The Cloud Computing Security Secure User Authentication Technique (Multi Level Authentication)

Shabir Ahmad, Bilal Ehsan

A b s t r a c t - Cloud computing is becoming an adoptable technology for many of the organizations with its dynamic scalability and usage of virtualized resources as a service through the Internet. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training of new personnel, or software licensing. The recent emergence of cloud computing has significantly changed everyone's opinion of infrastructure architectures, development models and software delivery. From a security perspective, several unchartered risks and challenges have been introduced from this move to the clouds, failing much of the effectiveness of traditional protection mechanisms.

As a result the aim of this paper is twofold; first, to evaluate cloud security by identifying unique security requirements and second, try to present a viable solution that eliminates these potential threats. This paper proposes a Multi-Level Authentication (MLA) of cloud user for secure access to the network and data centers. MLA protects cloud resources against unauthorized access by enforcing access control mechanisms. In our idea of MLA, We would like to outline our opinions about the usability of traditional text based password authentication along with biometrics authentication.

Keywords - Authentication, Cloud Computing, Biometrics, Server, Client, Data Centers, Security.

1. Introduction

Cloud computing is a model for enabling universal, suitable, on-demand network access to a mutual pool of configurable computing resources (different networks, servers, data storage, services and applications) those may be rapidly provisioned and released with minimal management effort or service provider inter-action. Today Small and Medium Business (SMB) companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best business applications or significantly boost their infrastructure resources, all at very low cost. Cloud computing applications have broadly three areas known as cloud delivery models: Infrastructure as a service **(IaaS)**, Platform as a service **(PaaS)**, Software as a service **(SaaS)**. So far, there have been little scientific definitions trying to develop a complete definition of the cloud computing phenomenon.

As the cloud computing is achieving popularity periodically, alarms (concerns) are being voiced about the security issues presented through the adoption of this new model. The usefulness and efficiency of traditional protection mechanisms are being reviewed, as the characteristics of this innovative deployment model, differ widely from them of traditional architectures.

In this paper we attempt to expose the unique security challenges introduced in a cloud environment and clarify issues from a security perspective. The notion of trust and security is investigated and specific security requirements are documented.

Authentication plays an important role in protecting resources against unauthorized use. But still the most widely used authentication system is based on the use of text passwords. Text based passwords are not secure enough for many applications that enforce security by access control mechanisms. Authentication based on text based passwords has major drawbacks. More sophisticated authentication process is costly and may need additional equipment or hardware.

This paper proposes a security solution regarding secure user authentication to the cloud network and data centers, which leverages clients from the security burden, by implementing Multi-Level Authentication (MLA) technique.

MLA is simple enough, cost effective and does not need any additional hardware. Thus MLA can be used in cloud computing as well as corporate world with ease.

- *Shabir Ahmad is currently pursuing M.Phil degree in computer sciences and working as lecturer computer at Govt. College of Commerce, Multan, Pakistan. E-mail: mian_shabbir@hotmail.com*
- *Bilal Ehsan is currently pursuing M.Phil degree in computer sciences and working as lecturer computer at Govt. College of Commerce, Multan, Pakistan. E-mail: bilal_636@hotmail.com*

2. Overview of cloud computing

This part of paper presents a general overview of cloud computing, what security issues are being faced in could-computing environment and how these can be overcome with purposed solutions.

2.1 Definitions

The main idea behind cloud computing is not a new one. John McCarthy in the 1960s already envisioned that computing facilities will be provided to the general public like a utility. The term "cloud" has also been used in various contexts such as describing large ATM networks in the 1990s. However, it was after Google's CEO Eric Schmidt used the word to describe the business model of providing services across the Internet in 2006, that the term really started to gain popularity. Since then, the term cloud computing has been used mainly as a marketing term in a variety of contexts to represent many different ideas. Certainly, the lack of a standard definition of cloud computing has generated not only market hypes, but also a fair amount of doubt and uncertainty. For this reason, recently there has been work on standardizing the definition of cloud computing.

NIST definition of cloud computing "Cloud computing is a model for enabling universal, suitable, on-demand network access to a mutual pool of configurable computing resources (different networks, servers, data storage, services and applications) those can be rapidly provisioned and released with minimal management effort or service provider inter-action".

The main reason for the existence of different perceptions of cloud computing is that cloud computing, contrasting other scientific terms, is not a new technology, but rather a new operations model that brings together a set of existing technologies to run big business in a diverse (unusual) way. Indeed, most of the technologies used by cloud computing, such as virtualization and as per service (utility) pricing, are not new. Instead, cloud computing leverages these existing technologies to meet the technological and economic requirements of today's demand for information technology.

2.2 Grid and Cloud Computing

There is an on-going confusion about the relationship between Grids and Clouds. Sometimes, it seems that Grids as "on top of" Clouds and in some situation it seems vice versa or identical. More surprising, even elaborate comparisons still have different views on what "the Grid" is in the first instance, hence making the comparison embarrassed (cumbersome). In fact most ambiguities can be quickly resolved if the underlying concept of Grids is examined first: just like Clouds, Grid is basically a concept rather than a technology thus leading to many potential misunderstandings between individual communities.

Grid computing is a distributed computing paradigm that coordinates networked resources to achieve a common computational objective. The development of Grid computing was originally driven by scientific applications which are usually computation-intensive.

Cloud computing is similar to Grid computing in that it also employs distributed resources to achieve application-level objectives. However, cloud computing takes one step further by leveraging virtualization technologies at multiple levels (hardware and application platform) to realize resource sharing and dynamic resource provisioning.

Grid Computing emerged in the early 1990s, as high performance computers were inter-connected through fast data communication links, with the aim of supporting difficult calculations and data-intensive technical applications. Grid computing is defined as ''a hardware and software infrastructure that offers trusty consistent, persistent, and low-cost access to high-end computational capabilities''.

Cloud Computing Service Models are:

The main models of clouds (currently in use) are as follow:

2.2.1 (Cloud) Infrastructure as a Service (IaaS), also referred to as *Resource Clouds*, provide (managed and scalable) resources as services to the user – in addition, they mostly provide improved virtualization potential. In the same way, different resources may be provided via a service interface like:

Data & Storage Clouds provide reliable access to data of potentially dynamic size, deliberate resource usage with access requirements and / or quality definition.

Examples: Amazon S3, SQL Azure.

Compute Clouds deals access to computational resources, i.e. microprocessors (CPU). Compute Cloud Providers therefore typically offer the capability to provide computing resources (i.e. raw access to resources unlike PaaS that offer full software stacks to develop and build applications), typically virtualized, in which to accomplish cloudified services and applications. IaaS (Infrastructure as a Service) offers additional capabilities over a simple compute service.

Examples: Zimory, Amazon EC2, Elastichosts.

2.2.2 (Cloud) Platform as a Service (PaaS), provide computational resources via a *platform* upon which applications and services can be hosted after development. PaaS specifically formulates (make) use of dedicated APIs to

control the behavior of a server hosting engine which executes and replicates the execution according to user requests (e.g. access rate). As each provider exposes his / her own API according to the respective pinpoint capabilities, the applications developed for one specific cloud provider cannot be moved to another cloud.

Examples: Force.com, Google App Engine, Windows Azure (Platform).

2.2.3 (Clouds) Software as a Service (SaaS), also sometimes referred to as *Service or Application Clouds* are offering implementations of specific business functions and business processes that are provided with specific cloud capabilities, i.e. they provide services / applications *using* a cloud network, (infrastructure) or platform, instead of providing cloud features themselves.
Examples: SAP Business by Design, Google Docs, Sales-force CRM.

3. Existing Research Work

According to a recent Merrill Lynch research note, Cloud computing is expected to be a $160-billion addressable market opportunity, including $95-billion in business and productivity applications, and another $65-billion in online advertising. So far, only few cloud committed research projects in the widest sense have been started, most prominent amongst them probably Open Nebula and Reservoir. However, many projects have initiated a dedicated cloud related research track investigating into how to move existing capabilities onto and into the cloud. What is more, countless projects have addressed similar concepts in related areas exhaustively and have provided relevant results that need to be taken up in order to exploit relevant intellectual results, as well as to ensure that no effort is unnecessarily repeated, thus reducing the chance for impact and uptake.

4. Gaps & Open Areas

The main gaps that can be identified relate to the following aspects:

4.1 Manageability and Self-detection

Cloud systems focus on intelligent resource management so as to ensure availability of services through their replication and distribution. In principle, this ensures that the amount of resources consumed per service / application reflects the degree of consumption, such as access through users, size of data etc. Whilst most cloud system allow for main features related to elasticity and availability, the management features are nowhere near optimal resource usage – issues not only relevant for cost reduction, but as well for meeting the green agenda and for ensuring availability when resources are limited.

4.2 Data Management

The amount of data available on the web, as well as the throughput produced by applications, sensors etc. increases faster than storage and in particular bandwidth does. Hence in particular storage clouds should be able to cater for such means in order to maintain availability of data and thus address quality requirements etc.

4.3 Privacy & Security

Strongly related to the issues concerning legislation and data distribution is the concern of data protection and other potential security holes arising from the fact that the resources are shared between multiple tenants and the location of the resources being potentially unknown. In particular sensitive data or protected applications are critical for outsourcing issues.

5. Cloud Computing Security (The Existing Core Issue)

Cloud computing security concerns all the aspects of making cloud computing secure. Many of these aspects are not unique to the cloud setting: data is vulnerable to attack irrespective of where it is stored. Therefore, cloud computing security encompasses all the topics of computing security, including the design of security architectures, minimization of attack surfaces, protection from malware, and enforcement of access control. But there are some aspects of cloud computing security that appear to be specific to that domain are:

5.1. Trust

The thought of trust, used to the case of two parties involved in a operation, can be illustrated as follows: An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required.

Consequently, an entity can be considered trustworthy, if the people or parties involved in transactions with that entity rely on its sincerity.

5.2. Security identification of threats

Essentially securing an Information System (IS) involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures.

Security in general, is related to the important aspects of confidentiality, availability and integrity; they thus become building blocks to be used in designing protected systems. The cloud infrastructure suggests unique security challenges which have to be considered in detail.

5.2.1. Confidentiality and Privacy

Confidentiality means only authorized systems or parties can have the facility to access protected data. Due to the increased number of parties, devices and applications involved in the cloud, the threat on data will also compromise. This will lead to an increase in the number of access points. Assign data control to the cloud, contrary leads to an increase in the threat of data compromise. A number of concerns emerge regarding the issues of multi-tenancy, data remanence, application security and privacy.

Protecting a user's account from theft is an instance of a big problem of controlling access to objects, including memory, software, devices etc. Lack of strong authentication can lead to unauthorized access to users account on a cloud, leading to a breach in privacy.

Unauthorized access can become possible through the exploitation of an application vulnerability or lack of strong identification, bringing up issues of data confidentiality and privacy. In addition, the cloud provider is responsible for providing secure cloud instances, which should ensure users confidentiality.

5.2.2. Integrity

Integrity means that resources can be modified only by authorized parties or in authorized ways. Data Integrity refers to protecting data from unauthorized deletion, modification or recreation. Organizations can achieve greater confidence in data and system integrity by preventing unauthorized access. Due to the increased number of entities and access points in a cloud environment, authorization is critical in assuring that only authorized persons can interrelate with data.

5.2.3. Availability

Availability refers to the property of a system being accessible and usable upon demand by an authorized person. Availability refers to data, software but also hardware being available to authorized users upon demand. The system must have the ability to continue operations even in the possibility of a security violation. Cloud computing services present a heavy reliance on the resource infrastructures and network availability at all times.

6. Existing Authentication Solution

Trusted Third Party services within the cloud, leads to the establishment of the necessary Trust level and currently provides ideal solutions to preserve the confidentiality, authenticity and integrity of data and communications. The authentication of user using these services provides up-to 93% secure access in the cloud.

In Trusted Third Party services Public Key Infrastructure (PKI) and Single-Sign-On technique are used currently for user authentication. PKI deployed in concert with Single-Sign-On (SSO) mechanisms are ideal for distributed environments, such as cloud environments, where users navigate between an abundance of cross-organization boundaries.

In a Single-Sign-On environment, a user does not need to repeatedly enter passwords to access resources across a network. Instead the user signs on once using a password, smart card, or other authentication mechanism, and thereby obtains access to multiple resources on different machines.

PKI-based Single-Sign-On mechanisms are essential within a cloud environment, since they provide the means for a smooth, transparent strong authentication across different physical resources. SSO in concert with PKI enhances complex free, authorization and authentication processes. In practice this results in enhancing the security of the whole infrastructure, among other obvious technical issues, because an adequate level of usability is guaranteed.

6.1 Server and Client Authentication

Digital signatures in combination with SSO and LDAP, implement the strongest available authentication process in distributed environments while guaranteeing user mobility and flexibility. The signing private key can be used to authenticate the user automatically and transparently to other servers and devices around the network whenever he/she wants to establish a connection with them.

Authentication in the trusted environment organizational boundaries, allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. Shibboleth technology relies on a third party to provide the information about a user, named attributes.

In the proposed system architecture, this is performed by the TTP LDAP repository. It is essential to distinguish the authentication process from the authorization process. During the authentication process a user is required to navigate to his home organization and authenticate him-self. During this phase information is exchanged between the user and his home organization only.

7. Multi-Level Authentication (Proposed Solution)

This paper proposes a Multi-Level Authentication (MLA) of cloud user for secure access to the network and data centers. MLA protects cloud resources against unauthorized access by enforcing access control mechanisms. In our idea of MLA, We would like to outline our opinions about the usability of traditional text based password authentication along with biometric authentication.

Appropriate user authentication is a critical part of the access control that makes the major building block of any system's security.

Traditionally, User authentication has been traditionally based on something, that the user knows (typically a PIN, a password or a passphrase).

Unfortunately, traditional methods are based on properties that can be stolen, forgotten, breached, or lost by any means. Passwords often are easily accessible to colleagues and even occasional visitors and users because in traditional password, user normally gives his/her name, birthdays, hobbies, home cities etc. So text based password is only single factor/level of authentication which is easily accessible.

To overcome these problems, we purposed new idea for authenticity, which uses multiple layers of security to access cloud named Multi-Level Authentication (MLA). In our idea, we ensure that in addition to passwords, if we use a biometrics authentication which is 100% reliable and not so easy to achieve. Biometrics are automated methods of identity verification or identification based on the principle of measurable physiological or behavioral characteristics such as a fingerprint, an iris pattern. Biometric characteristics are (or rather should be) unique and not duplicable or transferable. So highly confidential data, use MLA is much more secure than traditional authentication.

The MLA authentication consists of passwords and fingerprints that can be implemented physically in the presence of a user as well as by using smart cards. As cloud client insert the card into the card reader device attached with his/her computer, the cloud server will ask for entering the password and for scanning the fingerprints and system will processed for a process for matching the password and fingerprints with the smart card information. As the matching is done, applications of cloud computing are ready for use. When cloud computing clients finished his/her work, he/she will pull back the smart card.

8. Conclusion/Discussion

Without any doubt cloud computing will support a surplus of information systems as the benefits outnumber its shortcomings. Cloud computing offers deployment architecture, with the capability to deal with vulnerabilities recognized in traditional information system but its energetic characteristics are able to prevent the effectiveness of traditional countermeasures.

Security-sensitive environments protect their resources against unauthorized access by enforcing access control mechanisms. This paper attempts to propose a one of major security challenges in a cloud environment, which support multi level authentication of a user. In this paper, we proposed a new idea of integrating text based passwords with fingerprints (biometric) to strengthen the security of systems. We briefly discussed how the proposed authentication system could help enhance existing popular systems.

It will remove all the pitfall of existing authentication techniques and bring out clients from the security trouble. It really operates in a top-down fashion, as every layer needs to trust the layer immediately below it, and requires a security guarantee at a procedural, operational and technical level to enable secure access with it. A smart card having MLA information serves as a reliable electronic ''passport'' that establishes an entity's identity, credentials and responsibilities.

We have discussed several security issues that currently affect cloud systems. However, there may be many undiscovered security issues. Research is presently being conduct on the different well-known issues faced by cloud systems and its possible solutions. However there is still a need for better solutions if cloud systems are to be widely adopted.

References

1) DoD Computer Security Center, DoD 5200.28-STD, 1985 (Trusted computer system evaluation criteria)

2) Future Generation Computer Systems (2010), A. Nagarajan, V. Varadharajan, research on Dynamic trust enhanced security model for trusted platform based doi:10.1016/j.future.2010.10.008.

3) Computers & Security 11 (1) (1992) R. Sherman, Distributed systems security.

4) International Journal of Medical Informatics (2002) research by D. Lekkas, S. Gritzalis, S. Katsikas on Quality assured trusted third parties for deploying secure Internet-based healthcare applications.

5) Top threats to cloud computing, from Cloud Security Alliance, 2010.

6) A scalable, commodity data center network architecture (Al-Fares Metal (2008). In: Proc SIGCOMM

7) From, www.aws.amazon.com/ec2, Amazon Elastic Computing Cloud"

8) A Berkeley view of cloud computing by Armbrust M et al (2009) Above the clouds. UC Berkeley Technical Report

9) Uniform resource identifier (URI) by Berners-Lee T, Fielding R, Masinter L (2005) RFC 3986

10) Using distributed voluntary resources to build clouds from Chandra A et al (2009) Nebulas. In: Proc of HotCloud

11) On delivering embarrassingly distributed cloud services by Church K et al (2008). In: Proc of HotNets

12) www.en.wikipedia.org/wiki/Cloudcomputing by Cloud Computing on Wikipedia, 20 Dec 2009

13) http://www.gogrid.com from the GoGrid, Cloud Hosting & Cloud Computing and Hybrid Infrastructure

14) http://code.google.com/appengine, Google App Engine

15) A scalable and flexible data center network by Greenberg A, Jain N et al (2009) VL2. In: Proc SIGCOMM

16) A scalable and fault-tolerant network structure for data centers. In: Proc SIGCOMM, by Guo C et al (2008) DCell.

17) Art Conklin, Glenn Dietrich, Diane Walz, "Password-Based Authentication: A System Perspective", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

18) Matya, V., Rıha, Z. (2000). Biometric Authentication Systems.