# Securing Data Against Botclouds and IP Spoofing

Usha L[1], Chidananda Murthy P[2]
[1]M.Tech, Dept. of CSE, SET, Jain University
[2]Assistant Professor, Dept. of CSE, SET, Jain University

***ABSTRACT*- Cloud computing is the new trend in computing and resource management. Cloud offers great benefits in terms of flexibility, scalability and availability. Few people and organizations step back from adapting cloud technology mainly because of the security concerns. The security breaches of cloud computing include DoS attacks. BotClouds and IP Spoofing are two DoS attacks. Traditional network security techniques cannot be used to solve cloud computing threats because of the huge and variety of data in cloud. IP spoofing is presenting a false truth in a credible way to gain unauthorized access to cloud services. BotClouds are cloud based botnets which is the most commonly used platform attackers use to perform frauds in cloud environment. This paper proposes a methodology to secure cloud services by monitoring the traffic and logging the activities even for short periods.**

***Keywords: IP Spoofing, BotClouds, DoS attack, Cloud computing***

## I. INTRODUCTION

Moving data to a Cloud environment presents an opportunity to achieve tremendous cost savings compared to the cost to purchase an equivalent amount of data for a locally hosted data center. As with virtual machines, a customer's data is stored over a shared infrastructure that may be distributed throughout multiple Cloud data centers. Adequate security measures must be in place to ensure unauthorized users cannot access data either intentionally or accidently. One of the potential draw backs of moving data processing to a Cloud environment is losing direct control Monitoring at the OS or VM level is a basic means to monitor your systems but to closely monitor attacks tools such as an Intrusion Detection System (IDS) should be used. It is essential for the cloud service providers to maintain the data security to its clients for cloud computing and internet to reach their full potential. Inefficient data security measures will reflect on the cloud performance and reputation of the cloud provider. Clients expect their data and applications stored in cloud to remain private and secure. As the challenges of security and privacy are evolving along with cloud, security is responsibility of both the customer and the service provider.

IP spoofing is a technique used to gain unauthorized access to cloud services where by the attacker sends a request with a forging IP address [10] indicating that the request is coming from a trusted host. Many cloud applications use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed Attacker puts an internal or trusted IP address as its source IP address [13]. The cloud sees the IP address as trusted and lets it through. A hacker uses a valid IP addresses.

BotClouds are cloud based botnets [1]. Bots are collection of scripts that perform automated tasks in cloud. Rather than use a network of infected machines, Bots use Cloud services to build BotCloud.Botmasters registers to the CSP and introduce bots to the applications and data hosted on cloud. Bots cannot be noticed [5] easily because they perform tasks as similar to humans but at a higher rate than humans. Hence it is difficult to detect bots using an intrusion detection system (IDS), so it is appropriate to detect bots based on their behavior [4]. Bots are frequently used to launch DoS attacks [6].

## II. RELATED WORK

Surveys from Gartner [9] have shown that security is the main obstacle in cloud computing [3]because of which organizations do not adapt to cloud computing. Main reason for this is cloud computing facilitates the storage of data at remote site to maximize resource utilization. Bots act safe and are hidden as long as possible and they are easy to establish when compared to a traditional botnets. Firewalls are inefficient in preventing and detecting bots. Hence active monitoring of network traffic of anomalous activity is suitable to detect bots. A DoS attack can be launched by a BotCloud. Botnets bring down relatively unprotected websites just be directing thousands of traffic requests. DoS attack is accompanied by IP Spoofing so as to hide the source of flooding and to make every request look different. Source IP spoofing attacks are critical issues to the Internet. These attacks are considered to be sent from bot infected hosts.The cloud security alliance has initiated research group called Anti-Bot Working group to detect bot attacks on cloud using new and efficient methodologies. Cloud Security Alliance has also

mentioned threats to Cloud Computing [11] which includes BotClouds and IP Spoofing attacks.

Traditional security technologies lack the sophisticated capabilities and visibility required to detect and protect cloud data from attacks in real time monitoring of cloud, there is a need to analyze who is accessing which data from which resource at what time Or do we have a breach of compliance standard C because of action A? Traditional network security techniques [12] for detecting Bots and IP spoofing are inadequate to solve cloud attacks because

- Traditional tools were not designed to analyse and manage huge amount of data.
- Though traditional network security systems collect logs and events from a huge variety of systems they cover only a part of potentially relevant activity.
- Detection of threat relies on having signatures or knowing methods of attack in advance.

CAPTCHA- Computer Automated Public Turing test to tell Computers or Human Apart are used to differentiate between human and bots. They are used to prevent bots but recent surveys have reported that Captchas can be easily cracked by using advanced character and pattern recognition software's [14]. Websense security Labs have reported that Windows Live Captchas can be cracked in as little as 60seconds. Captchas are not a good choice because they are difficult for blind andpartially sighted people and bad Captchas are easy to decode where as good Captchas are difficult to decode.

## III. PROPOSED WORK

The proposed architecturesintend to detect requests from Spoofed IP addresses and detect Bot activity by continuous behavior based monitoring.

### *A. SPOOF DETECTION*

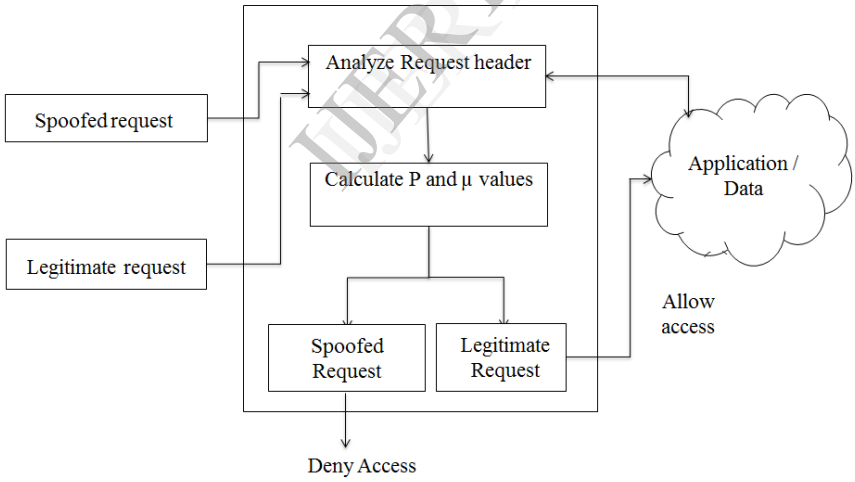


Fig.1 Proposed architecture to detect IP Spoofing

Spoofing the IP in cloud is done by customizing the HTTP header by manipulating the original source address IP with the forged IP address while sending the request to access the cloud data. The X-Forwarded-For is a HTTP header field to identify the originating IP address of a client connecting to a web server. This field can be forged to spoof the IP address and send requests. The X-Request-Start is a filed in the http header which holds timestamp at which the request was created.

The spoof detection module examines the HTTP header and detects the IP address in the header. It also examines for time the request was created and the time at which the request has reached the destination. According to the ANT algorithm to detect IP spoofing, legitimate packets choose the shortest route and reach the destination in less time where a spoofed packet does not take the shortest route and hence takes more time to reach the destination.Pheromone is the increase in possibility of choosing a path based on the number of requests previously chose the path

The X-Request-End time, X-Request-Start time, and the ping time is calculated for each arriving request. The difference of the X-Request-End and X-Request-Start is the time taken by the request to reach the destination. Then the Ping time and time taken is calculated as Difference in time. Initially the Pheromone is set to 0. If the Pheromone value (P) is 0, the difference in time value obtained is set as the pheromone value else the average of existing Pheromone value and Difference in time is set as the updated Pheromone value.The requests are categorized as Spoofed (µs) or legitimate (µleg). The request from Spoofed IP address is denied and the request access from legitimate IP address is granted.

*B. BOT DETECTION*

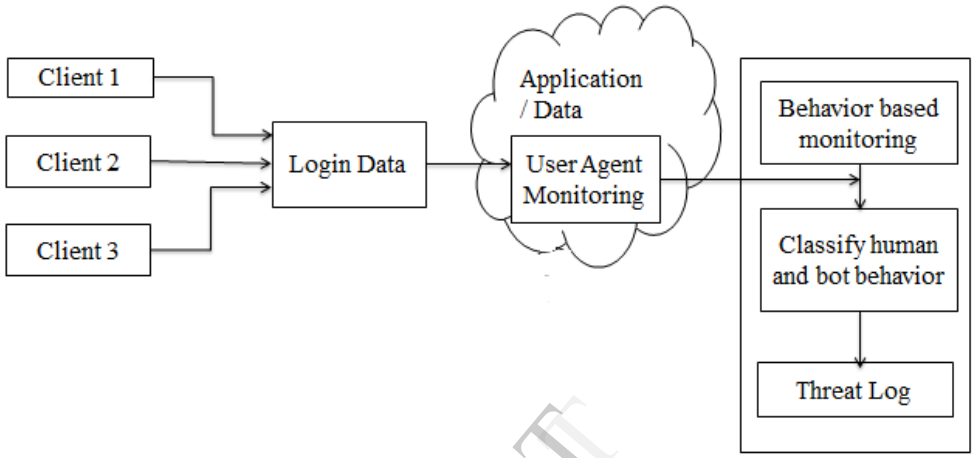


Fig.2 Proposed architecture to detect Bot activity in cloud



A traditional botnet requires substantial time to build, whereas a BotCloud can be online in minutes. The bots enter the cloud from any of the client machine, hence continuous monitoring of the network traffic is necessary to detect threats in cloud [2]. Bots attack the application by performing fraud activities at a very faster rate than humans. It is difficult to detect bots hence the details of the user agents like operating systems, browsers are also stored. The network traffic generated by activities on the cloud are monitored based on action time and action frequency[7] for parameters like number of clicks, file requests, failed requests html to image ratio and many more. The activities which generate abnormal network traffic and the user agents logged in are joined together to find out the IP address of the client from which bots are entering the cloud. The log of IP addresses is maintained and if the administrator wishes, an information email can be sent to the user logged in from the infected IP address.

## IV. RESULTS

The proposed methodology, which monitors the traffic generated by applications, hosted on cloud continuously, rather than monitoring the past traffic patterns are better. The Spoofed IP is detected by examining the HTTP header and categorization of spoofed and legitimate request is done based on time factor i.e. the time taken for the request to reach the destination. The administrator has an option ofinforming the clients about the suspicious activity detected from the clients IP address through email.

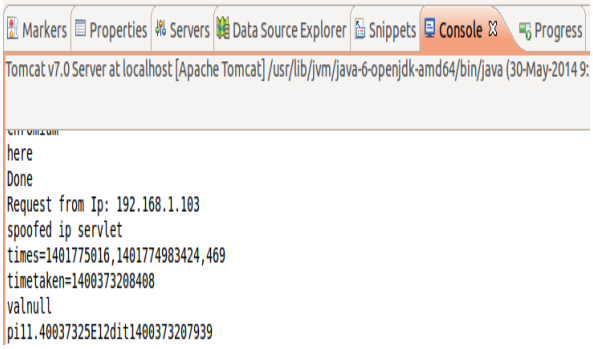


Fig.3 Detection of Spoofed IP

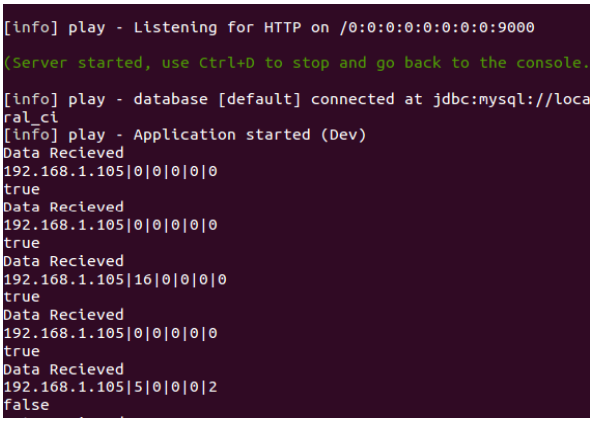


Fig.4 Continuous traffic monitoring for bot activity

## V. CONCLUSION AND FUTURE ENHANCEMENT

The proposed methodology detects, request from spoofed IP address and the presence of bots in the cloud. The user agent's properties are stored to track the client's. Currently monitored bot activities are click frauds and frequent inappropriate data submitted in the form. The IP address from which bots are entering are detected and logged in the database. The administrator can view the infected IP address and sends an information email to the user regarding malicious activity. The existing work can be extended to monitor more complex bot activity such as ban enforcement activity which finds and reverts changes, automatic importer by request for all types of document formats which has the same content.

## REFERENCES

[1] Kassidy Clark et al., "BOT-CLOUDS - The Future of Cloud-based Botnets", 2010.
[2] Mr. D. Kishore Kumar et al., "Cloud Computing: An Analysis of Its Challenges & Security", in IJCSN, 2012.
[3]Sateesh Kumar Peddojuet.al.,"Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing", in IJCSEE, 2012.
[4] Shun-Wen Hsiao, Yi-Ning Chen, "A Cooperative Botnet Profiling and Detection in Virtualized Environment", in IEEE, 2013.
[5] Keith Harrison1, BehzadBordbar, "A framework for detecting malware in Cloud by identifying symptoms", IEEE, 2012.
[6] MatijaStevanovic Jens Myrup Pedersen, "Machine Learning Based Botnet Detection", 2013.
[7] PedramHayatiet.al, "Behavior-Based Web Spambot Detection by Utilizing Action Time and Action Frequency", Springer, 2010.
[8] Kuochen Wang,et al., "A fuzzy pattern-based filtering algorithm for botnet detection, Elsevier journal", 2011.
[9] NarayananArumugam and Venkatesh, "Triangular fuzzy based classification of IP request to detect spoofing request in data network" academic journal of International Journal of Physical Sciences, 2013
[10].http://www.proofpoint.com/solutions/threat-management.php
[11].http://www.mediabuzz.com.sg/asian-emarketing/march-2011/1230-poofing-attacks
[12]https://cloudsecurityalliance.org/research/big-data/
[13]http://www.bankinfosecurity.com/webinars/unknown-threats
[14]https://blogs.oracle.com/vreality/entry/public_cloud_security_anti_spoofing2
[15]http://arstechnica.com/security/2008/04/gone-in-60-seconds-spambot-cracks-livehotmail-captcha/