© 2015 IJSRSET | Volume 1 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Study on Data Security in Cloud Architecture Based on Kerberos authentication System

Shital A. Salve
JSPM'S Imperial College of Engineering and Research, Wagholi, Pune, Maharashtra, India

ABSTRACT

Technological expansions in cloud computing due to increased connectivity and exponentially blooming data has resulted in journey towards cloud architecture. Cloud computing is a technology where the users' use high services in form of software that reside on different servers and access data from all over the world. Cloud storage allows users to access and store their data anywhere. It also guarantees best usage of the available resources. With a capable technology like this, it certainly abdicates users' privacy, putting new security threats towards the certitude of data in cloud. The security threats such as preservation of data integrity, data hiding and data safety concerns when the issue of cloud security bring up. In this research paper, we have studied design for cloud computing architecture which ensures secured movement of data at client and server end. We have used the aunthication Kerberos protocol mechanism for Authentication of client.

Keywords: – Cloud Computing, Kerberose.

I. INTRODUCTION

Cloud computing is a computing term or metaphor that evolved in the late 2000s, based on utility and consumption of computing resources. Cloud computing involves set up groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources. Clouds can be categorized as public, private or hybrid.[1][2]In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Server Internet-based computing," where different services — such as servers, storage and applications are delivered to an organization's computers and devices through the Internet .Cloud computing is similar to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. To do this, cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains big pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

II. METHODS AND MATERIAL

A. Cloud Computing.

Cloud computing promises several attractive benefits for businesses and end users. Three of the main benefits of cloud computing includes:

- Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand.

- Elasticity: Companies can scale up as computing needs increase and then scale down again as demands decrease.

- Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use. Cloud computing services are private, public or hybrid.

Private cloud services are delivered from a business' data center to internal users. This model offers adaptability and accessibility, while conserving management, control and security. Inside customers either may or may not be billed for services through IT chargeback. In the public cloud model, a third-party provider delivers the cloud service over the Internet. Public cloud services are retailed on-demand service to the users, typically by the minute or the hour. Customers only have to pay for the CPU cycles, storage or bandwidth they use. Leading public cloud providers include Amazon Web Services (AWS), Microsoft Azure, IBM/Soft Layer and Engine. Hybrid cloud is a mixture of public cloud services and on-premises private cloud – with composition and automation between the two. Companies can be run mission-critical jobs or sensitive applications on the private cloud while using the public cloud for busty workloads that must scale on-demand. The goal of hybrid cloud is to create a unified, automated, scalable environment which takes benefit of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.

Although cloud computing has changed over time, it has always been divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as service (SaaS). IaaS providers such as AWS supply a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large, and memory- or compute-optimized instances, in addition to customized instances, for various workload needs. In the PaaS model, suppliers host development tools on their infrastructures. Users access those tools over the Internet using APIs, Web portals or gateway software. PaaS is used for general software development and many PaaS providers will host the software after it's developed. Common PaaS providers include Salesforce.com's Force.com, Amazon Elastic Beanstalkand Google App Engine.SaaS is a sharing model that delivers software applications over the Internet; these are often called Web services. Microsoft Office 365 is a SaaS offering for production software and email services. Users can access SaaS applications and services from any location using a computer or mobile device that has Internet access.

B. How Cloud Works.

Consider an executive at a huge establishment. The particular responsibilities include making sure that all of the employees have the right access hardware and software they need to do their own jobs. Purchasing computers for everyone is not enough .it is essential buy software or software licenses to give employees the tools they require for their job. Whenever there is a new lease purchase more software or make sure that current software license permits another user. It's so worrying that find it difficult to go to sleep on a huge pile of money every night.

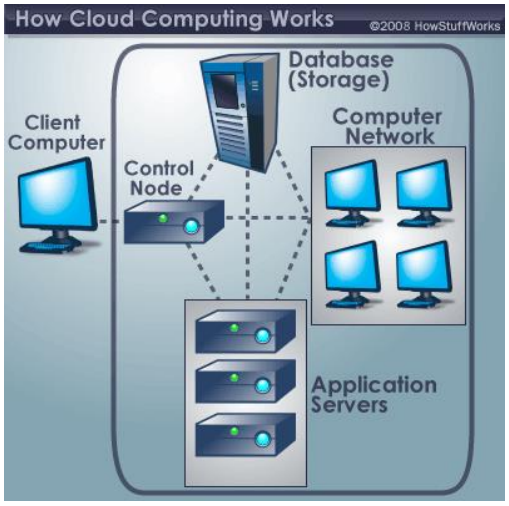

Figure 1.Working of cloud Computing

Soon, there may be a substitute for executives like client. Instead of installing a suite of software for each computer, client would have to load one application. That application will permit workers to log into a Web-based service which hosts all of programs the user would need for his or her job. Remote machines owned by another company would run everything from e-mail

to word processing to complex data analysis programs. It's called cloud computing, and it could change the whole computer industry.

Fig 1.shows that in a cloud computing system, there is an important work loading shift. Local computers do not have to do all the heavy lifting when it comes to runnable applications. The network of computers that made up the cloud handles them instead. Hardware and software demands on the users side is decrease. The only thing is that user's computer needs to be run in the cloud computing system's interface software, which can be as very easy as a Web browser, and the cloud's network takes care of the rest. There is a good chance users have already used some custom of cloud computing. If you have an e-mail account with a Web-based e-mail service like Hotmail, Yahoo! Mail or Gmail, then you have some experience with cloud computing. Instead of running an e-mail application on your computer, you log in to a Web e-mail account remotely. The software and storage for your account does not exist on your computer. it's on the service's computer cloud.

C. Disputes in Cloud Security

The disputes of cloud computing security are:

1. **Authentication** - assurance that communicating entity is the one claimed have both peer-entity & data origin authentication
2. **Access Control** - prevention of the unauthorized use of a resource like computing
3. **Data Confidentiality** –protecting of your data from unauthorized disclosure
4. **Data Integrity** - guarantee that data received is as sent by an authorized entity
5. **Non-Repudiation** - protection against denial by one of the parties in a communication

D. Literature Review

In 2010, Joshi et al. [1] provide an overview of different data security issues related to cloud computing. This work focuses on confirming security in cloud computing by providing secured trustworthy cloud environment. Farzad Sabahi [2] clarifies about the scope of various initiatives migrating to cloud. The author explains how migration to cloud can benefit various enterprises. Cloud computing journey involves considering the significance of issue of security. In 2011, Ashish Agarwal et al. [6] discourse about security issues concerned with cloud computing. This paper has convey about some severe security threats that prevails in this field. Ashutosh Kumar et al. [4] focused on providing a secure architectural framework for sharing and data gathering. This cynosure of this work is that the authors have made a permission hierarchy at different levels. The authors have focussed on security but with view of use hierarchy. In 2012, M.Venkatesh el al [5] proposes RSASS system for data security. The scheme uses RSA algorithm for encrypting large files and storing the date. The system used for storing large databases. But the use of linear methods compromises with the data recovery speed. Hence, this system is good for static data. Prashant Rewagad et al. [6] propose a system for providing security in cloud network.

Massachusetts Institute of Technology (MIT) developed Kerberos to protect network services provided by Project Athena. Several versions of the protocol exist; versions1–3 occurred only internally at MIT. Many members of Project Athena contributed to the design an implementation of Kerberos [4]. In [5] there is a dialogue that was written in 1988 to help its readers understand the fundamental reasons for why the Kerberos V4 protocol was the way it was. It was amazing how much this dialogue was still applicable for the Kerberos V5 protocol. Although many things were changed, the basic core ideas of the protocol have remained the same. Steve Miller and Clifford Neuman are the primary designers of Kerberos version 4 with contributions [6]. They published that version in the late 1980s, although they had targeted it primarily for ProjectAthena. Version 5, designed by John Kohl and Clifford Neuman, appeared as RFC 1510 in 1993 [3] (made obsolete by RFC 4120 in 2005 [7]), with the intention of overcoming the limitations and security problems of version 4.Security of Kerberos has been analyzed in many works, e.g. [8], [9], [10], [11], [12], [13] and [14]. Most commonly analyses identify certain limitations of Kerberos and sometimes propose fixes. This leads to the evolution of the protocol when a new version patches the known vulnerabilities of the previous versions. The current version Kerberos V5 is already being revised and extended [7], [15], and [16]. have analyzed portions of the current version of Kerberos and have formally verified that thedesign of Kerberos' current version meets the desiredgoals for the most parts [17]. it take a close look at Kerberos' encryption andconfirm that most of the options in the

current versionprovably provide privacy and authenticity [18].Kerberos is also used in wireless applications. M. Erdemproposed a high speed 2G wireless authentication systemsbased on kerberos [19]. He used DES, 3DES and AES as secret-key crypto algorithms. He also used SHA-1 message digest algorithm to hash the message blocks. study on the subject of using images as apassword and the implementation of Jaypee University ofInformation Technology (JUIT) Image BasedAuthentication (IBA) system called as JUIT-IBA using kerberos protocol.

III. RESULTS AND DISCUSSION

Proposed System

Kerberos is a network authentication protocol. It is designed to provide solid authentication for client/server applications by using secret-key cryptography. Kerberos work as an extra layer of security for any application which utilizes Kerberos Contains its own database of users and passwords visibly authenticates its users to save time from redundant password entries Limits accessibility. Kerberos is widely used in application-level protocols such as TELNET or FTP, to provide user to host security. It is used, though less frequently, as the implicit authentication system of data stream (such as SOCK_STREAM) or RPC mechanisms. It could also be used at a lower level for host to host security, in protocols like IP, UDP, or TCP although such implementations are currently rare, if they exist at all. It contains utility to recompile programs to run utilizing the kerberos authentication scheme effectively mercerizing them.it comes with programs with already built in kerberizationksu, ksh, telnet, etc…

A. The Ticket System

1. User will requests an initial ticket from KDC.
2. used as basic for all remote access requests

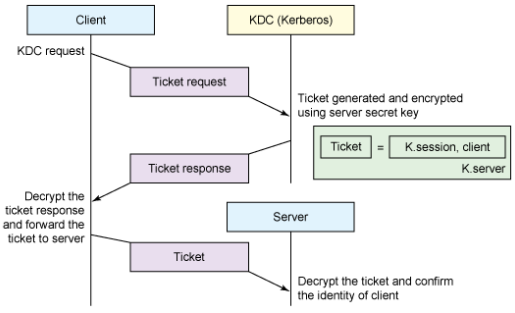

Figure 2. The Granting Ticket Process

Fig 2. Shows that A ticket is a sequence of a few hundred bytes. These tickets can then be embedded in virtually any other network protocol, thereby allowing the processes implementing that protocol to be sure about the identity of the principals involved.it has a Key Distribution Center (KDC), containing a database of:principles (customers and services)and encryption keys .it is based on the key distribution method by Needham and Schroeder steps in the ticket system.

1. User will sends request to the authentication server to use a particular program.
2. The server will creates a session key and proceeds to send to the user two encrypted replies the first is encrypted with the users key and contains the session key. second(ticket) is encrypted with the service's key and contains the same session key and the users information.
3. The user mines the session key from the first reply and sends two messages to the service.the ticket obtained from the server and the authenticator encrypted with the session key and containing a time-stamp.

B. The Granting Ticket

If that expressed in any way insecure there is an additional stage of security involved which Needham and Schroeder called the KDC in the first step rather than obtaining the ticket from the authentication server, the user will obtains a ticket granting ticket (TGT) the ticket granting server and authentication server are collectively stated to as the KDC.steps involved:user rather than using his secret key to decrypt the first reply from the AS for each ticket, he/she does so once for the TGT. After this, whenever a user want to use a service, he requests a new ticket with the TGT, now encrypted with the session key

C. The Importance Of Time Synchronization

To avoid replay attacks, Kerberos uses timestamp policies to all machines desirous to be a part of the kerberos network must be synchronised by within five minutes of each other any time stamp differing from the clock on the computer by more than 5 minutes it causes the service to disrespect the ticket as false in step 3 of the ticket process a time stamp was created, this was to block others from using this ticket at another time the TGT only lasts for a time set in one of the kerberos configures files.

IV. CONCLUSION

In this paper, we have studied the security issues faced by user's private data in the cloud system and the inevitable need to find a solution to the problem. Data security can be very well assured by use of kerbrose but the massive amount of data in cloud computing put a hindrance to the idea. So, we have studied kerbrose authentication help for the user as well as server, with the help of this protocol we assure that our data should be confidential In future; we accentuate on the implementation of the proposed architecture along with different comparisons to show the effectiveness of our proposed architecture.

V. REFERENCES

[1] Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.

[2] Farzad Sabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[3] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank

[4] Namdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG), CSI Sixth International Conference, Sept. 2012

[5] M.Venkatesh,M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. Recent Trends In Information Technology (ICRTIT), 2012 International Conference, April 2012.

[6] Prashant Rewagad, Yogita Pawar in. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[7] Ashish Agarwal, Aparna Agarwal. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946].

[8] Hai Yan, Zhijie Jerry Shi. Software Implementations of Elliptic Curve Cryptography. Information Technology: New Generations, Third International Conference, April 2006.

[9] Ravi Gharshi, Suresha. Enhancing Security in Cloud Storage using ECC Algorithm. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 7, July 2013.

[10] H. Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, R. Salleh. Make a Secure Connection Using Elliptic Curve Digital Signature. International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 ISSN 2229-5518 IJSER © 2012.

[11] Aqeel Khalique Kuldip Singh Sandeep Sood. Implementation of Elliptic Curve Digital Signature Algorithm. International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010.

[12] Neha Tritani,Ganesh R. Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography,2013

[13] B. Bryant, "Designing an Authentication System: A dialogue in Four Scenes". Project Athena document(February 1988). Available athttp://web.mit.edu/Kerberos/dialogue.html

[14] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "TheKerberos network authentication service (V5)". Network Working Group. Request for Comments: 4120. Available at http: //www.ietf.org/rfc/rfc4120.txt, 2005.

[15] S. Bellovin & M. Merrit, "Limitations of the Kerberos Authentication System," SIGCOMM Comput. Commun. Rev., 20(5):119–132, 1990.

[16] G. Bella and E. Riccobene, "Formal analysis of the Kerberos authentication system". Journal of Universal Computer Science, 3(12):1337–1381, 1997.

[17] G. Bella and L. Paulson, "Kerberos version IV: Inductive analysis of the secrecy goals". InESORICS '98. Springer, 1998.

[18] J. Kohl, "The use of encryption in Kerberos for network authentication". In CRYPTO '89. Springer, 1989.

[19] S. Stubblebine and V. Gligor. "On message integrity incryptographic protocols". In Symposium on Security and Privacy '92. IEEE, 1992.

[20] T. D. Wu. "A real-world analysis of Kerberos password security". In NDSS '99. The Internet Society, 1999.