Intrusion detection and prevention technique in cloud computing

Miss. S. P. Dhanorkar
SGBAU, Amravati
Maharashtra, India.

Dr. V. M. Thakare
SGBAU, Amravati
Maharashtra, India.

Dr. S. S. Sherekar
SGBAU, Amravati
Maharashtra, India.

ABSTRACT

Internet and web services have become an inseparable part of day to day lives. Hence, ensuring continuous availability of service has become imperative to the success of any organization. But these services are often hampered by constant threats from myriad types of attacks. One such attack is, distributed denial of service attack that results in issues ranging from temporary slowdown of servers to complete non-availability of service. Honeypot, which is a sort of a trap, can be used to interact with potential attackers to deflect, detect or prevent such attacks and ensure continuous availability of service. This paper gives insights and effective solution into the problems posed by distributed denial of service attacks, existing solutions that use honeypots and how a mesh of virtualized honeypots can be used to prevent distributed denial of service attacks.

Keywords—Distributed denial of service, handler, agent, attack source, victim server, firewall, honeypot, virtual machines, daemon, behavioural analysis, challenge response, virtual network, flooding, crashing, intrusion detection, router, honeywall, honeymesh.

I) INTRODUCTION

Slowly-Increasing Polymorphic DDoS Attack Strategy (SIPDAS) can be applied to several kind of attacks, that leverage known application vulnerabilities, in order to degrade the service provided by the target application server running in the cloud [1]. Energy-efficient hardware components, which are able to adapt their energy demand to the effective workload. In doing this, they dynamically switch between several operating states characterized by a reduced/increased component performance as a counterweight of a lower/higher degree of power consumption [2]. Time series anomaly detection has been a critical research topic in the domain of data analysis for decades. It has been widely applied to various areas related to the pro cessing of sequential datasets [3]. A more secure way is to use two-factor authentication (2FA). 2FA is very common among web-based e-banking services. In addition to a username/password, the user is also required to have a device to display a one-time password [4]. Virtualization, the basis for most CCSs, enables CSPs to start, stop, move, and restart computing workloads on demand. VMs run on computing hardware that may be shared by cloud tenants [5].

This paper, discusses five different strategy such as Slowly-Increasing- Polymorphic DDoS Attack Strategy (SIPDAS), LOW-RATE E-DDOS STRATEGY, Vector Data Description (SVDD), Fine-grained two-factor access control protocol and Trust service-oriented workflow scheduling (TWFS). But these strategy also have some problem so to overcome such problems improve version of mobility scheme is proposed here that is **"Intrusion detection and prevention using Honeypot technique".**

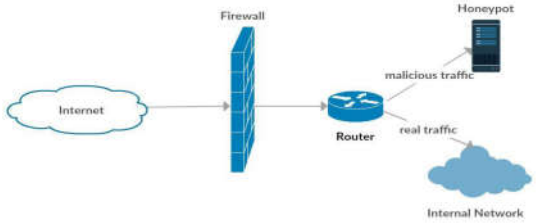

Fig.1. Basic Honey pot design

II) BACKGROUND

Many studies on services models have been done to develop the service scheme in recent past years. Such services are: Slowly-Increasing- Polymorphic DDoS Attack Strategy (SIPDAS) can be applied to several kind of attacks, that leverage known application vulnerabilities, in order to degrade the service provided by the target application server running in the cloud [1]. LOW-RATE E-DDOS STRATEGY effective e-DDoS strategy, the attack pattern should be indistinguishable from normal traffic and should be specifically designed in order to leverage the cloud flexibility. In particular consider that cloud applications are able to self-scale by dynamically increasing or reducing the amount of resources needed, depending on the users' requests [2]. Vector Data Description (SVDD) is investigated for time series anomaly detection in cloud computing systems to assure service trustworthiness. Generally speaking, SVDD is a promising and popular method for achieving efficient, accurate, and interpretable anomaly detection. Its popularity is mainly owing to the fact that it is a non-parametric sparse model, which naturally supports multivariate one-class classification [3]. Fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant [4]. Trust service-oriented workflow scheduling (TWFS) model is an NP-hard problem.WFS usually requires certain policies like LOSS, GAIN, and deadline-Markov Decision Process (MDP) to balance different and conflicting requirements such as time, cost, and trust at the same time in the cloud environment [5].

This paper introduces five cloud service strategies ie slowly-Increasing- Polymorphic DDoS Attack Strategy (SIPDAS), LOW-RATE E-DDOS STRATEGY, Vector Data Description (SVDD), Fine-grained two-factor access control protocol and Trust service-oriented workflow scheduling (TWFS) these are organizes as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on cloud services models. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III) PREVIOUS WORK DONE

Massimo Ficco et al (2015) [1] have proposed Slowly-Increasing- Polymorphic DDoS Attack Strategy (SIPDAS) validate the stealthy characteristics of the proposed SIPDAS attack explore potential solutions proposed in the literature to detect sophisticated low-rate DDoS attacks. Show that the proposed slowly-increasing polymorphic behaviour induces enough overload on the target system (to cause a significant financial losses)

Massimo Ficco et al (2017) [2] proposed LOW-RATE E-DDOS STRATEGY effective e-DDoS strategy Typical e-DDoS attacks aim at exploiting such feature, by taking advantage of such elastic behaviour in order to make the associated energy demand economically unsustainable. An attacker can inject a legitimate low-rate attack traffic flow, which will be able of originating a fraudulent increment in the overall energy consumption as a consequence of an unnecessary scale-up of resources.

Chengqiang Huang et al (2017) [3] have proposed the Support Vector Data Description SVDD (LPSVDD) is formulated and relaxed for detecting anomalies in time series; To ensure that the relaxed LPSVDD (RLPSVDD) is practical for anomaly detection,

Author have presented important insights into the selection of its parameters.

Jaseph K. et al (2016) [4] has proposed fine-grained attribute-based access which provides a great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user.

WenAn Tan et al (2014) [5] has proposed specific scheduling strategies to effectively optimize time, cost, and trust factors in ES. In order to address the problem of WFS in an optimal and reliable way, a TWFS model is proposed to meet the requirements of ES integration. Trust service-oriented workflow scheduling (TWFS)

IV) EXISTING METHODOLOGIES

A Slowly-Increasing- Polymorphic DDoS Attack Strategy (SIPDAS)

In order to validate the stealthy characteristics of the proposed SIPDAS attack, that explore potential solutions proposed in the literature to detect sophisticated low-rate DDoS attacks. Show that the proposed slowly-increasing polymorphic behaviour induces enough overload on the target system (to cause a significant financial losses), and evades, or however, delays greatly the detection methods.

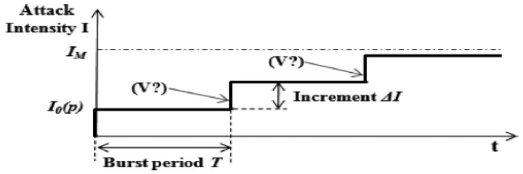

Fig.2. SIPDAS lowly-increasing intensity behaviour

I 0(p) means the initial attack intensity at the iteration p, T is the length of the burst period, and I is the increment of the attack intensity each time a specific condition V is false.

B LOW-RATE E-DDOS Strategy

Low-rate attacks to be effectively launched against very large cloud organizations, exposing several thousands of front-end servers that are the main targets for e-DDoS activities. Furthermore, since botnets have been explicitly conceived to operate within hostile environments, they natively provide the needed invisibility in achieving their specific goals.

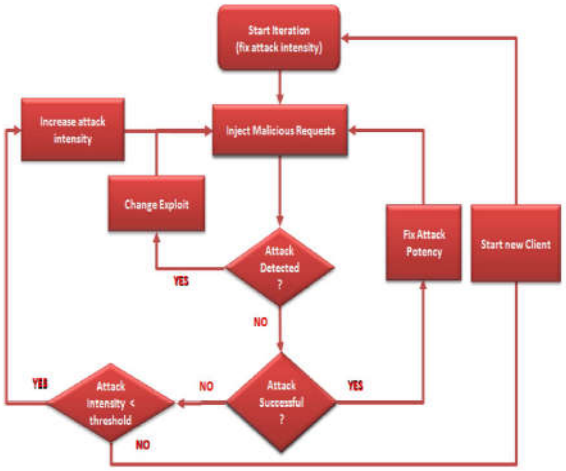

Fig.3. Attack algorithm

C Support Vector Data Description (SVDD)

SVDD is essentially a one-class classification or data description method that features a nonparametric model without requiring the knowledge of explicit data distribution. The existence of the sparse support vectors in SVDD enables a computationally efficient decision function for online anomaly detection. The essentials of LPSVDD lie firstly in the problem formulation. Intuitively, to describe a dataset, LPSVDD considers that the data instances in an enclosing ball aim to move away from the center as far as possible

$$\min_{a,R^2} \quad \sum_i \left(-\|\phi(x_i) - a\|^2 + R^2\right)$$
$$\text{s.t.} \quad \forall i, \quad \|\phi(x_i) - a\|^2 \leq R^2.$$

D Fine-grained two-factor access control protocol

Fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the

following properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside. Fine grained two factor access control based on attribute based cryptosystem.

E Trust service-oriented workflow scheduling (TWFS)

Trust plays an important part in e-commerce. Thus, building trust is also essential for cloud service providers. WFS require policies to strike a balance for the different requirements. For example, enterprise may expect to save budget but have longer time, or aim to minimize the execution time of schedule. In order to satisfy the multiple criteria simultaneously, a compromise should be made to find a suitable solution.

Input: request processing time, cost, and trust value
Output: A workflow schedule strategy for Enterprise Information Systems
1: request processing time, cost, and trust value from available service $\forall T_i \in T$
2: repeat
3: compute the indegrees for $\forall T_i \in T$
4: while !stack.isEmpty() do
5: forall s in available services of the ith task do
6: compute $\lambda_k = \max\{\sum_{j=0}^{2} U_{Z_j(x)}^{T_i} * w_j\}$
7: end for
8: Mapping service S_k onto the ith task
9: forall edge e in adjacent do
10: vertices of the ith task
11: vertex w = e.dest
12: if w.indegree == 0 then
13: insert w into stack
14 end if
15: end for
16: end while
17: until all tasks have been scheduled

V) ANALYSIS AND DISCUSSION

The Slowly-Increasing Polymorphic DDoS Attack Strategy shows that more accurate than traffic based technique and it maintained flexibility of the system. It aims at exploiting the cloud flexibility, forcing the services to scale up and consume more resources than needed [1].

LOW-RATE E-DDOS STRATEGY Flexible and transparent infrastructure requests from the legitimate traffic, by using a comprehensive security solution that considers energy-related aspects as a fundamental part of its monitoring focus e-DDoS attacks do not have easily appreciable impacts on the availability of the services provided by the victim organization [2].

Support Vector Data Description (SVDD) investigated for detecting anomalous performance metrics of cloud services. RLPSVDD solves a linear programming problem to provide a flexible data description for time series anomaly detection [3].

Fine-grained two-factor access control protocol provide a great flexibility for the system to set different access policies and highly confidential. Presented 2FA access control system for web based cloud computing services [4].

Trust service-oriented workflow scheduling (TWFS) Improve security using Trust service oriented scheduling model Improve the Trust metrics that combines direct trust and recommendation trust. Effective and feasible [5].

Mobility scheme	Advantages	Disadvantages
Slowly-Increasing-Polymorphic DDoS Attack Strategy	1. More accurate than traffic based technique 2.Maintain Flexibility	Performance is degradation.
LOW-RATE E-DDOS STRATEGY	These techniques must be able to effectively recognize and isolate malicious service requests from the legitimate traffic.	e-DDoS attacks do not have easily appreciable impacts on the availability of the services provided by the victim organization.
Support Vector Data	RLPSVDD solves a linear programming	1. High false alarm rate. 2. Huge

Description (SVDD	problem to provide a flexible data description for time series anomaly detection	computational complexity.
Fine-grained two-factor access control protocol	1. Provide a great flexibility for the system to set different access policies. 2. Highly confidential.	Lack of efficiency.
Trust service-oriented workflow scheduling (TWFS)	1. Improve security using Trust service oriented scheduling model 2. Improve the Trust metrics that combines direct trust.	It requires advancing collaborative model in response to changes cloud computing environment.

TABLE 1:Comparisons between different mobility models.

PROPOSED METHODOLOGY

"Intrusion detection and prevention using Honeypot technique"

The proposed solution is to create a network of virtualized honeypots within the existing infrastructure with minimal cost and maintenance overheads. The existing security infrastructure consists of services such as ftp, mail, web and DNS that are offered to the outside world through a demilitarized zone (DMZ) DMZ consists of two firewalls. The first firewall is meant to protect these servers from external malicious traffic while the second one is an internal firewall meant to protect the organization's internal network. The two firewall approach provides multiple layers of protection to the internal network. In addition to this, other security mechanisms such as encryption, host based intrusion detection systems, vulnerability scanners are used to bolster protection. Further, the organization might choose to add further protection to its local services using a virtual private network (VPN). Honey VM's have security mechanisms similar to the real servers but some vulnerabilities are deliberately exposed so as to lure the attacker into a trap. These VM's continuously monitor the incoming traffic for potential malicious activities and once an attack is discovered. This ensures that malicious traffic doesn't reach the production servers.

Detection of an Attack

Honeypot VM's in the honey farm employ machine learning algorithms to perform a behavioral analysis of incoming traffic Since each production server receives different types of requests, appropriate honey VM's can be tailored for the corresponding servers. For example, one honey VM can analyze web server traffic while another can examine file server requests.

Preventing Flooding Attacks

Once an attack is discovered, the routing information in the internal routers is modified so as to redirect all incoming traffic from the attack source to the honey farm. Since malicious traffic now flows to the honey farm, it ensures that the production network is shielded from flooding attacks. Honey VM's in the farm keep the attacker engaged through a set of challenge-response queries further slowing down the attacker **"Intrusion detection and prevention using Honeypot technique".**

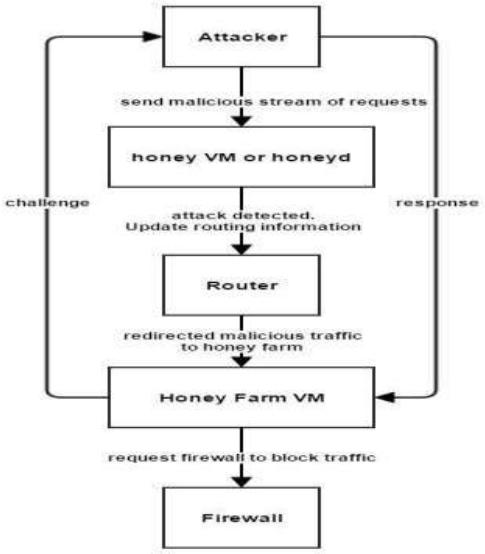

Fig.4. Honeymesh sequence flow

Algorithm

If Attack occurred:
Step 1 attacker send malicious of requests to honey VM or honeyd
Step 2 If attack detected
Then update routing informations

Step 3 Router re-directed malicious traffic to Honey farm
Step 4 Honey Farm VM send request to firewall for Block the traffic

OUTCOME AND POSSIBLE RESULT

Honeypots are implemented as virtual machines and daemon processes rather than actual physical servers; this solution is economical and has low maintenance costs. The mesh of honey VM's and daemons provides multiple layers of security against DDoS attacks. Even if honey VM's in the honey farm miss out a possible attack, it can be caught by honey-d's running on individual servers. This authentication provides enhanced security to the production servers. The proposed method "Intrusion detection and prevention using Honeypot technique" will be successfully improve.

VII) CONCLUSION

Distributed denial of service (DDoS) attacks are dangerous and can potentially render the production site unusable either by flooding the server network with thousands of malicious requests or crashing the server by exploiting the vulnerabilities in its software. Several solutions have been proposed to deal with DDoS attacks. However, these solutions are either expensive due to usage of multiple physical servers for honeypots or do not successfully address the issue of flooding type of DDoS attacks. The new solution proposes to create a virtual network or mesh of honeypot VM's and honey daemon processes to provide multiple levels of security checks and intrusion detection using behavioural analysis and challenge response models.

FUTURE SCOPE:

Although production servers and organization's internal network (LAN) are fully protected, there should be a mechanism to protect the organization's routers from being flooded with malicious requests. Honeypot VM's may be hosted on a network of servers to create a more robust honey farm. Currently, all VM's in the honey farm are hosted on a single server to reduce maintenance and recovery costs. In future work to further improve the efficiency while keeping all nice features of the system

REFERENCES

[1] Massimo Ficco and Massimiliano Rak, "Stealthy Denial of Service Strategy in Cloud Computing," IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL 3, NO.1, 1 JANUARY-MARCH 2015.

.

[2] Massimo Ficco and Francesco Palmieri, "Introducing Fraudulent Energy Consumption in Cloud Infrastructures: A New Generation of Denial-of-Service Attacks," IEEE SYSTEMS JOURNAL, VOL. 11, NO, JUNE 2017.

[3] Chengqiang Huang, Geyong Min, Senior Member, Yulei Wu, Member, Yiming Ying, Member, Ke Pei, and Zuochang Xiang, "Time Series Anomaly Detection for Trustworthy Services in Cloud Computing Systems," TRANSACTION ON BIG DATA, VOL. *, NO. *, *,2017.

[4] Joseph K. Liu, Member, IEEE, Man Ho Au, Member, IEEE, Xinyi Huang, Rongxing Lu, Senior Member, IEEE, and Jin Li, "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO.3, MARCH 2016.

[5] Wen An Tan, Yong Sun, Ling Xia Li, Gang Zhen Lu, and Tong Wang, "A Trust Service-Oriented Scheduling Model for Worflow Applications in Cloud Computing," IEEE SYSTEMS JOURNAL, VOL. 8, NO. 3, SEPTEMBER 2014.