ISSN 2320-9984 01 >
9 772320 998022

Volume 2 Issue 1 | March 2014 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Secured Transaction Mechanism over Cloud Computing SaaS layer

Neha Jain
M. Tech. Scholar
Department of Computer Science
Gyan Ganga Institute of Technology & Science
Jabalpur (M.P.) [INDIA]
Email : jainneha818@gmail.com

Prof. Ashok Verma
Associate Professor
Department of Computer Science
Gyan Ganga Institute of Technology & Science
Jabalpur (M.P.) [INDIA]

Abstract**—***In the recent era, cloud computing has evolved as a net centric, service oriented computing model. As defined by National Institute of Standards and Technology (NIST), cloud computing is model which enables the convenient, on-demand network access to a shared pool of configurable computing resources (e.g., servers, services, applications, networks, storage, and networks,).*

Cloud computing allow computer users access to powerful computers and software applications hosted by remote groups of servers, but security concerns related to data privacy are limiting them. There are big security concerns when using cloud services. In cloud computing security is very iportant since people and companies store confidential data in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. However, in order to enjoy the widely utilization of cloud computing through wired/wireless networking, providing sufficient assurance of information security such as confidentiality, authentication, non-repudiation, and integrity is the critical factor of success promotion.

This paper focuses on user authentication on cloud and on the way by which user information is securely transferred between client and server.

Keywords:—*Cloud computing, security, authentication, static password, dynamic password, time synchronization*

1. INTRODUCTION

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet, basically a step on from Utility Computing a collection/group of integrated and networked hardware, software and Internet infrastructure (called a platform). Using the Internet for communication and transport provides hardware, software and networking services to clients. These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface).

Cloud computing is an umbrella term used to refer to Internet based development and services A number of characteristics define cloud data, applications services and infrastructure:

Remotely hosted: Services or data are hosted on remote infrastructure

Ubiquitous: Services or data are available from anywhere.

Commodities: The result is a utility computing model similar to traditional that of traditional utilities, like gas and electricity - you pay for what you would want!

Figure 1: Characteristics of the Cloud Computing

A. Application Area

Cloud computing is a collection of technologies that allow IT resources to be virtualized, used on an on-demand basis and delivered via the Internet as services. Cloud computing can be considered a new computing paradigm in so far as it allows the utilization of a computing infrastructure at one or more levels of abstraction, as an on-demand service made available over the Internet or other computer network. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time and the service is fully managed by the provider. Because of the its features of greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention Cloud Computing can be classified into 4 types on the basis of location where the cloud is hosted:-

Public Cloud: A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. It is owned by a cloud provider selling cloud services and, by definition, is external to an organization..

Private Cloud: A private cloud a proprietary network or a data center that supplies hosted services to a limited number of people. It may be managed either by the organization or a third party, and may be hosted within the organization's data center or outside of it.

Community Cloud: A community cloud is somewhat similar to a private cloud, but the infrastructure and computational resources are shared by several organizations that have common privacy, security, and regulatory considerations, rather than for the exclusive use of a single organization.

Hybrid Cloud: A hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables interoperability.

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The three delivery models are the SaaS, PaaS and IaaS which provide infrastructure resources, application platform and software as services to the consumer.

1) Software-as-a-Service- SAAS is defined as a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network. Also known as "on demand" software, it is the most mature type of Cloud Computing because of its high flexibility, proven support services, enhanced scalability, reduced customer maintenance, and reduced cost due to their multi-tenet architectures. It is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

2) Platform-as-a-Service- PAAS provides infrastructure on which software developers can build new applications or extend existing applications without requiring the need to (purchase development, QA, or production

server infrastructure. It is a model of software deployment where the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber.

3) Infrastructure-as-a-Service- Infrastructure-as-a-Service (IaaS) is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted Security provisions beyond the basic infrastructure are carried out mainly by the cloud subscriber.

Security is one of the major issues which is ruining the growth of cloud computing. It is not always convenient, from a user perspective, to over-protect a service. If you make the login process too hard for a user, the user might grow tired of that service. It is a question of what you store or what information is available in a service. It is also important for the cloud providers to have good security standards in order for the common users to trust the cloud, for future growth of the cloud technology. Cloud computing can also mean big risks in the integrity, privacy areas and also greatly in users authentication. In a cloud system, company susceptible data and information will be stored on third-party servers, and user will possibly have very inadequate understanding or control regarding this information. So, there was a great demand for strong authentication system, which will not going to allow, the unauthorized user to access the cloud.

Mobile Ad hoc Networks (MANETs) are technically different from the traditional wireless networks (e.g. wireless LANs, cellular, digital trunked radio or satellite networks). In traditional wireless networks, the fixed network infrastructures such as access points, base stations or satellites are necessarily required to function as the repeaters to relay/ retransmit the signal from one node to the others. However, none of these network infrastructures is required in ad hoc networks, that is why ad hoc networks are sometimes called as infrastructure less wireless networks.

Moreover, in traditional wireless networks, data can be transmitted from source to destination within two hops. One hop is required to send data from source to fixed infrastructure, and another from this fixed infrastructure to destination. While data can be sent to destination with one or more hops in ad hoc networks. This means that data can be directly sent to destination by using just one hop if destination is in transmission range of source. However, if it is not in this range, data can be delivered through one or more intermediate nodes until reaching destination. This is simply called multihop communication.

2. PROBLEMS IN CLOUD COMPUTING

In a complex corporate IT environment passwords are very often the only possible means of protection against unauthenticated intruders. To ensure security of corporate networks is a never ending task of system administrators. That is why passwords are widely used to prevent frauds and system cracks. But very often static passwords are not enough and extra security is needed. As these static passwords are easy to guess and employees, customers, business partners write them down, send them in e-mails, they become ineffective. Therefore, different cloud providers have lately started with one time

password with two-factor authentication. The problem with their solutions is that it cost money, for the user or the provider, it can be complicated to use, or that the user have to carry a separate authentication device with him at all time.

One of the main concerns regarding cloud services is the security part, and is one large factor to why companies and customer hesitate to migrate their services into the cloud. At the same time, the security must be easy for the customers to understand and appeal to all kinds of people with different technical knowledge. And lastly, the security solutions should be very cheap or free of charge to implement, both for providers and customers, to attract more people to the cloud. So, in conclusion, for cloud services to grow even more, it needs a simple and cheap security solution.

3. EXISTING SYSTEM

In the promoting of cloud computing services, the issue of data security is one of the most important problems to be solved. Today's network construction, safety products, and encryption protocol have been protected the safety of data transmission basically; Data storage security can be solved through technical means in the design stage of cloud services, such as redundancy, parity, user authentication and access control; Data management security involves many aspects, the first is to improve the relevant laws and regulations as soon as possible, and the second is compatible with data between cloud computing service providers to ensure that users can seamlessly pan data, and service providers should establish a rapid and effective disaster recovery mechanisms to guarantee the availability of the data.

At present, in a short period of time, the cloud computing cannot completely replace traditional computing. It is still not being fully accepted that to manage data by a third party, especially for large enterprises and government departments.

In order to take full advantages of cloud computing characteristics, some large enterprises with strong economic and technological strength have begun to try to establish their own cloud computing platforms, such as China Mobile Big Cloud, but the Chinese government is still in a wait-and see.

It is foreseeable that in the near future, the average user will not shift entirely to the cloud computing model, firstly, because of the aforementioned security reasons, and secondly, they also hoard some computing devices, turning to cloud computing means to abandon existing investments. But some businesses with low level data confidentiality or even completely open can use commercial cloud computing model, such as some entertainment sites, SNS sites as well as public service platform, such as network library and public information release platform and so on. In addition, enterprises can also try to separate from the business, one part of the businesses involves confidential information are still running in the local network in accordance with the original mode and the other part complete by the cloud computing platform.

Cloud computing becomes more and more familiar to people, and its application field becomes more and more widely. How to build secure computer cloud computing environments becomes one of the hot research subjects. In this paper, from the definition of clouding computing, introduced its development status, and analysized the security problems. Put forward some trains of thought about the security, and at last this paper believes that trusted cloud computing will be a promising direction of the future cloud security researches. [1]

This article discusses cloud computing data security issues, including tile security of data transmission, storage, security and management of security. Focus on universal data management affect cloud security analysis, and pointed out that a breakthrough in the development of this cloud computing, try to enumerate the corresponding strategies and long-term development direction. [2]

Cloud computing materializes the vision of utility computing. Tenants can benefit from on demand provisioning of compute, storage, and networking resources according to a pay-per-use business model. Tenants have only limited visibility and control over network resources. The owners of cloud computing facilities are also facing challenges in various aspects of providing and efficiently managing IaaS facilities. In this work we present the networking issues in IaaS and federation challenges that are currently addressed with existing technologies. We also present innovative software-defined networking proposals, which are applied to some of the challenges and could be used in future deployments as efficient solutions. [3]

Cloud computing will play a major role in the future Internet of Services, enabling on-demand provisioning of applications, platforms, and computing infrastructures. However, the cloud community must address several technology challenges to turn this vision into reality. Specific issues relate to deploying future infrastructure-as-a-service clouds and include efficiently managing such clouds to deliver scalable and elastic service platforms on demand, developing cloud aggregation architectures and technologies that let cloud providers collaborate and interoperate, and improving cloud infrastructures' security, reliability, and energy efficiency. [4]

With the development of cloud computing, simulation can use the sharing software resource which is provided by cloud. This paper designed the architecture and modules of simulation in cloud. The simulation cloud workflow and management were proposed. We designed and analyzed how to efficiently schedule the knowing and unknowing compute resources to support discrete simulation in cloud computing. [5]

4. PROPOSED WORK

1. High secure and verification mechanism for cloud storage

Applications and databases in one location and those applications and databases can be accessed by any authorized users. That makes users need not to have infrastructure required for them at user side. User feels free and need not to have more knowledge on infrastructure maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud computing a very challenging and very difficult task, mostly for users who have limited computing resources and capabilities. By enabling public audit ability for cloud data storage security is very importance so that users can resort to an external audit party to check the integrity of outsourced data when they want to get that data. third party auditor (TPA) should be more secure, to do that it should met the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without storing the copy of the original data, and it should not have additional burden to the cloud user; 2) he third party auditing process should bring in no new vulnerabilities towards user data privacy.

2. Secure data storage and retrieval in cloud

With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, Organizations across the world generate a large amount of Data daily. This data would be more useful to cooperating Organizations if they were able to share their data. Two major Obstacles to this process of data sharing are providing a common Storage space and secure access to the shared data.

3. Secure Cloud Storage Service with an Efficient DOKS Protocol

Storage services based on public clouds provide customers with elastic storage and on-demand accessibility. However, moving data to remote cloud storage also raises privacy concerns. Cryptographic cloud storage and search over encrypted data have attracted attentions from both industry and academics.

4. Providing a secure data forwarding in cloud storage system using threshold proxy re encryption scheme

Cloud computing treats the resources on the Internet as a unified entity, cloud. A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers. Storing data in a third party's cloud system causes serious concern on data confidentiality. In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method. General encryption schemes protect data confidentiality but also limit the functionality of the storage system because a few operations are supported over encrypted data.

5. Security Testing Mechanisms

This article does not cite any references or sources. Please help improve this article by adding citations to reliable sources. Un-sourced material may be challenged and removed. (December 2009)

Security testing is a process to determine that an information system protects data and maintains functionality as intended.

The six basic security concepts that need to be covered by security testing are: confidentiality, integrity, authentication, availability, authorization and non-repudiation. Security testing as a term has a number of different meanings and can be completed in a number of different ways. As such a Security Taxonomy helps us to understand these different approaches and meanings by providing a base level to work from.

Contents

1. Confidentiality
2. Integrity
3. Authentication
4. Authorization
5. Availability
6. Non-repudiation
7. Security Testing Taxonomy
8. See also

Confidentiality: A security measure which protects against the disclosure of information to parties other than the intended recipient that is by no means the only way of ensuring the security.

Integrity: A measure intended to allow the receiver to determine that the information provided by a system is correct.

Integrity schemes often use some of the same underlying technologies as confidentiality schemes, but they usually involve adding information to a communication, to form the basis of an algorithmic check, rather than the encoding all of the communication.

Authentication: This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that a product is what its packaging and labeling claims to be, or assuring that a computer program is a trusted one.

Authorization: The process of determining that a requester is allowed to receive a service or perform an operation.

Access control is an example of authorization.

Availability: Assuring information and communications services will be ready for use when expected.

Information must be kept available to authorized persons when they need it.

Non-repudiation: In reference to digital security, non repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and

that the recipient cannot deny having received the message.

Security Testing Taxonomy

Common terms used for the delivery of security testing;

Discovery - The purpose of this stage is to identify systems within scope and the services in use. It is not intended to discover vulnerabilities, but version detection may highlight deprecated versions of software / firmware and thus indicate potential vulnerabilities.

Vulnerability Scan - Following the discovery stage this looks for known security issues by using automated tools to match conditions with known vulnerabilities. The reported risk level is set automatically by the tool with no manual verification or interpretation by the test vendor. This can be supplemented with credential based scanning that looks to remove some common false positives by using supplied credentials to authenticate with a service (such as local windows accounts).

Vulnerability Assessment - This uses discovery and vulnerability scanning to identify security vulnerabilities and places the findings into the context of the environment under test. An example would be removing common false positives from the report and deciding risk levels that should be applied to each report finding to improve business understanding and context.

Security Assessment - Builds upon Vulnerability Assessment by adding manual verification to confirm exposure, but does not include the exploitation of vulnerabilities to gain further access. Verification could be in the form of authorised access to a system to confirm system settings and involve examining logs, system responses, error messages, codes, etc. A Security Assessment is looking to gain a broad coverage of the systems under test but not the depth of exposure that a specific vulnerability could lead to.

Penetration Test - Penetration test simulates an attack by a malicious party. Building on the previous stages and involves exploitation of found vulnerabilities to gain further access. Using this approach will result in an understanding of the ability of an attacker to gain access to confidential information, affect data integrity or availability of a service and the respective impact. Each test is approached using a consistent and complete methodology in a way that allows the tester to use their problem solving abilities, the output from a range of tools and their own knowledge of networking and systems to find vulnerabilities that would/ could not be identified by automated tools. This approach looks at the depth of attack as compared to the Security Assessment approach that looks at the broader coverage.

Security Audit - Driven by an Audit / Risk function to look at a specific control or compliance issue. Characterised by a narrow scope, this type of engagement could make use of any of the earlier approaches discussed (vulnerability assessment, security assessment, penetration test).

Security Review - Verification that industry or internal security standards have been applied to system components or product. This is typically completed through gap analysis and utilises build / code reviews or by reviewing design documents and architecture diagrams. This activity does not utilise any of the earlier approaches (Vulnerability Assessment, Security Assessment, Penetration Test, Security Audit)

This work focuses on security aspect of cloud computing. For security following methodologies are adapted

- Authentication
- Authorization
- Confidentiality
- Integrity
- Non-Repudiation

- Availability

This work proposes to implement a new technique of authentication and authorization and will display the methodology adapted using an example cloud SaaS based application for Shopping Cart.

The proposed work shall be consisting of the following steps:

Proposed Shopping cart will have following factors:

- Admin(s)
- Moderators
- Customers

Following are the various authorizations which will be there in the proposed system

- add
- delete
- view
- approve
- Edit

The shopping cart will be having the roles of the various actors defined as per the requirement. Every actor will have a User name and password for initial authentication ey Identification will be used for transactions Proposed work shall provide an Identity to every actor generated automatically which will be verified during all transactions at the Data Center Level. The Key will be refreshed after each session/transaction or specified duration and forwarded to every user for future transactions. The security of the system shall be checked with the various techniques from the following available techniques:

Common terms used for the delivery of security testing;

- Discovery
- Vulnerability Scan
- Vulnerability Assessment
- Security Assessment
- Penetration Test
- Security Audit
- Security Review

5. CONCLUSION

It is foreseeable that in the near future, the average user will not shift entirely to the cloud computing model, firstly, because of the aforementioned security reasons, and secondly, they also hoard some computing devices, turning to cloud computing means to abandon existing investments. But some businesses with low level data confidentiality or even completely open can use commercial cloud computing model, such as some entertainment sites, SNS sites as well as public service platform, such as network library and public information release platform and so on. In addition, enterprises can also try to separate from the business, one part of the businesses involves confidential information are still running in the local network in accordance with the original mode and the other part complete by the cloud computing platform.

REFERENCE:

[1] Liu Xiao-hui, Song Xin-fang "Analysis on Cloud Computing and its Security ",The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka, 978-1-4673-4463-0/13/$ ©2013 IEEE

[2] Du meng, "Data security in cloud computing", The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka, 978-1-4673-4463-0/13©2013 IEEE

[3] Siamak Azodolmolky, Philipp Wieder, and Ramin Yahyapour, Gesellschaft für Wissenschaftliche

Datenverarbeitung mbH Göttingen (GWDG), "Cloud Rafael Moreno-Vozmediano, Rubén S. Montero, and Ignacio M. Llorente, "Key Challenges in Cloud Computing", Internet of Services, Published by the IEEE Computer Society 1089-7801/13 © 2013 IEEE

[4] Qunhua Pan, Juhui Pan, Chuncai Wang, "Simulation in Cloud Computing Environment", 2013 International Conference on Service Science, 2165-3836/13 © 2013 IEEE DOI 10.1109/ICSS.2013.61

[5] "Dynamic Authentication: Need than a Choice", A. Saxena, Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference, 10 (1) (2008), 214.

[6] "Value of Cloud Computing by the View of Information Resources", Chunlan Li, Zhonghua Deng, 2011 International Conference on Network Computing and Information Security, 978-0-7695-4355-0/11 $26.00 © 2011 IEEE DOI 10.1109/ NCIS.2011.30.

[7] "A survey on security issues in service delivery models of cloud computing", S. Subashini n, V. Kavitha, Anna University Tirunelveli, Tirunelveli, TN627007, India, Journal of Network and Computer Applications 34 (2011) 1–11.

[8] "Privacy and consumer risks in cloud computing", Dan Svantesson, Roger Clarke, computer law & security review 26 (2010) 391e97, @ 2010 Svantesson & Clarke. Published by Elsevier Ltd. doi:10.1016/ j.clsr.2010.05.005.

[9] "Guidelines on Security and Privacy in Public Cloud Computing", Wayne Jansen, Timothy Grace.

[10] "Cloud computing" http:// en.wikipedia.org/wiki/ Cloud_computin.

[11] "Authentication" http:// en.wikipedia.org/wiki/Authenticatio.