www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

EVALUATION OF DDOS INVASIONS

[1]Mrs. V. MOUNIKA,[2] K. SRAVYA,[3]K. SURYA,[4]K. PAVAN,[5]G. SIRISHA,
[1] Assistant Professor,[2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

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, hence the Evaluaion of DDoS came ahead.

I. INTRODUCTION

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. 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. 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. The foremost purpose is the swift identification of DDoS attacks. This enables security teams to respond promptly, minimizing

potential damage and service disruption.

Risk Mitigation and Impact Assessment:

Evaluating DDoS invasions helps in quantifying potential risks and understanding their impact. This includes assessing the severity of service disruptions, financial losses, and potential reputational damage.

Protection of Digital Assets:

The system aims to shield an organization's digital infrastructure from being overwhelmed by malicious traffic. This safeguards websites, applications, and networks from debilitating downtime.

Ensuring Service Availability:

By evaluating DDoS invasions, the objective is to ensure the continuous availability of online services to legitimate users.

Forensic Analysis and Attribution:

Post-incident evaluation enables comprehensive forensic analysis. This involves tracing the attack's origin, understanding the attack vectors, and potentially attributing the attack to a specific entity.

II. LITERATURE SURVEY

TITLE: DDOS Attacks in Cloud Computing and its Preventions

AUTHORS: Madeeha Anam, Nuzha Deekshitha

ABSTRACT:

Cloud Computing is a popular phrase that is shorthand for applications that were developed to be rich Internet applications that run on the Internet (or "Cloud"). Cloud computing enables tasks to be assigned to a combination of software and services over a network. This network of servers is the cloud. Cloud computing can help businesses transform their existing server infrastructures into dynamic environments, expanding and reducing server capacity depending on their requirements. As it provides services to customers, so same way time it provides facility to attackers. They are several types of threats that attacks the Cloud Computing and Distributed Denial of Service (DDoS) threat is the most prominent attacks in this area of computing This paper provides a wide survey on various DDOS attacks and its preventions, By using neif and Honeypot techniques it helps in preventing DDOS attacks from cloud computing.

TITLE: The Evaluation of DDoS Attack Effect Based on Neural Network.

AUTHORS: Han Qiu, Zimian Liu

ABSTRACT:

DDoS attack effect evaluation is the basis of security strategy deployment. The traditional effect evaluation method relies on the original data, ignoring the relationship between features and the evaluation target and indicator data redundancy, which affects the accuracy and reliability of the evaluation result. To this end, we introduce distance entropy to measure the similarity between features and evaluation target and use LSTM and Triplet networks to measure multiple correlations simultaneously. Then, a 2D-CNN is used to mine deep feature information and filter irrelevant information. We also combine 1D-CNN and attention models to achieve hierarchical sampling of different local features. Finally, three fully connected layers‘ training obtains a total evaluation value. We conducted experiments on five commonly used DDoS datasets. The results showed that the average ranking accuracy of the neural network-based DDoS attack evaluation method (NNDE) reached 87.2%, 91.3%, 88%, 85.6%, and 94.5%, respectively. Compared with other

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

evaluation methods, an average increase of 19.73% indicates that this method can better evaluate the effect of DDoS attacks.

TITLE: Detection Techniques for DDoS Attacks in Cloud Environment

AUTHORS: Sultan Alanazi, Shankar Karuppayah

ABSTRACT:

Cloud computing security remains the goal of both cloud service pro-viders and customers. With many of the security threats to the security of cloud computing, Distributed Denial of Service (DDoS) attacks is one of the most wor-risome. The danger posed by the DDoS attacks are already known and continue to be the predominant security challenge in reaching an impervious and guaran-teed safe cloud computing resources and service delivery. Many researchers have proposed many detection and defense techniques to protect cloud computing against DDoS attacks. In this paper, we present a review of many detection tech-niques that are useful in spotting DDoS attacks that are cloud-based and make comparative analysis between them to find a suitable technique for spotting these cloud computing-based DDoS attacks.

TITLE: Detection of DDoS Vulnerability in Cloud Computing

AUTHORS: Narendra Mishra

ABSTRACT:

Cloud computing security has been a critical issue with its increase in demand. One of the most challenging problems in cloud computing is detecting distributed denial-of-service (DDoS) attacks. The attack detection framework for the DDoS attack is tricky because of its nonlinear nature of interruption activities, atypical system traffic behaviour, and many features in the problem space. As a result, creating defensive solutions against these attacks is critical for mainstream cloud computing adoption. In this novel research, by using performance parameters, perplexed-based classifiers with and without feature selection will be compared with the existing machine learning algorithms such as naïve Bayes and random forest to prove the efficacy of the perplexed-based classification algorithm. Comparing the performance parameters like accuracy, sensitivity, and specificity, the proposed algorithm has an accuracy of 99%, which is higher than the existing algorithms, proving that the proposed algorithm is highly efficient in detecting the DDoS attacks in cloud computing systems. To extend our research in the area of nature-inspired computing, we compared our perplexed Bayes classifier feature selection with nature-inspired feature selection like genetic algorithm (GA) and particle swarm optimization (PSO) and found that our classifier is highly efficient in comparison with GA and PSO and their accuracies are 2% and 8%, respectively, less than those of perplexed Bayes classifier.

III.SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Considering how hackers are using very sophisticated attacking tools and methods

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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. 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. Different schemes have been used with these detection mechanisms.

DISADVANTAGES:

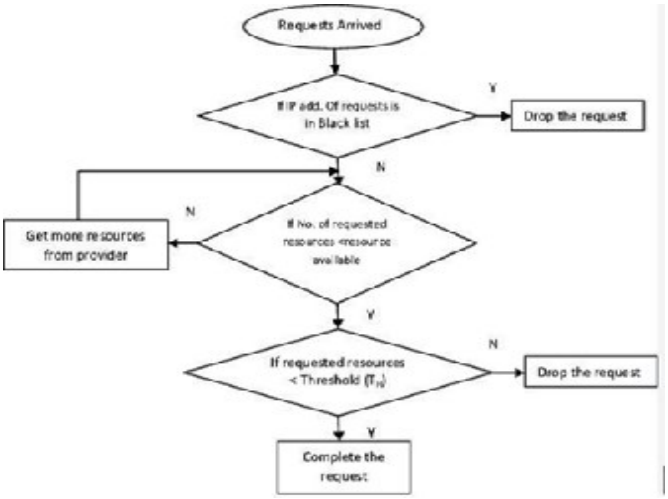
- The main challenge in detecting such attacks efficiently is the reduction of the false alarm rate. Different types of DDoS detection methods have been proposed based on different architectures namely, victim-end, source-end, and in-network
- While the important aspect of these detection schemes is to defend itself from attacks, those traditional intrusion detection systems have not adapted to new technological paradigms like mobile and wireless networks

3.2 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

ADVANTAGES

- We introduce DDoS attack scenario in infrastructure clouds and identify how various elements of cloud computing are affected by DDoS attacks. We present a detailed survey and taxonomy of solutions of DDoS attacks in cloud computing. Based on the developed taxonomy, we identify weaknesses in the state-of-the-art solution space leading to future research directions
- This work would help security researchers to deal with the DDoS differently as compared to the treatment given while considering traditional IT infrastructure.SYSTEM ARCHITECTURE



IV IMPLEMENTATION

3.3 MODULES

- Admin

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

- User
- Owner
- Cloud

3.4 MODULE DESCRIPTION

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 detect DDoS add viewgraph and logout.

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.
- A ―User Module‖ typically refers to a part of a software system that is designed for use by end users. It often includes features for user registration, login, profile management, and other user-related tasks

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/Rejectand logout.
- An ―Owner Module‖ typically refers to a part of a software system that is designed for use by owners or administrators. It often includes features for managing and configuring the system, user management, data management, and other administrative tasks.

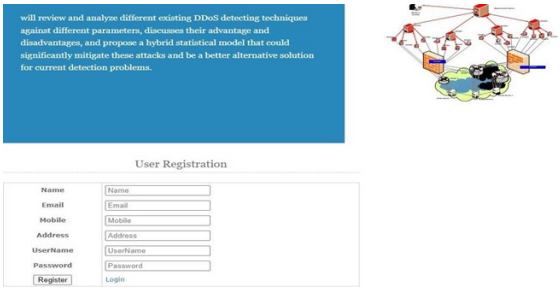
CLOUD:

- 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.
- A ―Cloud Module‖ typically refers to a module within a cloud-based software system. It can be a part of a larger suite of cloud services, providing specific functionality within that system.

SCREEN SHOTS

HOME PAGE

USER REGISTRATION:



USER LOGIN

FIG 5: OWNER REGISTRATION PAGE

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

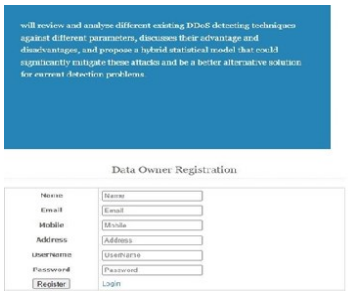
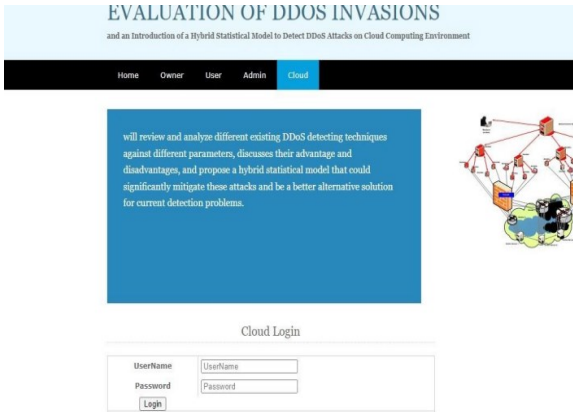


FIG 6: OWNER LOGIN PAGE

CLOUD LOGIN PAGE

.



V. CONCLUSION

CONCLUSION

Evaluating DDoS invasions is paramount for cybersecurity. Assessing impact reveals disruptions, financial losses, and reputational damage. Understanding attack duration and intensity exposes attacker persistence and motives. Identifying targets sheds light on vulnerabilities. Analyzing attack vectors and techniques guides tailored mitigation strategies. Effective response time and post-incident analysis are critical. Proactive measures like load balancing and incident response plans bolster defenses. Collaboration and information sharing with industry peers and authorities enhance collective resilience. Continuous monitoring and adaptation are imperative in this evolving field. A robust evaluation framework ensures organizations are better equipped to combat future DDoS threats.

Additionally, the hybrid statistical model contributes to a reduction in false positives. Traditional statistical methods, while useful, can sometimes flag legitimate traffic as suspicious, leading to unnecessary disruptions in services. Machine learning algorithms, with their ability to discern intricate patterns, refine this process, minimizing false alarms. This not only conserves resources but also maintains a seamless user experience.

VI. FUTURE SCOPE

- The future of DDoS invasion evaluation holds promising advancements driven by technological innovation and evolving cyber threats. Here are key aspects of its future scope
- AI-Driven Threat Detection: Artificial Intelligence (AI) and machine learning algorithms will play a pivotal role in enhancing the accuracy and speed of DDoS attack detection. Advanced models will be trained on vast datasets to recognize subtle attack patterns.

- Behavioral Analysis: Future evaluations will focus on understanding normal network behavior and deviations from it. AI-powered systems will employ behavioral analysis to detect anomalies, thereby improving the ability to identify and respond to DDoS attacks.

REFERENCES

- An NTT Communications, ―Successfully combating DDoS Attacks‖, White Paper,August 2012
- Amit Khajuria1, Roshan Srivastava, ―Analysis of the DDoS Defense Strategies in Cloud Computing‖, international journal of enhanced research in management AND computer applications vol. 2, issue 2, February 2013
- Radware Ltd, ―The Ultimate Guide to Everything You Need To Know About DDoSAttacks‖, 2013
- David Dittrich. ―The ―Stacheldraht‖ Distributed Denial of Service Attack Tool‖.
- University of Washington, December 31, 1999,
- http://staff.washington.edu/dittrich/misc/stacheldraht.analy sis.txt (8 April 2003).
- 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
- 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.
- 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).
- ―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)