IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-2, Issue-10 E-ISSN: 2347-2693

Authentication Model on Cloud Computing

Swapnil Rajesh Telrandhe[1*] and Deepak Kapgate[2]

[1*,2]G.H Raisoni Academy of Engineering & Technology, Nagpur

Received: 22 Sep 2014 Revised: 10 Oct 2014 Accepted: 24 Oct 2014 Published: 31 Oct 2014

Abstract: Cloud computing is an internet-based computing, where a set of resources and services such as applications, Storage and servers are delivered to computers and devices through the Internet. It incorporates large open distributed system, virtualization and internet delivery of services, dynamic provision of reconfigurable resources and on – demand operations. Cloud Computing is continuously growing and showing consistent growth in the field of computing. The major challenging task in cloud computing is the security and privacy issues caused by the outsourcing of infrastructure, sensitive data and critical applications and its multi- tenancy nature. The security for Cloud Computing is emerging area for research work and this paper discusses various types of authentication methods and multi-factor user authentication.

Key words: Cloud Computing, Security Issues, Cloud Computing Layers, Architecture diagram of AMOCC

I. INTRODUCTION

The increasing need for securing access to computer systems and networks from intruders is growing rapidly as the type of data and capabilities of these systems is significantly sensitive. To provide access to these systems while providing illegitimate access is the key requirement of the modern day computing. Since biometric system do not identify the person by what he/she knows (a code) or by what he/she possesses (a card), but by unique characteristic that is difficult for different individuals to reproduce, the possibility of forgery is greatly reduced. And it is difficult to implement because it requires huge setup and hardware for authentication. The most commonly used method of securing any system or application is the textual password i.e. easy to implement and easy to remember also. But the textual password has many drawbacks, like it can be cracked very easily by intruders, it can be easy to guess, it is very commonly implemented method, etc. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available.

The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST):-"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models"[1]

Necessity

Cloud computing is now becoming a business standard. It simplifies the user's accessibility. It provides a virtual storage space to the user which could be used without bothering about the details of the entire mechanism. Here are some other reasons why every enterprise might need cloud computing for their business:

- Cost savings - Cloud computing removes the requirement of a company to invest in storage hardware and servers.
- Focusing on the business -Since all the services will execute over the internet, a company does not have to bother about technical issues and other problems associated with physical storage and backup. A company can thus focus more on their core business.
- Performance - It delivers reliable performance irrespective to the geographical location of the user. Another key feature could be the automatic updating of services and applications.
- Security - Cloud Computing offers optimum security which protects you against any unauthorized access, modification and loss of data.
- Flexibility - Even if part of the cloud environment fails or stops working, the other resources continue to work until the problem is fixed.

© 2014, IJCSE All Rights Reserved

II. Work on cloud security

This section aims to discuss which factors drive an upward trend of cloud adoption in information system development. Moreover, the activities that current cloud users prefer and the way they use them are also mentioned in this section.

- *Characteristics of cloud services*

It is widely recognized that Service Providers (SPs) view software services as their business basis and they make these accessible to Service Users via Internet-based interfaces. Currently, Infrastructure Providers (IPs) struggle to build the large data centers called Cloud Centers for the provision of the cloud-computing infrastructure required to host services. Therefore, cloud services can be defined as a business model provided by IPs[9]. Cloud services with general purpose data-centre capacity are elastic, scalable and cost-saving. SPs could choose their optimum resource requirements when moving their computing infrastructure to IPs (Leavitt, 2009; Vaquero et al., 2009). This section aims to discuss types of cloud services and make comparisons of cloud service providers. Moreover, the issue of private clouds and successful examples of the usage of cloud services are also dealt with[2].

- *Authentication requirements*

1) Sensitivity: The authentication system must be able to detect any content modification or manipulation. For any authentication algorithms, detection of any manipulation is required and not only content modification[6].

2) Robustness: The authentication system must tolerate content preserving manipulations[6].

3) Localization: The authentication system must be able to locate the image regions that have been altered[6].

4) Recovery: The authentication system must be able to partially or completely restore the image regions that were tampered[6].

5) Security: The authentication system must have the capacity to protect the authentication data against any falsification attempts[6].

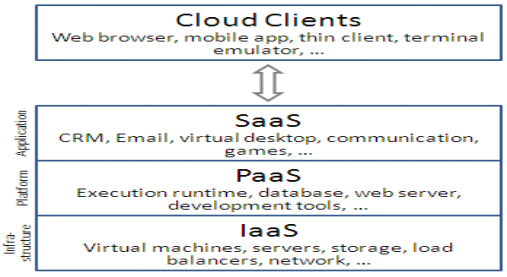

Figure: Cloud Computing Layers

1) MAC ADDRESS AUTHENTICATION

A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet.

Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model. MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. A network node may have multiple NICs and each must have one unique MAC address per NIC.

MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64. The IEEE claims trademarks on the names EUI-48 and EUI-64, in which EUI is an abbreviation for Extended Unique Identifier[4].

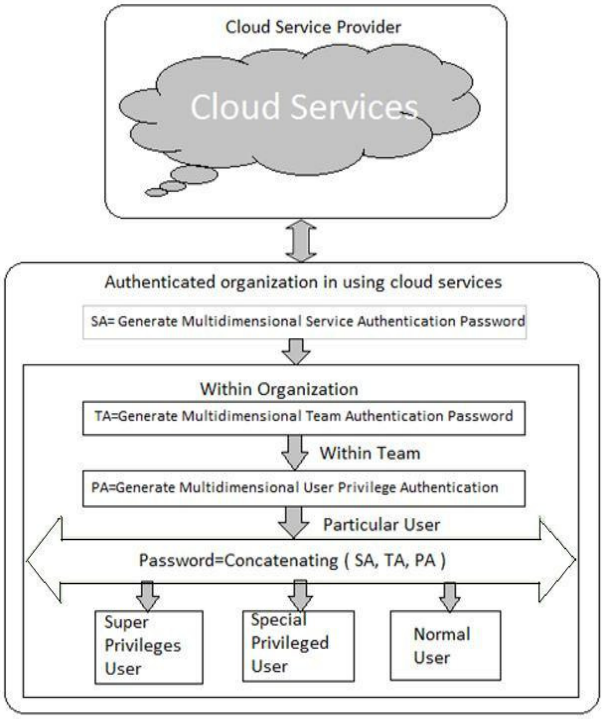

Figure: Architecture diagram of AMOCC

© 2014, IJCSE All Rights Reserved

Each wireless network interface card (NIC) used by a wireless client has a unique media access control (MAC) address. A client's MAC address can be used to control access to the access point. MAC authentication can be done either locally or with a RADIUS server. MAC authentication can be the only method of client authentication or it can be performed in addition to other authentication methods. When used in conjunction with other authentication methods, MAC authentication is performed after other authentication. MAC authentication is configured on a per virtual access point basis and can be set to one of the following options:

- Disabled—No MAC authentication is performed for the virtual access point.
- Local—The client's MAC address is checked against a global list of client MAC addresses that are allowed or denied access to the network. You configure the list with the station-mac-filter statement in the hierarchy. This function is similar to configuring a MAC filter. MAC authentication of a client fails if either an allow-list is specified and the client's MAC. is not in the list, or a deny-list is specified and the client's MAC is in the list. In either case the client is denied association. The global list is applicable to every virtual access point, but the usage of this list is determined by the MAC authentication mode for each virtual access point.

2) *DIGITAL CERTIFICATE AUTHENTICATION*

A certificate is an electronic document that is used to identify an individual, a server, a company, or some other entity, and to associate that identity with a public key. Like a driver's license, a passport, a student ID, a library card, or other commonly used personal IDs, a certificate provides generally recognized proof of a person's identity. Certificates use public key cryptography to address the problem of impersonation.

To obtain a driver's license, you typically apply to the Department of Motor Vehicles, which verifies your identity, your ability to drive, your address, and other pertinent information before issuing you a driver's license. To obtain a student ID, you apply to a school or college that, in turn, performs different checks (such as whether you paid your tuition) before issuing the student ID. To obtain a library card, you may only need to provide your name and a utility bill with your address on it. Certificates work much the same way as any of the previously mentioned forms of identification. Certificate authorities (CAs) are entities that validate identities and issue certificates. Clients and servers use certificates issued by the CA to determine the other certificates that can be trusted. Just like the methods to validate other forms of identification can vary depending on who is issuing the ID and the purpose for which it is being used, the methods used to validate an identity can vary depending on the policies of a given CA. In general, before issuing a certificate, the CA must use its published verification procedures for that type of certificate to ensure that an entity requesting a certificate is, in fact, who it claims to be.

The certificate issued by the CA binds a particular public key to the name of the entity that the certificate identifies; for example, the name of an employee or a server. Certificates help to prevent the use of false public keys for impersonation. Only the public key that is certified by the certificate will work with the corresponding private key that is owned by the entity identified by the certificate.

In addition to a public key, a certificate also includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The CA digital signature allows the certificate to function as a letter of introduction for users who know and trust the CA, but do not know the entity that is identified by the certificate[3].

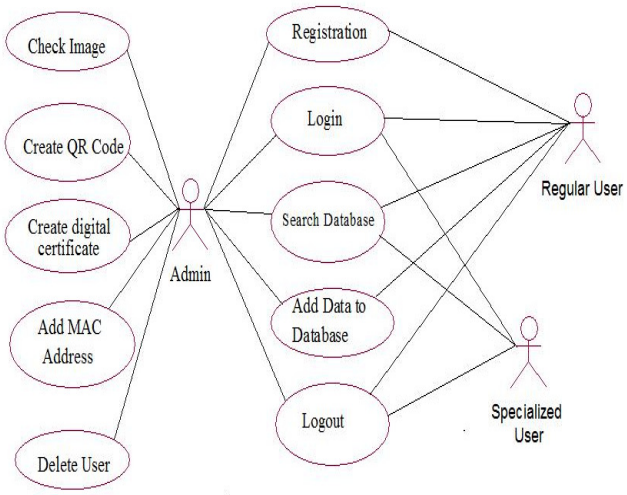

Figure: Use-Case Diagram

Certificate-based authentication: Certificate-based authentication is based on what the user has, which is the user's private key, and what the user knows, which is the password that protects the private key (if the key is not located in a secure keystore). However, both of these assumptions are true only if unauthorized personnel have not gained access to the user's workstation or password, the password for the client's private key database has been set, and the client is set up to request the password at reasonably frequent intervals. Although certificate-based authentication addresses security, it does not address issues related to the physical access of individual workstations or passwords. Public key cryptography only verifies that a private key that is used to sign some information corresponds to the public key in a certificate. It is your responsibility to protect the

© 2014, IJCSE All Rights Reserved

physical security of a workstation and to keep the password for the private key a secret.

Authentication using digital certificates: Authentication is the process of confirming an identity. In the context of how a network interacts, authentication involves the confident identification of one party by another party. Authentication over a network can take many forms, and the use of certificates is one way of supporting that authentication. Network interactions generally occur between a client and a server. Client authentication is the confident identification of a client by a server; that is, identification of the person assumed to be using the client. Server authentication is the confident identification of a server by a client; that is, the identification of the organization assumed to be responsible for the server at a particular network address.

3) PASSWORD AUTHENTICATION

A password authentication protocol (PAP) is an authentication protocol that uses a password.PAP is used by Point to Point Protocol to validate users before allowing them access to server resources. Almost all network operating system remote servers support PAP.

PAP transmits unencrypted ASCII passwords over the network and is therefore considered unsecure[8]. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP (the latter is actually a framework).

Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. Existing password authentication schemes can be categorized into two types: weak-password authentication schemes and strong-password authentication schemes. When compared to strong-password schemes, weak-password schemes tend to have lighter computational overhead, the designs are simpler, and implementation is easier, making them especially suitable for some constrained environments. Working cycle

Password Authentication: In most enterprises, the use of passwords is the primary means of authenticating a user. Unfortunately, it is also the weakest form of authentication. In today's digital world, the ways to bypass this form of security are trivial. While many enterprises focus on strengthening passwords, these efforts are by and large meaningless in the face of the tools that attackers can use. The tools provide criminals with easy ability to hack, trap, or crack most passwords easily. The use of password authentication is further weakened by software attacks. Password authentication logging software programs are embedded in email that are activated by clicking on the links in the email or by visiting a fake site that looks like the normal commercial site (phishing attack). It is now common that large commercial organized crime web gangs have developed keyboard logging software such that it will recognize the user's bank id and authentication passwords you enter when you logon to your bank's website to conduct a transaction. The id and password information is then sent within seconds to the organized crime servers somewhere in the world. They are then auctioned off, via the internet, to other organized criminals. The use of the id and password is then quickly used to begin emptying your bank account.

The use of passwords can be used in a layered identity defense strategy. What this means is that your enterprise will allow the use of user id and password to gain general access to low risk enterprise applications and information e.g. the enterprise portal. However, when the user tries to access applications or information that is higher risk, the enterprise should require stronger authentication. This may include the use of security tokens, digital certificates, biometrics, smartcards or combinations thereof in addition to the password.

4) QR CODE AUTHENTICATION

QR Code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional code) first designed for the automotive industry. The QR barcode is a two dimensional symbol developed by Denso Wave in 1994. More recently, the system has become popular outside the industry due to its fast readability and large storage capacity compared to standard UPC barcodes. The code consists of black modules (squaredots) arranged in a square pattern on a white background. The information encoded can be made up of four standardized kinds ("modes") of data (numeric, alphanumeric, byte/binary, Kanji), or through supported extensions, virtually any kind of data[5].

The code contains information in both the x-axis and y-axis, whereas traditional barcodes contain data in one direction only. The outer range is the quiet zone. The upper-left, upper-right, and left bottom square areas of QR code are used for position detection and pattern separators for positioning.

Figure: depicts basic block diagram of QR Code scanning with any image capturing device.

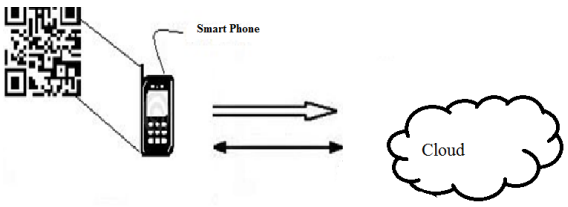

Figure: QR Code

Advantages of QR codes

- There is no need to write vital details down. A simple scan captures the desired information.
- QR Codes can be used to store addresses and URLs that can appear in magazines, on signs, buses,

© 2014, IJCSE All Rights Reserved

business cards or just about any product that users might need information about.

5) *IMAGE AUTHENTICATION*

Image Authentication techniques enable the recipients to verify the integrity of the received image. The increasing need for trustworthy distribution of digital multimedia in business, industry, defense etc. has lead to the concept of content-based authentication.[10]

Nowadays manipulating digital images efficiently and seamlessly has become very easy with the availability of powerful software and necessary to ensure confidentiality as well as integrity of the images that are transmitted.[7] Military, medical and
quality control images must be protected. To protect the authenticity of images, several approaches have been proposed. Number of image processing tools to change images for different purposes, it leads to problems such as copyright infringement and hostile tampering to the image contents. Image authentication techniques have been developed rapidly to verify content integrity and prevent forgery. Image hashing is an important method for image authentication.

III. CONCLUSIONS

There are many authentication schemes in the current state. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

Hence we provided more security to general authentication system so that no intruder can access the data. This will provide more security to any application or windows OS. This system will be providing authentication in five steps. They will be userid & textual password, digital certificate, Mac address, QR code, image authentication respectively. This advance security system will provide security from the intruders the attacker will not able to break the system easily. This system will act as a protecting cover to any application which needs more security and has some confidential data. The access method should be able to correctly authenticate the identity of an individual and then allow them access to the defined resource this will provide more security to any application or windows OS.

The authentication model is still in its early stages. Moreover, gathering attackers from different backgrounds to break the system is one of the future works that will lead to system improvement and prove the complexity of breaking this authentication model. Moreover, it will demonstrate how the attackers will acquire the knowledge of the most probable multilevel authentication model to launch their attacks. Therefore, a proper solution is a field of research on cloud. So keep the fear of losing your data away. All your data with complete back up can be stored on the cloud. So with rising popularity the computers will act as an interface to communicate with cloud Computing.

REFERENCES

[1] P. Barham et al., Xen and the Art of Virtualization, Proc. ACM Symposium on Operating Systems, Bolton Landing, NY, October 19–22, 2003.
[2] M.N. Bennani and D.A. Menasc´e, Resource Allocation for Autonomic Data Centers Using Analytic Performance Models, Proc. 2005 IEEE International Conference on Autonomic Computing, Seattle, WA, June 13-16, 2005
[3] R.J. Creasy, Digital Certificate Authentication, IBM J. Research and Development, Sept. 1981, pp. 483–490.
[4] R. Figueiredo, P.A. Dinda, and J. Fortes, Cloud services, IEEE Internet Computing, May 2005, Vol. 38, No. 5.
[5] R.P. Goldberg, Survey of Virtual Machine Research for Authentication, IEEE Computer, June 1974, pp.34–44
[6] G.J. Popek and R.P. Goldberg, Formal Requirements for Cloud Architectures, Comm. ACM, July 1975, pp. 412–421.
[7] D.A. Menasc´e, V.A.F. Almeida, and L.W. Dowdy, Performance by Design: Computer Capacity Planning by Example, Prentice Hall, Upper Saddle River, 2004.
[8] M. Rosenblum and T. Garfinkel, Virtual Machine Monitors: Current Technology and Future Trends, IEEE Internet Computing, May 2005, Vol. 38, No. 5.
[9] R. Uhlig et. al., Microsoft Cloud Technology, IEEE Internet Computing, May 2005, Vol. 38, No. 5.
[10] A. Whitaker, R.S. Cox, M. Shaw, and S.D. Gribble,- Rethinking the Design of Virtual Machine Monitors, IEEE Internet Computing, May 2005, Vol. 38, No. 5

 © 2014, IJCSE All Rights Reserved