Preventing Insider Attack, DDos in Cloud Computing using Restricted Access Protocol to Enhance Security and Reducing Bandwidth Consumption

Swati Sharma
Lovely Professional University, Phagwara

Abstract— The CLOUD COMPUTING is happening technology which is most commonly used now days. As more and more users are accessing the cloud security is under danger. In order to resolve the problem the security mechanism within the cloud has to be implemented. Cloud prone to number of attacks. Most common attack over the cloud is DDOS. It is Distributed Daniel of Service. The main operation of the DDOS is to block the resources which are present over the cloud. The cloud computing will depend over the network. The data on the network will be transferred on the basis of the packets. When data is transferred over the network there will always be a upper bound over the packet limit. As cloud is used more often, it is prone to security issues. The security issues will be the prime objective of the proposed paper. Along with the security issue we will also introduce packet redundancy handling mechanism using the concept of service queue. The proposed paper will introduce the restricted access protocol which will secure the packet transfer and service queue which will eliminate the redundant data.

Key words: Cloud Computing, Data, Network, Service Queue, packet, redundancy, restricted access protocol

I. INTRODUCTION

The cloud is now days used in order to store the important data from multiple sites. The advantage of using the cloud is that individual site does not have to maintain the several GB's of space. As the device become overloaded the data present over the device will be offloaded to the cloud. The cloud hence is an important storage mechanism which is provided to different class of users. As cloud is exposed to more and more users with different intentions the security of the cloud is at stake. There are number of services which are provided by the cloud. Accordingly cloud service model is presented.

1) IaaS
2) SaaS
3) PaaS

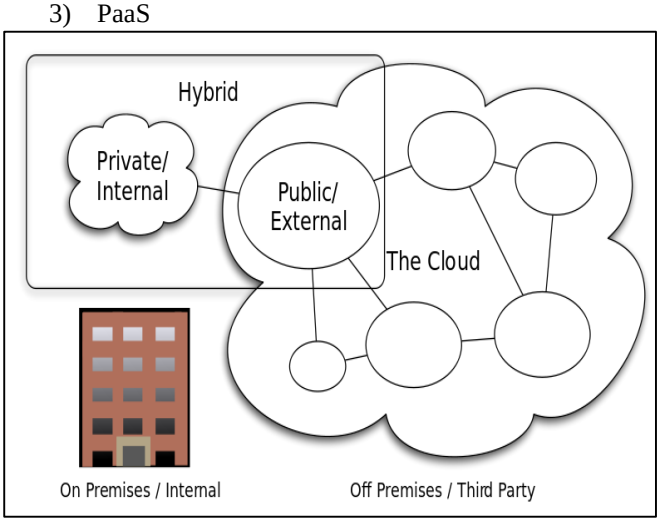

Fig. 1: Showing Different Cloud Computing Types

The cloud is versatile in nature. It can be used for a private organization. In that case the cloud is known as Private Cloud. If cloud is used for the public purpose then the cloud is known as public cloud. Hybrid cloud on the other hand will be the combination of two or more clouds.

The data when transferred over the network the bandwidth is considered. The bandwidth is the parameter on the basis of which cost over the network is encountered. So consuming bandwidth has to be reduced. So in the second phase we will use service queue in order to handle the redundancy present with the data which is transferred. The cloud security can be handled at different layers of the network. The cloud security is handled in number of papers but we have handling the data part by checking the extension of the packet which is being transferred.

II. ARCHITECTURE OF CLOUD

All Cloud computing schemes are one of IT services that are provided to users on rental basis over a network. The ability to increase or decrease service requirements will affect the utilization of cloud computing. The cloud does not have any centralized ownership. Anyone having desired equipments can use the cloud resources. The cloud services are generally free in nature. The cloud models are scalable, flexible and efficient in nature. The cloud models are also present. User can utilize the model according to their own requirements. The cloud computing models are divided into following categories.

- Cloud Service Model
- Cloud Deployment Model

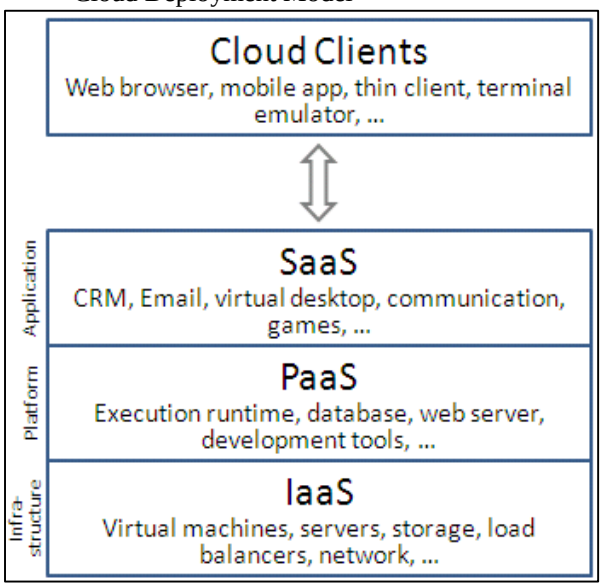

Fig. 2:

A. Characteristics of Cloud Computing

There are number of properties which are associated with the cloud computing. All the characteristics are as listed below

1) Scalable

The cloud network is scalable in nature. Which means any number of nodes can participate within the cloud. The nodes which are not required can be removed from the cloud.

2) Platform Independent

The cloud network is platform independent. This means that it does not matter which remote device we are using the services are accessible to the user.

3) Offloading

With the help of the cloud computational offloading is achieved. This means that load on single data center is not enforced.

4) Reliability

When computational offloading is achieved then reliability is also increased. This indicates that if one data center goes down then data is recoverable from other datacenter.

5) Positive Redundancy

The redundancy is used in the positive manner. With the redundancy reliability is achieved. Hence redundancy is used in the positive manner.

6) Pooling of Resources

There exist numbers of resources which are present over the cloud. All of these resources are sharable in nature. So resources are kept in a common pool from which it is accessible by the users of the cloud.

III. SECURITY AND DDOS – DISTRIBUTED DENIAL OF SERVICE

Cloud computing is a method by which storage capacity increase or additional capabilities are added dynamically without requiring in new infrastructure, training new personnel, or purchasing new software. It increases existing features of Information Technology's. In the previous years, cloud computing has extended from being a committing business concepts to one of the rapid increasing segments of the information technology industry. But as more as more information is invested or focused on cloud, concerns are beginning to grow about just how safe a Supra system is. The users of the cloud are of many categories. These users may use the Cloud for indifferent purpose. The most common type of attack which occurs over the cloud is DDOS attack. This attack will block the resources which are available over the cloud. Hence deadlock situation will occur if this effect goes on. So security mechanism has to be provided. The services of the cloud are generally be provided to the users. So the services are needed to be deployed. These services are deployed in different than the normal. The deployment model will indicate that services are being used by the user. the services are listed as: public, private, community and hybrid. These services also are affected by the problems present within the cloud. In order to solve the problems security mechanisms are enforced.

IV. COMPONENTS AND ARCHITECTURE OF DDOS

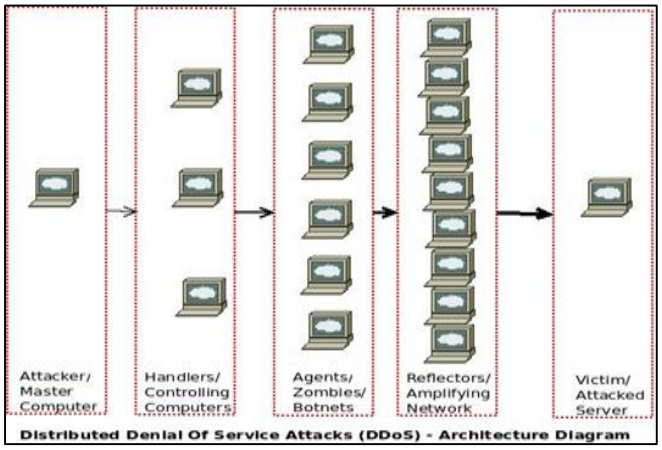

Fig. 3:

In DDOS architecture there are following terms which are considered.

A. Attacker

The attacker is the malicious machine which is present over the cloud. The attacker is responsible for causing the machines over the cloud to be blocked.

B. Handlers

The handlers are responsible for handling the attacks which are occurring on the cloud computing devices.

C. Agents

The agents are the intermediate machines which are present over the network. The agents can also be zombies in nature. The zombie processes are those which remain in the cloud even after finishing their tasks.

D. Reflectors

Reflectors are used in order to check the status of the cloud when multiple machines operate over the cloud. It is with the help of reflectors that the malicious nodes can be detected.

E. Victim

It is the targeted machine on which attack do takes place. The resources of the cloud will be blocked if the attack occurs. The server which is blocked is the victim.

V. FIREWALL

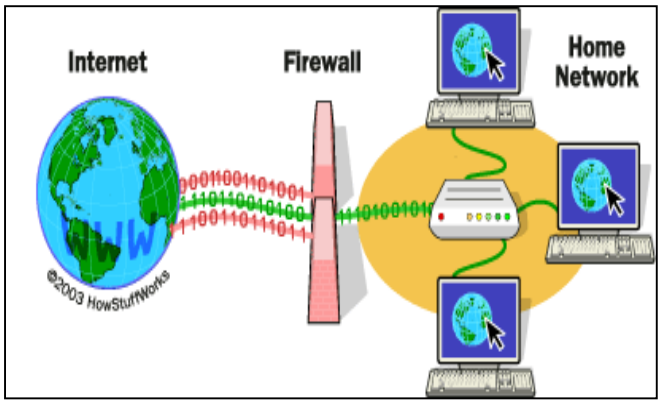

Fig. 4: Firewall

Firewalls are light weight software's which are used to provide the security against the malicious nodes. The

contents which are malicious are blocked however the contents which are purr are accepted. The firewalls are implemented in mobile ad-hoc network. However we can also implement this mechanism on the cloud also. So in the proposed system same will be implemented on the cloud.

VI. RELATED WORK

There is legion of work which is being done toward the cloud. The cloud provides the mechanism by which storage requirements associated with individual device is reduced. (Jain, 2012) the paper describes the security issues which are present within the cloud. The cloud is exposed to wide variety of users. When the user access the cloud the intension of the user must be considered. The negative intension of the user will lead to the attacks within the cloud. All such attacks are described within this paper. (Zissis & Lekkas, 2012) The recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result the aim of this paper is twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. (Kumar, Bhushan, & Pandey, n.d.)modified third party auditing is considered in this case. It means the data which is transferred must be verified by the third party which does not have any partial views. This can enhance the security of the cloud system. (Cachin, 2010)paper describes the mechanism of ensuring secure cloud. The vulnerabilities present within the cloud when user use cloud is high. So in this paper security mechanisms are suggested which can be followed for secure transmission of data. (Okuhara, Shiozaki, & Suzuki, 2010) Moving computing into the ``Cloud{"} makes computer processing much more convenient for users but also presents them with new security problems about safety and reliability. To solve these problems, service providers must establish and provide security architectures for Cloud computing. This paper describes domestic and international trends in security requirements for Cloud computing, along with security architectures proposed by Fujitsu such as access protocol, authentication and identity (ID) management, and security visualization.

From the above discussion we conclude that cloud is vulnerable to many distinct activities. In order to overcome these difficulties we can use restricted access with service queue.

VII. PROPOSED SYSTEM

In the proposed system the security is considered by verifying the packet along with its extension. The special bit patterns will be introduced within the packet during the transfer process. If for any reason the packet is corrupted then bit pattern within the packet will be altered. Once, the first level of security is cleared than second level of security known as extension checking will be performed.

After the security problem is resolved we will go toward the bandwidth conservation. The repeated packets will be eliminated from the data being transferred. The repeated packets will be eliminated by the use of the service queue. The proposed algorithm will be as follows

A. Algorithm RAP

a) Receive the packets(Pi) from the cloud and insert special bit pattern(e.g. 001100) at the beginning and end of the packet
b) Transfer the packet
c) Compare the packet special bit pattern
If(corrupt(Pi)) then
Return unsecure
Else
Return Secure
End of if

The above algorithm is going to check only the data at deep intense level. The extensions will be checked in the next algorithm

B. Algo RAP1

a) Check for the extension of the packet being delivered
b) If(∑di==∑pi) then
Return safe
Else
Return unsafe
End of if

After checking the data for security we will use service queue for redundancy handling. The redundancy when eliminated bandwidth will be saved. The bandwidth will also decrease the overall cost of transfer.

C. Algo Main($Packet_i$)

a) If(RAP($Packet_i$)) then
b) If(RAP1($Packet_i$))then
c) Compare the $Packet_i$ with the Contents of the service Queue(SQ_i)
d) If match occur then
e) Neglect the packet
f) Else
g) Accept the packet
End of if
End of if
End of if

The proposed algorithm will consist of three algorithms. The data will be successfully transmitted only if first two algorithms return true.

VIII. CONCLUSION AND RESULT

The proposed algorithm will introduce the new level of security. The security along with bandwidth conservation is suggested in the proposed model. The security at the packet level will be achieved. The intense data analysis will be conducted for this purpose. The packet will be categorized by the unique packet number. The packet will be compared and then verified for the special bit pattern. If that pattern is altered then the packet is not secured. Overall security will be enhanced by the use of the suggested protocol. Also bandwidth conservation is also achieved.

The proposed algorithm uses two different mechanisms for enhancing security of packet. In the future work the two different mechanisms will be combined together to reduce the complexity.

REFERENCES

[1] G. Ollmann, "Understanding the Modern DDoS Threat," Damballa, pp. 1–10, 2011.
[2] Cisco, "Defeating Ddos Attacks," Group. pp. 1–11, 2002.
[3] R. Malhotra and P. Jain, "Study and Comparison of Various Cloud Simulators Available in the Cloud Computing," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 9, pp. 347–350, 2013.
[4] M. Ahmed and M. A. Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE Cloud," Int. J. Netw. Secur. Its Appl., vol. 6, no. 1, pp. 25–36, 2014.
[5] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Futur. Gener. Comput. Syst., vol. 25, no. 6, pp. 599–616, 2009.
[6] B. B. Gupta, R. C. Joshi, and M. Misra, "Distributed Denial of Service Prevention Techniques," Int. J. Comput. Electr. Eng., vol. 2, no. 2, pp. 268–276, 2012.
[7] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013.
[8] P. Jain, "Security Issues and their Solution in Cloud Computing," Researchmanuscripts.Com, 2012.
[9] C. A. Labs and I. S. Solutions, "Insider Threat Detection."
[10] M.-D. Nguyen, N.-T. Chau, S. Jung, and S. Jung, "A Demonstration of Malicious Insider Attacks inside Cloud IaaS Vendor," Int. J. Inf. Educ. Technol., vol. 4, no. 6, pp. 483–486, 2014.
[11] L. Ramaswamy, L. L. L. Liu, A. Iyengar, A. Sayler, D. Grunwald, G. Suciu, C. Cernat, G. Todoran, V. Suciu, V. Poenaru, T. Militaru, S. Halunga, Q. Zhang, L. Zhu, H. Bian, X. Peng, E. Afgan, D. Baker, J. Chilton, N. Coraor, J. Taylor, L. A. Bastiao Silva, C. Costa, A. Silva, J. L. Oliveira, T. Cruz, P. Simoes, J. Rodrigues, E. Monteiro, F. Bastos, O. Heen, C. Neumann, L. Montalvo, S. Defrance, P. Meye, P. Raipin, F. Tronel, E. Anceaume, R. Shuanglin, B. Mao, H. Jiang, S. Wu, Y. Fu, L. Tian, A. Hajnal, Z. Farkas, P. Kacsuk, R. Dooley, J. Stubbs, J. Basney, M. M. Jaghoori, A. J. Van Altena, B. Bleijlevens, S. D. Olabarriaga, S. Q. Ren, S. Cheng, Y. Zhang, E. S. Lim, K. L. Yong, Z. Li, and C. S. C. Council, "Cache Clouds: Cooperative Caching of Dynamic Documents in Edge Networks," 2014 6th Int. Work. Sci. Gateways, vol. 86, no. Iccse, pp. 335–338, 2012.
[12] C. Science and M. Studies, "Securing user data on cloud using Fog computing and Decoy technique," vol. 7782, pp. 104–110, 2014.
[13] J. Sen, "Security and Privacy Issues in Cloud Computing," arXiv Prepr. arXiv1303.4814, no. iv, 2013.
[14] P. K. Tiwari and B. Mishra, "Cloud Computing Security Issues , Challenges and Solution," vol. 2, no. 8, p. Aug, 2012.
[15] Z. M. Yusop and J. Abawajy, "Analysis of Insiders Attack Mitigation Strategies," Procedia - Soc. Behav. Sci., vol. 129, pp. 581–591, 2014.
[16] "Solution to DDoS issues for streamers and players." .
[17] V. R. Chandrasekhar and W. K. G. Seah, "Range-free Area Localization Scheme for Wireless Sensor Networks."
[18] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks 1," 2003.
[19] Kumar, N. Chand, V. Kumar, and V. Kumar, "Range Free Localization Schemes for Wireless Sensor Networks," Int. J. Comput. Networks Commun., vol. 3, no. 6, pp. 115–129, 2011.
[20] J. Zheng and A. Dehghani, "Range-Free Localization in Wireless Sensor Networks with Neural Network Ensembles," J. Sens. Actuator Networks, vol. 1, no. 3, pp. 254–271, 2012.

