International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-12, Dec.-2014

AUTHENTICATION MODEL FOR CLOUD COMPUTING USING SINGLE SIGN-ON

[1]ANIESH KRISHNA K, [2]BALAGOPALAN A S

[1,2]Department of Computer Science and Engineering, Sri Ramakrishna engineering College, Coimbatore.
E-mail: [1]anieshtintin@gmail.com, [2]balagopalan40@gmail.com

Abstract- Cloud computing is a way to provide IT resources with the help of internet in a pay-on-use pattern. In spite of the various benefits of using cloud still there exists many vulnerabilities in cloud security which hinders its adoption. The security in cloud is limited to network and application securities. There is a need to establish a system to authenticate the cloud users while he is attempting to access the cloud services within the bounds of the SLA between the cloud provider and the user. The existing system provides authentication based on keys Encryption algorithms either symmetric key-based or asymmetric are key-based. Encryption management is the main problem. This paper proposes a secure authentication and authorization in Cloud Environment with the help of an optimized infrastructure using SL(Single Login).SL is a process gaining access to multiple resources using a single authentication that aims at reducing number of login and password in heterogeneous environment and to have an overall balance in Security, Efficiency and Usability. The authentication model based on the Kerberos protocol to provide single Login and to prevent DDOS attacks is also presented in this paper.

Keywords- Security, DDOS, Cloud Computing, Encryption, Sign-on, Kerberos.

I. INTRODUCTION

Through cloud computing IT-related capabilities are provided as services to multiple external customers using Internet technologies. It allows users to consume services without knowledge and control over the technology and infrastructure supporting them. Today's businesses are very complicated, whenever there is a new hire we need to purchase new hardware, software licenses etc. Also organizations need experts to install, configure, test and run them. Cloud computing reduces this entire burden as organizations need not to own all these resources. Resources are owned by the third party cloud provider. The best idea behind this is reusability of IT-related capabilities. Computing software, hardware and other resources are prone to be outdated very soon. Therefore cloud computing platforms are smart solution for the users to handle complicated IT infrastructures.

The important advantages of cloud computing are: Fast delivery of resources, lower entry cost, agility, device independency, services independency, location independency and scalability. Services are provided like utilities in Cloud computing, so end users only pay according to the type and amount of usage. It facilitates on-demand service delivery and also quality of service. Cloud computing is usable in several applications areas such as education, banking, medical and health and several financial applications. But as cloud is a distributed and shared environment there are several issues related to its security.

Also it is the major target for an attacker. Some of the attacks that an attacker may launch are DOS or DDOS attacks, man in the middle, side channel attack, injection attacks, indexing attacks, flooding, packet sniffing, etc. In cloud computing environment an important issue is to provide reliable and secure services.

One of the major security issues is how to handle distributed denial-of-service (DDoS) and denial-of-service (DoS) attacks and their impact. The main purpose of DDOS attacks is to consume large volume of server resources, so that the legitimate users would not be able to get services. For an attacker DDOS attacks are easy and simple to implement but are very difficult to prevent for security experts. We are proposing a solution to DDOS attacks by integrating strong Kerberos authentication protocol with cloud computing. Also it provides single sign-on for whole session along with convince and ease of usage for users. This reduces the need to login again and again for a complete session unlike simple cloud system. In a cloud computing environment where everything is provided as services to client such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Data as a Service (DaaS), this proposed system for cloud computing can provide secure access to all of these services for the clients as shown in Fig 1.In other words, Cloud services are like applications that are running somewhere in the Cloud and can be accessed through Internet or Intranet. For users, who don't need to care about their data where to be stored or services where to be provided.

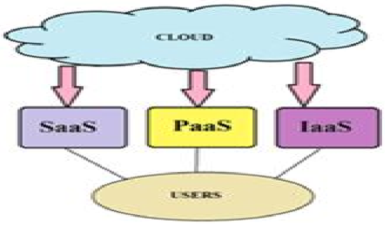

Fig 1: Cloud Services

II. RELATED WORK

Minqi Zhou, Rong Zhang and others have discussed several security and privacy issues related to cloud. They investigated several Cloud Computing system providers and their concerns on privacy and security issues. Kevin Hamlen, Murat Kantarcioglu and et al. have followed bottom up approach to security and worked on small problems in the cloud environment in the hope that it will solve the larger problems of cloud security. They discussed security issues for cloud middleware security, storage security, network security, data security and application level security. Richard Chow, Philippe Golle et al. characterize the problems and their impact on adoption of cloud computing. They have proposed to extend control measures through the use of Trusted Computing and by applying cryptographic techniques. B.Meena, Krishnaveer Abhishek Challa identifies all the possible security attacks on clouds including: Authentication attack, Denial of Service attack, Wrapping attacks, Man-in-the Middle attack, Flooding attacks, Malware-Injection attacks, Browser attacks, and also Accountability check problems. They mentioned the root causes of these attacks and also proposed specific solutions for all of these attacks. Farhan Bashir Shaikh and Sajjad Haider identifies top security concerns of cloud computing, these concerns are Leakage of Data, Data loss, User‘s Authentication, Client‘s trust, Malicious users handling, risk management, Wrong usage of Cloud services and Hijacking of sessions while accessing data. They propose to use new release of governance The Cloud Security Alliance (CSA) and compliance stack for cloud computing. To counter these kinds of attacks, Chi-Chun Lo, Chun-Chieh Huang and Joy Ku have proposed a framework of cooperative intrusion detection system (IDS). This system could reduce the DDOS attacks impacts. This cooperative IDS send the alert messages to other IDSs, if they detect any region suffers from DoS attacks.

AO Shan and Guo Shuangzhou have designed and implement the SHIFT (Speculative Hardware based Information Flow Tracking) system. This can enhance security of software in cloud computing platform. This can detect low-level attacks such as buffer overflow attack and also other SQL injections based high-level semantic attacks and cross-directory traversal attacks. Bansidhar Joshi, A. Santhana Vijayan, proposes a solution model is to Trace Back through proposed Cloud Trace Back (CTB) to find the DDOS attacks source, and also introduced the use of a back propagation neutral network, called Cloud Protector, which can be trained to filter and detect such attack traffic.Yang Xiang and Wanlei Zhou present a new approach, called Flexible Deterministic Packet Marking (FDPM), this can perform a large-scale IP traceback to defend against Distributed Denial of Service (DDoS) attacks. Ashley Chonka et al. also proposed an IP traceback scheme using a machine learning technique called Intelligent Decision Prototype (IDP). IDP can be used on both Deterministic Packet Marking (DPM) and Probabilistic Packet Marking (PPM) traceback schemes to identify DDoS attacks. An Lei and Zhu Youchan propose a solution for DDOS attacks based on multi-agent. They have discussed DDOS attacks and also the methods to launch DDOS attacks. So this solution increases the server-side bandwidth and computing speed.

III. PROPOSED SYSTEM

The main focus of this model is to authenticate a client before accessing service and to find the source of DDOS attack. Merely username and passwords checking is not enough for a cloud computing like distributed and shared environment. Kerberos is an authentication protocol for network and also provides single sign-on facility to clients. Kerberos was developed in the mid of 1980’s at MIT. It is upgraded to different versions since it comes to action. Currently Kerberos version 5 is in use. The main entities used are key distribution center (KDC), authentication server (AS) and ticket-granting server (TGS). Control node at cloud acts as interface between cloud and client. Control node receives the requests from clients and must check each client for identification. Till now, author has proposed a single sign-on authentication model for an open environment that combines the platform trust in user systems and trusted module security using Kerberos. Kerberos acts as third party in every transaction as identity or authentication service provider. This can helps to achieve strong security, enhanced privacy and platform trust. Nitin and others have proposed an Image Based Authentication (IBA) systems combined with strong Kerberos Protocol to assure a scope for secured communication systems in the future. They proposed to use images as password set and also implemented their solution it for a JUIT university (Jaypee University of Information Technology).

Here we will see how cloud computing can be integrated with the Kerberos protocol to provide authentication, secure access and to provide secure single sign-on. Cloud Servers or Control Node must have the ability to check the identities and authenticity of clients before granting access to subscribed services. Task for each client/server interaction, server can be required to undertake this. But in a cloud computing like open and shared environment, this places a substantial burden on each server. AS does this work on behalf of cloud server, who knows the passwords of all users and stores them in a centralized database. AS then interacts with the TGS that grant a master ticket to the clients to access all the subscribed cloud services for a session. In cloud system a client has to login every time, whenever he/she wants to access a service. But with this proposed system the client can have access to subscribed services for the entire session. One full session can be of 8, 9 or more hours. By this it minimizes the number of times that a client has to log on.

Suppose every ticket is once usable. If the user wants to access the same or different services at the server at different times after once logon, re-login is required for every attempt.

This situation can be improved by making the ticket reusable. This will be the case of single sign-on for an entire session. Once received the ticket from TGS, the client's workstation can store it and can use it on behalf of client for all accesses to the cloud server for a session. It also facilitates encrypted transmission of passwords and tickets. Kerberos uses PKI (private key encryption).

3.1 Initial Authentication of Client

I. Suppose a client wants to access cloud server. Then this server requires a Kerberos "ticket" before it will honor client's request. Only on the basis of that ticket the Cloud Server will grant access to all the subscribed services to client. This ticket proofs client's authentication to server. This removes burden of cloud server for performing authentication checks. And also saves cloud's processing time and memory.

II. To get ticket, client first request authentication from the Authentication Server (AS). The Authentication Server creates a "session key" (which is also an encryption key) basing it on client's password and a random value that represents the requested service. This complete process is shown in Figure shown below. The session key is effectively a "ticket-granting ticket." That will be used by the client to get master ticket to access services from cloud server. The Authentication server (AS) may send the session key to any request. But it's only the legitimate client who can decrypt the session key to obtain the Ticket-Granting ticket.

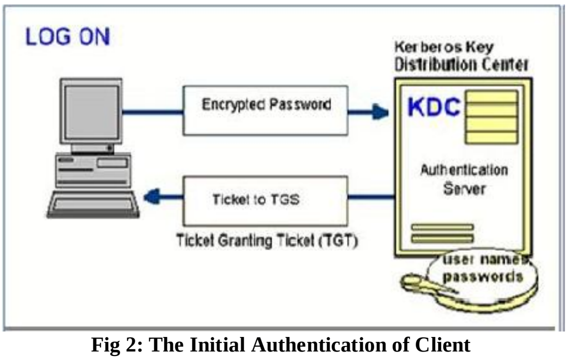

Fig 2: The Initial Authentication of Client

3.2 Ticket-Granting Ticket Exchange to Obtain Service-Granting Ticket

I. Client next sends the ticket-granting ticket to a ticket-granting server (TGS). The TGS may be physically the same server as the Authentication Server, but it's now performing a different service. The TGS returns the ticket that can be sent to the cloud server for the requested service. We named this ticket as "Master Key". This ticket will be used to access services from cloud server.

II. The server either rejects the ticket or accepts it and performs the service. The master key granted to client can only be decrypted by the cloud server with the secret key shared between cloud server and the TGS. Client or anybody else will not be able to decrypt the master ticket.

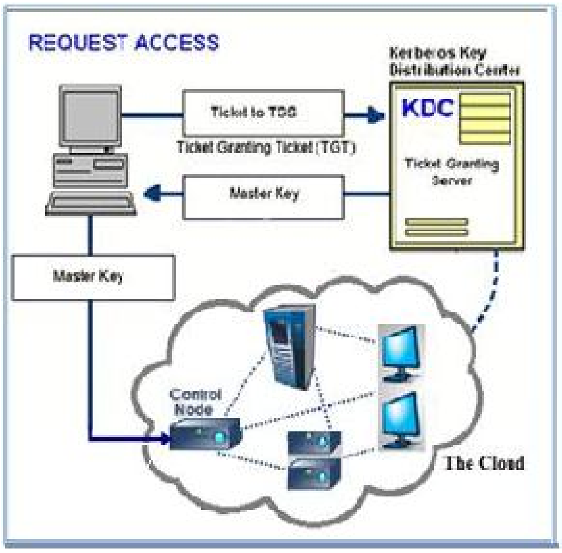

Fig 3: The Proposed Model for accessing cloud services

I. Because the ticket client has received from the TGS is time-stamped, it allows client to make additional requests using the same ticket within a certain time period (typically, 8 hours) without need to prove authenticated again. As the ticket is valid for a limited period of time, this makes fewer chances that anyone else will be able to use it later.

II. The control node at cloud receives the client request. It acts as the interface between the Data Center/Cloud service provider and external users/brokers. It examines the service request, performs accounting and pricing functions, keeps track of the availability of VMs and their resource entitlements and also starts the execution of accepted service requests on VMs those are allocated. The actual process may be more complicated than just described. On the basis of implementation the user procedure may vary.

IV. MESSAGE TRANSMISSION

4.1 Authentication Service Exchange to obtain TGT

(1) Encrypted Password: With message (1) the client request for a ticket-granting ticket. It includes the user's ID, TGS's ID and timestamp 1.

(2) Ticket to TGS (TGT): AS responds back with ticket to TGS, client ID, timestamp 2 etc. These all are in encrypted form and this encryption is done using the key generated from the client's password.

4.2 Ticket-Granting Service Exchange for getting TGT

(3) Ticket to TGS (TGT): Client sends the TGT along with its authentication and ID of TGS.

(4) Master Key: TGS sends the ticket to cloud server along with client ID to client.

5.3 Client/Server Authentication Exchange

(5) Master Key: Client sends the cloud server ticket and its authentication to cloud server.

(6) Authentication: Cloud may either request authentication from client or client can directly start accessing service from cloud.

4.3 The Sequence Diagram

The Fig-4 given below shows sequential or interactive diagram for the whole working. It shows the sequential process of messages transmission for accessing the Cloud Services. The solid arrow lines here depict message transmission for messages from (1) to (6). The vertical lines depict the timeline and text in boxes represents objects interacting with each other. Such as client interacting with AS, TGS etc.

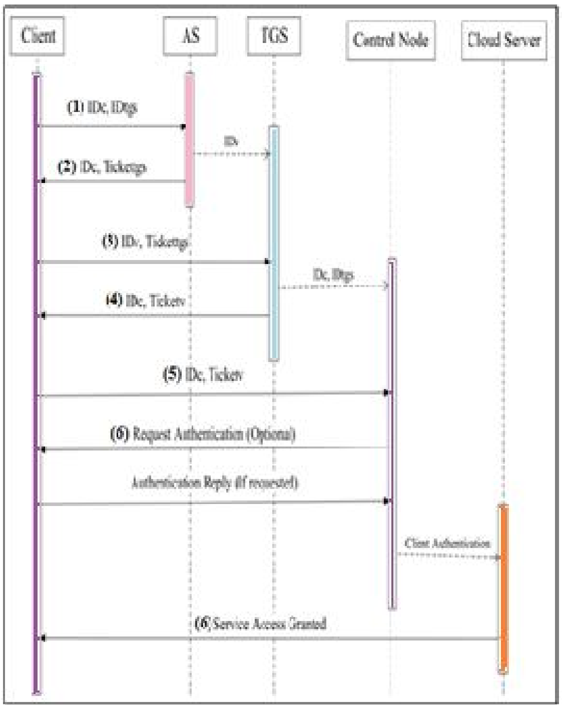

Fig 4: Sequence Diagram Depicting Exchange of messages

4.4Reason forDDOS Attacks

1. The cloud providers claim that they have vast amounts of bandwidth. Anyone with a lot of bandwidth can make the excuses.

2. The cloud firms personally use very low tech way to mitigate against these attacks.

3. Several Mature networks and hosting providers with years of experience in mitigation handle these attacks better than others cloud providers.

V. DDOS PREVENTION THROUGH THIS PROPOSED MODEL

The DDOS attacks are composed of four elements. It involves victim, attack daemon agents, control master program and finally the real attacker. Kerberos reveals and checks the identity of the source. Kerberos messages exchange are very secure and in encrypted form. After authenticating and granting session ticket to client, client can send the message to the cloud server to access service. Then cloud's service will prepare a response and send it to client as part of HTTP response. Kerberos handles most of the traffic to cloud and also helps in congestion control. It pays no attention to any outgoing transmission between user and cloud after this and will not interfere with any response request or incoming and outgoing messages. This model prevents against DDOS attacks in following manner:

a) Filter and detect DDOS attacks: Kerberos can be trained to detect and filter DDOS attacks. The entire prior authentication will be done by Kerberos, instead of cloud provider. This helps to prevents direct attacks.

b) Proper source Detection: Kerberos can also help to locate source of attack by examining the frequency of requests. It is also able to detect all attacks that damage at the victim. It can separate Attack and legitimate Traffic by applying certain precedence rules.

c) Priority checking at Control Node: Control node at cloud receives master ticket that includes timestamp and session information. Control node may also records the time of last access of client. And at every next access give priority to requests that have the least access before and being waiting for response. And allocate services and resources to next selected request. This can also prevent against denial of service to legitimate users.

d) Accurate identification of attacks & response: In the case of response by agent identification, the system can accurately identify the majority of attack machines regardless of their distribution. This identification can be prompt so that the action can be taken while the attack is on-going.

e) Congestion avoidance and traffic control: It stops the attack streams near the source and preserves the resources that are usually overwhelmed by the attack traffic. This reduces overall congestion and increases resources availability for legitimate users.

f) Earlier traceback: As it is closer to the source, it facilitates earlier traceback and investigation of attack. Kerberos can receive attack alerts from source-end defense systems and examine all the machines in the protected source network in order to detect those that are compromised.

5.1 Secure Single Sign-On (SL) With Kerberos

This allows customers of cloud to include database access in a Single Sign-On (SL) environment that:

- Boost up security of the system.
- Now users need not to log in separately for each application within a session.
- Reduces the costs for Cloud servers that are aSLciated with managing user accounts.

Firewall only makes assumption that attackers are always outsiders but in reality, attacks usually come from inside. Kerberos makes assumption that network connections are the weakest link of network security instead of servers and work stations.

Kerberos lets users to access network resources by simply presenting these secure tickets rather than repeatedly entering a user name and password. Instead of sending password to cloud servers client requests ticket from AS, and only ticket and encrypted request transmitted to cloud server. Possible Summarized benefits are:

- Encrypted interactions between the clients and the host.
- Single sign-on for an entire session that provides more easy and convenient access for the clients.
- Prevention from intercepted credentials and DDOS attacks and also against direct attack to cloud server.
- It is easier for the administrator to maintain a single and centralized password store thereby reducing the burden at cloud's control node.
- Passwords are never intercepted on the network that prevents from password sniffing, password filename/database stealing.
- Frees client from repeatedly authenticating themselves to cloud servers.
- This provides a scalable authentication infrastructure and limits the duration of user's authentication.
- Saves memory and computational time of cloud.
- Access priority checking at control node can prevent denial of cloud services for clients waiting from a long time.
- Above all, improved cloud network security.

CONCLUSIONS AND FUTURE WORK

Cloud computing offers sharing of resources in a location independent and cost effective way. Now many organizations, educational institutes, banking sector, health centers are relying on cloud services. Cloud is not only for Multinational companies but it is also being used by Small and medium enterprises. Cloud computing improves productivity while reducing the cost. Now employees can focus on development work and planning instead of wasting time for managing storage of data and other resources. Although advantages of cloud computing are very appealing but nothing can be 100 percent perfect on the shared internet environment. Cloud computing also involves several security and management risks and concerns. Cloud involves virtual machines that are very prone to attacks. Also DDOS attacks can be easily influence the cloud resources. These issues have made the adaptation cloud a bit difficult. These hurdles have several management issues. Still many new providers are stepping into this business. So choices for customers are increasing day by day. But there are always threats of attacks, data leakage and security breach. The solutions proposed here can be implemented in future to prevent cloud from direct access, DDOS attacks and to produce satisfactory improvements in cloud security. This will also helps to enhance the client's interest and satisfaction.

There are also some issues related to Kerberos such as:

- TGT can be misused by attacker for accessing cloud services until the session expires, in case if TGT is stolen.
- As authentication server is the main entity that stores complete database of login details, it will be worst if in any case its security is compromised. AS must be physically protected.
- Kerberos protocol can only authenticate a client's identity; it cannot authorize the accesses of users once they got ticket to access services from cloud.

Although these issues are rare but need special attention. Once satisfactory care is taken for all these, and then this solution can be able for better detection and filtration of DDOS attacks.

ACKNOWLEDGEMENTS

We wish to express our deep sense of indebtedness and sincerest gratitude to all the experts and Prof. M.Madhumathi for her invaluable guidance and appreciation.

REFERENCES

[1] Minqi Zhou, Rong Zhang and others, "Security and Privacy in Cloud Computing: A Survey", Sixth International Conference on Semantics, Knowledge and Grids, IEEE, 2010

[2] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing",

International Journal of Information Security and Privacy, 4(2), April-June 2010

[3] Richard Chow, Philippe Golle, Markus JakobSLn, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", Fujitsu Laboratories of America, CCS. 2009

[4] B.Meena, Krishnaveer Abhishek Challa, "Cloud Computing Security Issues with Possible Solutions", IJCST Vol. 3, Issue 1, Jan. - March 2012

[5] Farhan Bashir Shaikh and Sajjad Haider, "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, IEEE, 11-14 December 2011

[6] Chi-Chun Lo, Chun-Chieh Huang and Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010

[7] AO Shan and Guo Shuangzhou, "An enhancement technology about system security based on dynamic information flow tracking", IEEE, 2011

[8] Bansidhar Joshi, A. Santhana Vijayan, "Securing Cloud Computing Environment Against DDoS Attacks, ICCCI, IEEE, Jan 10-12, 2012

[9] Yang Xiang and Wanleiu Zhou, "A Defense System Against DDoS Attacks by Large-Scale IP Traceback", ICITA'05, IEEE, 2005

[10] Ashley Chonka, Wanlei Zhou, Jaipal Singh, Yang Xiang, "Detecting and Tracing DDoS attacks by Intelligent Decision Prototype", PERCOM.2008, IEEE

[11] An Lei and Zhu Youchan, "The Solution of DDOS attack based on Multi-agent", ICEIT 2010, IEEE

[12] Zubair Ahmad and Jamalul-Lail Ab Manan, "Trusted Computing based Open Environment User Authentication Model", 3rd International Conference on Advanced Computer Theory and Engineering(ICA CTE), IEEE, 2010

[13] Nitin, Durg Singh Chauhan et al, "Security Analysis and Implementation of *JUIT–Image Based Authentication System using Kerberos Protocol", Seventh IEEE/ACIS International Conference on Computer and Information Science, 2008.

★★★