ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

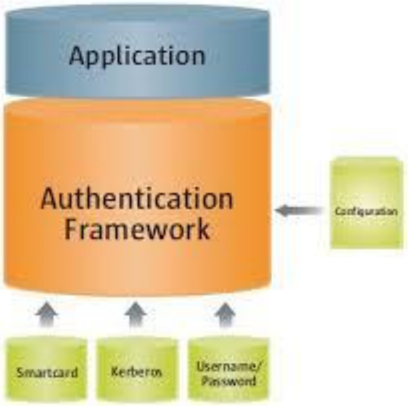
SECURED MULTI-TENANCY APPROVAL FOR DATA STORAGE IN CLOUD

[1]N.THILLAI DINESH, [2]A.SELVA DEVI
[1]Student, Dept. of Computer Application, GKM College of Engineering& Technology Tamil Nadu, India
[2]Asss. Professor, Dept. of Computer Application, GKM College of Engineering & Technology, Tamil Nadu, India

Abstract: Cloud Computing is a general term for delivery of hosted services over the internet. Cloud organization and institutions are increasingly driven to cloud computing as a way to increase functionality, lower cost and enhance convenience to user by making the service and resource availability anywhere there is an internet connection. With cloud computing, user have readily available a suite of application, feature, and infrastructure that would normally require significant investment if provide in the traditional in house computing environment.

Keyword: Security, Authentication, Cloud Computing

Introduction: Cloud computing provides Internet-based services, computing, and storage for users in all markets including financial, healthcare, and government. This new approach to computing allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. However, security is a huge concern for cloud users. Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software.



I. Cloud Development Model:

1. Public Clouds:

In public cloud vendors dynamically allocate resources on a per-user basis through web applications. For example: Drop Box , Sky Drive and Google drive.

2. Private Clouds:

Due to security and availability issues more and more companies are choosing Private Clouds. It provides more secure platform to the employees and customers of an Organization. For example Banks, in banks all the employees and customers can access the bank data which is assigned to them particularly.

3. Hybrid Cloud:

Hybrid cloud is the combination of the Public cloud and private cloud. In this type of cloud services the internal resources, stays under the control of the customer, and external resources delivered by a cloud service provider.

4. Community Cloud:

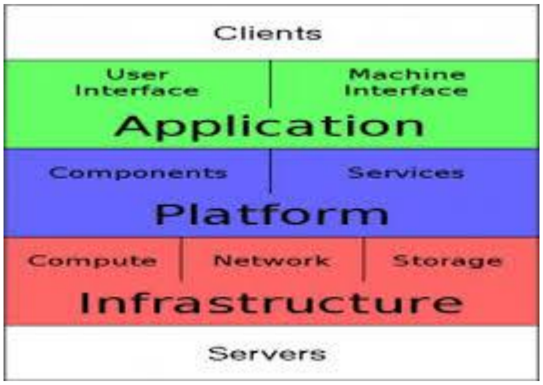
The community cloud shares the infrastructure around several organizations which can be managed and hosted internally or by third party providers....

II. Cloud Layers:

1. SAAS (Software as a service):
In this companies host applications in the cloud that many users access through internet connections. E.g. Gmail, face book.

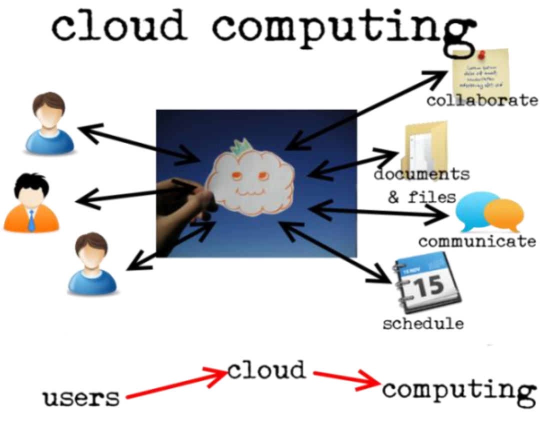
2. PAAS (Platform as a service):
Developers can design, build and test applications that run on the cloud provider's infrastructure. E.g. Google app Engine

3. IAAS (infrastructure as a service):
This part is basically belong to the admin part or we can say the service provider. In this part the service provider provides the user with the basic infrastructure.



III. Authentication Protocol:

An authentication protocol is a defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has control of a valid token to establish his or her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.



1.Threads:

Denial of Service attacks in which the Attacker overwhelms the Verifier by flooding it with a large amount of traffic over the authentication protocol. Malicious code attacks that may compromise or otherwise exploit authentication tokens.

1.1 Threat Mitigation Strategies

*Online guessing resistance – An authentication process is resistant to online guessing attacks if it is impractical for the Attacker, with no a priori knowledge of the token authenticator, to authenticate successfully by repeated authentication attempts with guessed authenticators. The entropy of the authenticator, the nature of the authentication protocol messages, and other management mechanisms at the Verifier contribute to this property. For example, password authentication systems can make targeted password guessing impractical by requiring use of high-entropy passwords and limiting the number of unsuccessful authentication attempts, or by controlling the rate at which attempts can be carried out. Similarly, to resist untargeted password attacks, a Verifier may supplement these controls with network security controls.

*Phishing and pharming resistance (verifier impersonation) – An authentication process is resistant to phishing and pharming (also known as Verifier impersonation,) if the impersonator does not learn the value of a token secret or a token authenticator that can be used to act as a Subscriber to the genuine Verifier.

*Eavesdropping resistance – An authentication process is resistant to eavesdropping attacks if an eavesdropper who records all the messages passing between a Claimant and a Verifier finds it impractical to learn the Claimant's token secret or to otherwise obtain information that would allow the eavesdropper to impersonate the Subscriber in a future authentication session. Eavesdropping-resistant protocols make it impractical26 for an Attacker to carry out an off-line attack where he or she records an authentication protocol run and then analyzes it on his or her own system for an extended period to determine the token secret or possible token authenticators.

*Replay resistance – An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Protocols that use nonce or challenges to prove the “freshness” of the transaction are resistant to replay attacks since the Verifier will easily detect that the old protocol messages replayed do not contain the appropriate nonce or timeliness data related to the current authentication session.

*Hijacking resistance – An authentication process and data transfer protocol combination are resistant to hijacking if the authentication is bound to the data transfer in a manner that prevents an adversary from participating actively in the data transfer session between the Subscriber and the Verifier or RP without being detected.

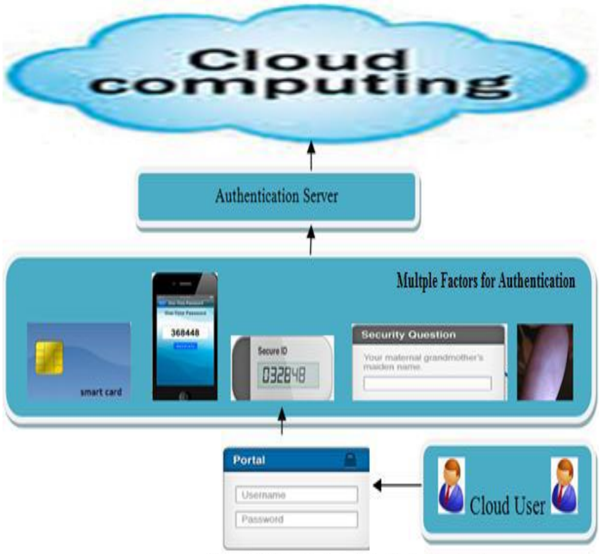


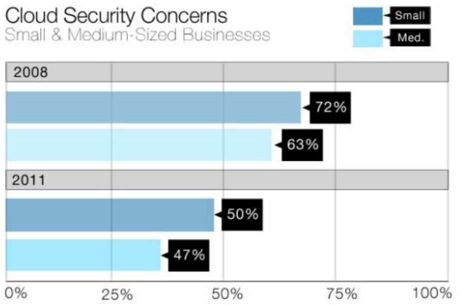
Figure 2 Multi-factor User Authentication for cloud Data Secutiry

*Man-in-the-middle resistance – Authentication protocols are resistant to a man-in-the-middle attack when both parties (i.e., Claimant and Verifier) are authenticated to the other in a manner that prevents the undetected participation of a third party. There are two levels of resistance:

*Weak man-in-the-middle resistance – A protocol is said to be weakly resistant to man-in-the-middle attacks if it provides a mechanism for the Claimant to determine whether he or she is interacting with the real Verifier, but still leaves the opportunity for the non-vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be used to masquerade as the Claimant to the real Verifier.

*Pre-authentication personalization – The Verifier displays to the Claimant some personalized indicator (such as an image or user-chosen phrase picked at registration) prior to the latter submitting the token authenticator to the former. This indicator may be established by the Subscriber at the time of registration.

*Post-authentication personalization – The Verifier displays a personalized indicator to the Subscriber after successful authentication of the latter. The personalized indicator provides assurance to the Subscriber that he or she has in fact logged in to the correct site. This indicator may be established by the Subscriber at the time of registration.



Data from IDC, reported by WSJ

2. Tokens

*Hard token – a hardware device that contains a protected cryptographic key. Authentication is accomplished by proving possession of the device and control of the key. Hard tokens shall: o requires the entry of a password or a biometric to activate the authentication key;

*Soft token – a cryptographic key that is typically stored on disk or some other media. Authentication is accomplished by proving possession and control of the key. The soft token key shall be encrypted under a key derived from some activation data.

*One-time password device token - a personal hardware device that generates “one time” passwords for use in authentication. The device may or may not have some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port).

*Password token – a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings, however some systems use a number of images that the subscriber memorizes and must identify when presented along with other similar images.

2.1 Token Thread

*Multiple factors raise the threshold for successful attacks. If an attacker needs to steal a cryptographic token and guess a password, the work factor may be too high.

*Physical security mechanisms may be employed to protect a stolen token from duplication. Physical security mechanisms can provide tamper evidence, detection, and response.

*Complex passwords may reduce the likelihood of a successful guessing attack. By requiring use of long passwords that don't appear in common dictionaries, attackers may be forced to try every possible password.

*System and Network- security controls may be employed to prevent an attacker from gaining access to a system or installing malicious software.

User name: john_smith

Password: •••••••••••

PASSCODE:

CONCLUSION:

In cloud-based architectures, multi-tenancy means that customers, organizations, and consumers are sharing infrastructure and databases in order to take advantage of price and performance advantages that come with economies of scale. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it. However, the future looks less cloudy as far as more people being attracted by the topic and pursuing research to improve on its drawbacks. .In this article we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage.The delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges

REFERENCE:

[1]. Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology, Vol-2 No 5 October, 2011 , 316-322 .

[2]. [2] Z. Wang, "Security and Privacy Issues Within Cloud Computing" IEEE Int. conference on computational information sciences, Chengdu, China, Oct. 2011.

[3]. Mathisen, "Security Challenges and Solutions in Cloud Computing" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011) , Daejeon, Korea, 31 May -3 June 2011.

[4]. Mohamed Al Morsy, John Grundy, Ingo Müller, "An Analysis of The Cloud Computing Security Problem," in Proceedingsof APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[5]. Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About Cloud Computing Security?" Technical Report No. UCB/EECS-2010-5.http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

BIOGRAPHIES:

Author 1:

About: Myself Thillai Dinesh N currently doing MCA in GKM College of Engineering & Technology in Chennai