ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/107975, December 2016* ISSN (Online) : 0974-5645

Intrusion Detection and Prevention using Lockout policy with ACL on Cloud Computing

D. Narmadha, P. Padmakumari*and A. Umamakeswari

School of Computing, SASTRA University, Thirumalaisamudram, Thanjavur - 613401, Tamilnadu, India;
narmadhadamodaran@gmail.com, padmalec.sastra@cse.sastra.edu, aum@cse.sastra.edu

Abstract

Background/Objectives: Cloud computing supports many enterprise and government organizations in business perspective due to its advantage such as high scalability and high flexibility. However, despite potential gains that can be achieved, security is fundamental issue. Denial of service attack attempted by attacker to exhausts the resources available to a network, application or service. The orchestrated flow of attack patterns by attacker affect the customers in terms of financial cost cause service inability to legitimate users, attacker overloads target system with massive amount of request, which results in loss of equipment resources affecting network bandwidth. **Methods:** To address this issue, the proposed lockout policy with access control list is applied to prevent the access to illegitimate user without affecting legal users. **Findings:** The proposed technique helps in differentiating legitimate and illegitimate users. The attack can be controlled by locking out malicious user access. Thereby the financial cost can be controlled by preventing the resource consumption by malicious node. Applications The proposed methodology can be applied in signature based analysis and strong user identification. There by providing security by building Anti-spam devices at customer site such as E-commerce application. **Applications:** The proposed methodology can be applied in the signature based analysis and strong user identification. Thus providing security by building Anti-spam devices at customer site, such as in an e-commerce application.

Keywords: Access Control List, Attack Pattern, DDoS, DoS, Lockout Policy, Service Inability

1. Introduction

Cloud computing is on demand computing provides shared processing of resources and data to devices on demand. Since cloud computing is a pay and use model, it provides Quality of Services (QoS)[1] for paid customers on basics of SLA. Such models experience Denial of Service (DoS) Attack and Distributed Denial of Service (DDoS) Attack. Those attacks generate orchestrated flow of attack patterns[2] towards targeted application, services or networks. During this attack the resources like Bandwidth, Memory and Processing resources can be depleted. There by performance of the system is degraded by these attacks. Other major advantage of cloud computing is auto-scaling and load balancing. In the case of DoS attack the malicious request is also injected along with authorized request. If job size of arrived malicious request is more the auto-scaling and load balancing features of cloud deplete more resources and affect the customers on increasing financial cost. To address this issue the collaborative Lockout policy with Access Control List is used (ACL).

1.1 Lockout Policy

Lockout policy acts as physical barrier to malicious user from accessing available processing resources, network bandwidth and application. Thereby unwanted resource consumption can be avoided which results in effective performance.

1.2 Access Control List

ACL is a powerful security feature which helps in filtering unwanted traffic while entering or leaving interface. There are two types of ACL: Inbound ACL and Outbound ACL. In Inbound ACL the packets are processed before routing. In Outbound ACL, the packets are routed to outbound interface and then processed by ACL.

* *Author for correspondence*

2. Related Work

Triton, a high level language policy is a common access management middle layer, provides authorization policies to administrate all sub-networks under large-scale networking[3]. Intrusion plays a major role in network security. Prevention of intrusions at businesses and homes can be done by router configuration. By making use of Snort IDS, a system has been developed where alerts are entered into a database and it generates ACL rules. Then these rules are configured to prevent intrusions[4]. ACL is used to provide security in many devices for new vulnerabilities and threats that might occur. ACL can be compressed by an approach called Diplomat. It splits original pattern of dimensions into a pattern of lower dimensions with series of hyperplanes and uses the rules to identify difference between two hyperplanes[5]. The on-demand, self-service, pay and use nature of cloud, is prone to DoS attacks which results in over consumption of resources. The orchestrated flow of attack patterns affect the quality of delivered services and affect the financial aspects of cloud customers with increased job size and service arrival rate[6]. Authenticated key is used to exchange the important information via the Internet. The exchange of secret key is based on Diffie-Hellman exchange of key value with one-time ID that provides security while exchanging information[7]. Intrusion detection and prevention can be done by using a traffic analyzer called Bro Traffic Analyzer, which provides elastic and dynamic provision of resources, a simple algorithm for detecting DoS attacks, handling DoS attacks and deducting the attacks even in multi-tenants infrastructure[8]. In processing big data, decision making analysis and innovative processing are needed because a variety of structured and unstructured data from different sources need to be processed, which makes use of a simple authentication algorithm called one time pad model. Thus parallel processing of voluminous data with enhanced security is achieved.

[9]Cloud computing is a pooling framework for resources which delivers more reliable services, which reduces initial investment on setting up infrastructure, training cost, operational cost and software cost by using multi factor authentication[10].

3. Proposed System Model

Triton, a high level language policy is a common access management middle layer, provides authorization policies to administrate all sub-networks under large-scale networking[3]. The proposed model designed with three modules namely Cloud provider, Cloud customers and Cloud users. Cloud providers provides the services to cloud customers based on Service Level Agreement (SLA). The users can makes use of the cloud storage with the help of cloud customers. In the case of business environment or educational enterprises the cloud storage is very useful in reducing the physical storage of data.

In a business scenario, the cloud customer acts as the administrator which provides storage space from cloud storage provider based on SLA, and maintains ACL for different hierarchy of users. The list of users stored in ACL is considered as valid users and services are provided to them by matching a shared secret key provided by the administrator. If the shared secret key of the admin does not match, the lockout policy is used to prevent malicious users from accessing the cloud. The security is then preserved by collaborating the lockout policy with ACL (shown in Figure 1). The proposed model of lockout policy with ACL helps in classifying authorized users from malicious users and denies access to a malicious node. Thus the resources consumed by malicious nodes are reduced. Request from both authorized cloud user and intruder is sent to a service request queue, where filtration of DoS attack is done. The legitimate request is processed and service is provided to legal users effectively by preventing unwanted exploitation of resources by malicious users.

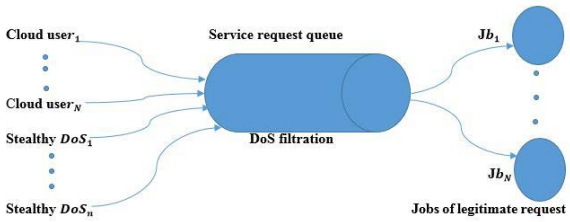

Figure 1. Collaborative lockout policy with ACL.

2.1 Administrator Module

Admin act as cloud storage provider it provides the cloud storage space to customers on the basis of SLA, where the cloud customers can host their own services and provides access to the authorized users. Administrator can have capability to activate or deactivate services hosted on the provided storage space.

2.2 Client Registration Module

Client act as cloud customer buys cloud storage from cloud service provider. Pay and use feature of cloud enables client to pay for requested quality of services provided based on SLA specification. The customer can post the service details and provides access to users of ACL with proper authentication.

2.3 User Registration Module

The user registration results in storing the user details into Access Control List where security is incorporated by sharing secret key to user via stored credential for user communication. If the login credential is valid and shared key matches with user key then the user is comes under legitimate user otherwise users are considered as illegitimate users.

3. Results and Discussions

The collaborative model of lockout policy with ACL helps in enhancing quality of service and preventing unwanted consumption of resources by malicious node. Figure 2 Shows comparison of result in Stealthy DoS with proposed Method of collaborative modelling. Advantage of collaborative Lockout policy with Access Control List over Orchestrated Stealthy DoS attack Pattern is depicted by Table 1.

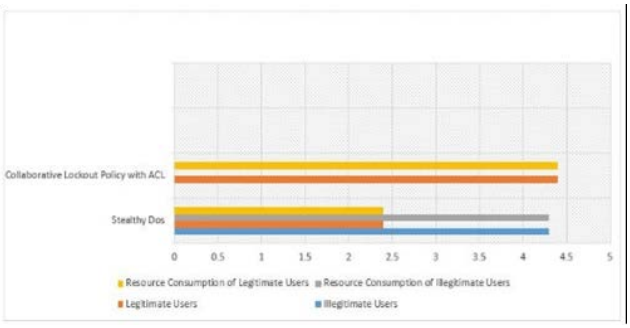

Figure 2. Comparison of stealthy DoS with collaborative lockout policy with ACL.

4. Conclusion

Thus lockout policy with access control mechanism promotes the security of the targeted system without affecting legitimate user access. The proposed architecture classifies users into malicious and non-malicious nodes and denies services to non-malicious nodes. The overall resource consumption of illegitimate users is eliminated and promotes the orchestrated flow of attack pattern

Table 1. Advantage of proposed collaborative policy over stealthy DoS

Parameters	Orchestrated stealthy DoS attack pattern	Collaborative Lockout policy with ACL
Request handling	Process both legitimate and illegitimate request	Allow and process only legitimate request. Filtration of malicious request will be done
Auto scaling	Exhaust the resources provided by cloud provider while handling malicious request of increased job size. Creates service inability to authorized users	Capable of providing better services to authorized user with out any interruption
Load balancing	Balancing loads of malicious request consumes more space and creates overhead on targeted application , services or network	Balancing of load of authorized request results in effective performance
Resource consumption	Increased resource consumption by both malicious and legal users with increased in job size	Resource consumption can be controlled by allowing only authorized request for processing
Financial cost	Increases financial cost while exploiting more resources by malicious node	Reduces the financial cost by filtering malicious request
Arrival rate	Performance of application, services or network is reduced in increased arrival rate of job request	Performance of application, services or network is enhanced even in increased arrival rate of job request
Quality of service (QoS)	Reduces the QoS to authorized users	Increases QoS to authorized users

filtration. ACL provides access to users based on their roles. Confidentiality and integrity is also achieved in the proposed method. The efficient filtration of unwanted traffic towards a targeted network, application or service is preserved and security is enhanced. In future, the compressed access control list mechanism can be used to improve the security of cloud.

5. References

1. Mount MC, McCorry K, Papanikolaou N, Pearson S. Security and Privacy Governance in Cloud Computing via SLAS and a Policy Orchestration Service. Proceeding 2nd International Conference Cloud Computing Services; 2012 Apr; 670-74.
2. Lu K, Wu D, Fan J, Todorovic S. Nucci A. Robust and Efficient Detection of DDoS Attacks for Large-Scale Internet, Computer Networks. 2007 Dec; 51(18):5036-56.
3. Access Control List Mediation System for Large-Scale Network. Date Accessed: 5/12/2005. Available at: http://ieeexplore.ieee.org/document/1578962/.
4. Network Intrusion Prevention by Configuring ACLs on the Routers, Based on Snort IDS Alerts. Date Accessed: 18/10/2010. Available at: http://ieeexplore.ieee.org/document/5638482/.
5. Daly J, Liu AX, Torng E. A Difference Resolution Approach to Compressing Access Control Lists, IEEE/ACM Transactions on Networking. 2016 Feb; 24(1):610-23.
6. Ficco M, Rak M. Stealthy Denial of Service Strategy in Cloud Computing, IEEE Transactions on Cloud Computing. 2015 Jan- Mar; 3(1):80-94
7. A Design of Diffie-Hellman Based Key Exchange using One-Time ID in Pre-Shared Key Model. Date Accessed: 29/03/2004. Available at: http://ieeexplore.ieee.org/document/1283932/.
8. Lopez M A, Duarte OCMB. Providing Elasticity to Intrusion Detection Systems in Virtualized Software Defined Networks, Communication and Information System Security Symposium; 2015. 7120-25.
9. Nivethitha Somu, Gangaa A, Shankar Sriram VS. Service in Hadoop using One Time pad, Indian Journal of Science and Technology. 2014 Apr; 7(S4):56-62.
10. Sabout Nagaraju, Latha Parthiban. SecAuthn: Provably Secure Multi-Factor Authentication for the Cloud Computing Systems, Indian Journal of Science and Technology. 2016 Mar; 9(9):1-18.