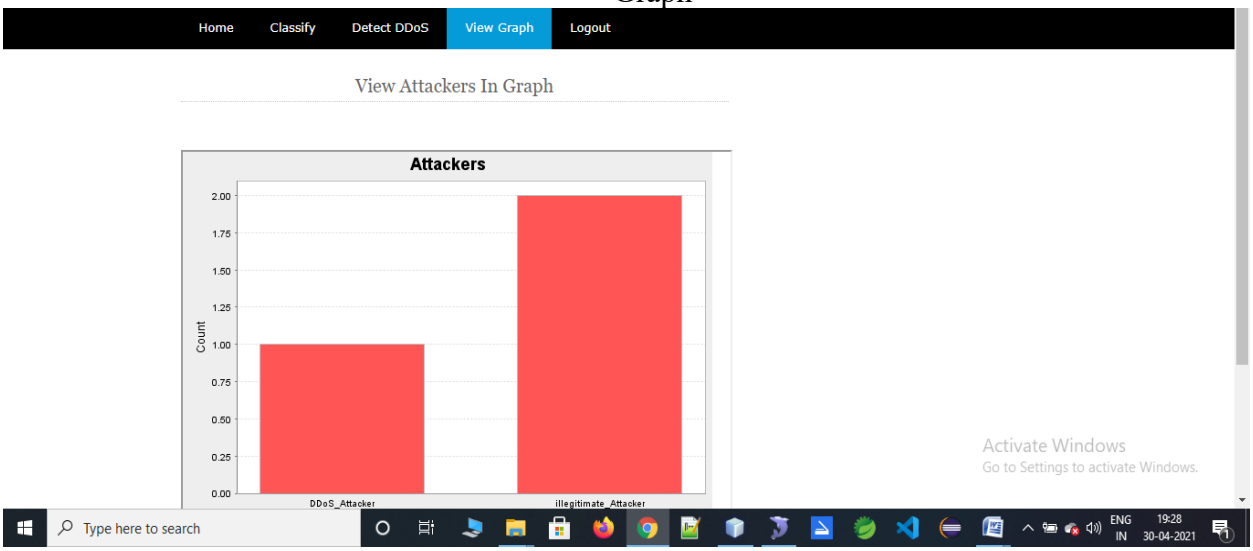
7 RESULTS / EXPECTED OUTPUT



Ddos attack



Graph



8. CONCLUSION

In this paper, we proposed an effective alternative hybrid scheme against DDoS attacks based on Entropy and Covariance Matrices. We are looking forward to apply a different approach with a comprehensive hybrid detection scheme at both the network and host level. Because, many of the available DDoS detection schemes performance found to be below the par and DDoS attacks are growing exponentially, it prompts the real need of having a comprehensive solution. We believe that this proposed scheme with double check points is expected to be a better alternative solution in mitigating the risk significantly by producing a better result.

FUTURE SCOPE:

One or multiple motivations can lead to an attack. Future researchers need to develop techniques that not only detect an attack but also intelligently identify the attacker's methods and the traffic rates. As well, the mechanisms should be capable of determining the legitimacy of the source of the attack.For instance, instead of concentration on one point for detecting an attack, the approach can work towards having distributed points of attack detection and correction. To increase the detection and inference speed, the approaches can further provide distributed points of attack analysis separate from the attack points but relaying attacks descriptions to a central point. This would ensure that all facets of an attack are determined without negatively affecting performance.

9. REFERENCES

[1] An NTT Communications, "Successfully combating DDoS Attacks", White Paper, August 2012
[2] Amit Khajuria1, Roshan Srivastava, "Analysis of the DDoS Defense Strategies in Cloud Computing", international journal of enhanced research in management & computer applications vol. 2, issue 2, February 2013
[3] Radware Ltd, "The Ultimate Guide to Everything You Need To Know About DDoS Attacks", 2013
[4] David Dittrich. "The "Stacheldraht" Distributed Denial of Service Attack Tool". University ofWashington, December 31, 1999, http://staff.washington.edu/dittrich/misc/stacheldraht.analy sis.txt (8 April 2003).
[5] Sven Dietrich, Neil Long, and David Dittrich, "Analyzing Distributed Denial of Service Tools: The Shaft Case", USENIX Association, Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, Louisiana, 2000
[6] A.M. Lonea, D.E. Popescu, H. Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment", International Journal of Computing and communication, ISSN 1841-9836 8(1):70-78, February, 2013.
[7] CERT Coordination Center, Carnegie Mellon Software Engineering Institute, "CERT® Incident Note IN-2001- 13", November 27, 2001. http://www.cert.org/advisories/CA-2001-20.html. (14 March 2003).
[8] "CERT® Advisory CA-2001-20 Continuing Threats to Home Users", CERT Coordination Center, Carnegie Mellon Software Engineering Institute. July 23, 2001. http://www.cert.org/advisories/CA-2001-20.html. (14 March 2003)
[9] F-Secure.F-SecureVirusDescriptions: Agobot. http://www.f-secure.com/v-descs/ agobot.shtmlS, 2003.
[10] Dittrich D. "The ''mstream'' distributed denial of service attack tool", University of Washington, http://staff.washington.edu/dittrich/misc/mstream.analysis. txtS, 2000.