International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 5 Sep.-Oct. 2017 p-ISSN: 2394-8280

A SURVEY TO ANALYZE THE IMPACT OF DDOS ATTACK ON CLOUD COMPUTING ENVIRONMENT

Durgesh Kumar Patel[1], Prof. Sumit Nigam[2]
Mtech Scholar, Assistant Professor & HoD
Computer Science & Engineering Department, Sanghvi Institute of Management & Science, Indore (M.P.)

ABSTRACT
The privacy is primary requirement of growing technology. Maintaining Isolation over sensitive data in public environment is a big challenging task. It becomes more complex when data set becomes very large and number of users reaches to huge figure. Subsequently, cloud computing is one of the growing technology which is shifting the complete technical world into cloud environment. Public cloud computing is one of the major primary atmosphere consider as the most targeted field of attackers to degrade the server and network performance. DDOS attack is one of resource draining attack can be applied without the having the knowledge of infrastructure. This works aim to explore a mitigation technique to defend DDOS attack and save cloud server from intentional draining. It also aims to keep privacy and safety of content along with storage.

Keyword: DDOS attack, Cloud computing, Packet Classification and Mitigation

1. INTRODUCTION

The enhancement in technology is changing the practice of human. Development of industry without computer and use of computer without internet is a joke today. Internet based services and applications are rapidly emerging and increases demand to upgrade applications and existing solutions. Internet based large storage and services is known as cloud computing. Cloud computing services often rely on specific systems such as Hadoop Map Reduce, an open source proposed by Google. Map Reduce is being adopted by many academic researchers for data processing in different research areas, such as high-end computing, data intensive scientific analysis, large scale semantic annotation and machine learning.

A big challenge of preserving privacy and security in cloud computing is that developers and users wanted to spend as little effort and system resources on security as possible. Therefore, motivation of this research is how to design a system that satisfies below demands.

1. Enables efficient distributed computations

2. Provides privacy's enhancement to results.

3. Supports a friendly usability that users can write

Cloud computing technology is seen as the collection of internet based services for better utilizing the resources and services. It is the new utility which provides virtualization, parallel and distributed computing into single unit. It implies the sharing of resources to handle applications with reduces capital and low maintenance cost. It gives increased scalability and ease of access feature with low complexity.

2. LITERATURE REVIEW

Hussain, M. et. al.[1] presented a new algorithm for a research honeypot, by utilizing it as an exploration instrument to study and distinguish the dangers on the internet. Results are encouraging and feel that the next level of collaboration should be considered. This study requires to be expanded. To expand on this research, the next step should be to build an execution framework with an alternate recognition procedure with some optimization problems as an example.

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 and research honeypot. Handling honeypot are use 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 their behavior.

This study proposes a framework referred as a covariance matrix mathematical model. It has two stages:

1) Training and monitoring stage

2) DDoS detection and prevention stage

3. DISTRIBUTED DENIAL OF SERVICE

Denial of Service attack or Distributed Denial of Service attack is kind of resource draining attack where multiple compromised nodes attempt to exhaust the resources of one targeted node without considering the vulnerabilities of routing protocols. Study of another security threats conclude that DDOS wormhole, blackhole kind of attacks can only be deployed by exploiting the vulnerabilities of routing protocols such as shortest path selection or routing table update. Beside these circumstances,

DDOS attack exploits the limitations of infrastructure and exhausts the resources by generating huge load and initiating redundant communication.

Study concludes that objective of this attack is to degrade the performance and quality of services by exploiting either protocol level vulnerabilities or forcing the victim node to compromise by overwhelming processing. Another words, DDOS attack attempt to exhaust the resources such bandwidth, buffer, battery or processing unit by creating huge number of packets. Impact of such irrelevant and unnecessary activity creates wastage of resource capability. This flooding not only reduces node working capability but also reduce the life of node. A block diagram of such DDOS attack is shown in Figure 3.

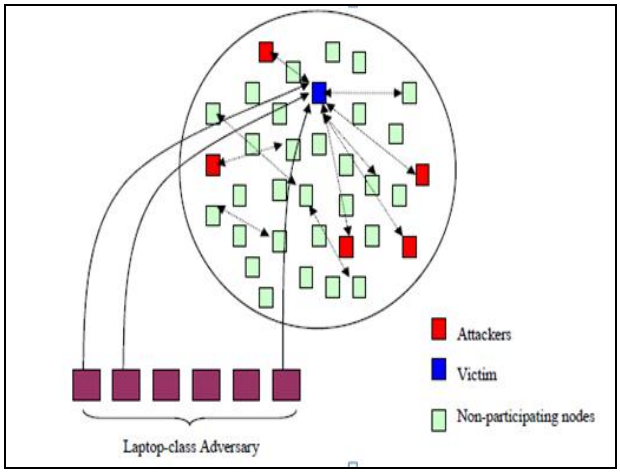

Figure 1: Distribute Denial of Service [DDOS]

Study observes that DDOS attack can be classified into three categories which are listed below;[5][6]

1. Application DDOS attack
2. Protocol DDOS attack
3. Volume DDOS attack

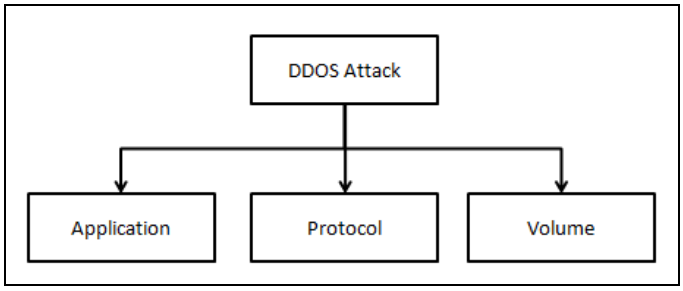

Figure 2: DDOS attack Classification

4. PROBLEM DOMAIN

"Privacy is a state in which one is not observed or disturbed by other people" Privacy protection policy is an approach to isolate the sensitive information from unauthorized

access. The complete work concludes that Cloud Framework does not consist security policy and suffering with data leakage problem and DDOS attack.

Subsequently, Security threat attack is also possible and malicious framework may give open system access to unauthorized user. Furthermore, DDOS can lead to vampire attack or another resource draining like jellyfish attack to collapse the communication.

The complete study observes certain problems can be listed as below;

1. Cloud computing doesn't have any significant solution to mitigate DDOS attack or resource draining attacks into public cloud environment.
2. Current solution only creates a simulated environment and evaluated as the network scenario not like actual cloud computing environment.

The complete phenomena generate a problem to implement security policy with actual

5. SOLUTION DOMAIN

Security is the one of the major concern for any network. Cloud computing also suffers with the issue of security and privacy. Proposed solution would use packet capturing and classification technique to observe the current status of the network. Usually, attackers like to use UDP packet to create conjunction into network along with at server end to degrade the performance as well create jam at server end. Similar patterns are used to waste the bandwidth and power draining into other networks.

This work will use Classification technique to classify all incoming packets at server end and observe the malicious activity by misleading packet pattern such continuous bombarding of same message from same node.

To classify the packet Custom classification technique would be developed inspired from Naïve bysien classifier. The complete work can be described in following steps.

1. Initially, performance observation of normal communication will be implemented and performed.

2. A java based tool will be developed to flood large amount of packets in UDP format to drain the server and network resources.

3. This activity would not only degrade the performance but would also create jam at server end. The complete phenomena would create denial of services activity.

4. To diagnose the malicious activity, a continuous monitoring system will be developed as intrusion detection system, which will monitor each and every activity of network.

5. This monitoring tool would capture packet traces after a fix periodic time period.

6. A java based diagnosis module would help to classify the all traced packet and capture the communication. In case of very consistent message type from same computer node with high latency would be an symptoms for malicious activity.

7. Afterwards. Detection and prevention mechanism would detect the origin of the packet by extracting the payload of any of traced packet.

8. Prevention mechanism will force server machine to block the respective computer node to safe the services and network.

9. The complete philosophy will help to detect and prevent DDOs attack in cloud computing environment.

10. A Java technology and Private cloud deployment with Open Stack solution would be used to implement and evaluate the proposed solution.

6. CONCLUSION

The complete work concludes that DDOS is one of the severe security threats and it may be apply to drain the quality of communication. This works aims to implement a DDOS attack and explore technique to mitigate the same.

References

1. Hussain, M. et. al. "*Data Security Analysis for DDoS Defense of Cloud Based Networks*" published in IEEE Data Security Analysis for DDoS Defense of Cloud Based Networks, 2015

2. Tran, Q. and Sato, H. "*A Solution for Privacy Protection in MapReduce*" published in IEEE 36th International Conference on Computer Software and Applications available on IEEE-Computer Society.

3. James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers "*Big data: The next frontier for innovation, competition, and productivity"*. McKinsey Global Institute. 15 May 2011.

4. Shilpa and Manjit Kaur " BIG Data and Methodology-A review" International Journal of Advanced Research in Computer Science and Software Engineering