ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Effective Grade Planning and Instant Cloud Storage Provisioning

Sumathy

Research Scholar, Bharath University, Chennai, India

ABSTRACT: The circulation of Cloud Service push the increasing demands of storage resources to the service vendors like Amazon, IBM, Google and etc,. Along with the talented business opportunities, this project brings new technique challenges such as effective grade planning and instant cloud storage provisioning. To ensure the correctness of user's data in the cloud, we suggest an effective and flexible distributed scheme in which we overcome the problem of secure Graded keyword search over encrypted cloud data. By utilizing the Graded search improves the system usability by enabling search result relevance ranking instead of sending undifferentiated results, and then it will further ensures the file retrieval accuracy and also improving the service quality for the capacity planning and instant cloud resource provisioning problem.Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against malicious data modification attack, and even server colluding attacks. Our Analytics method can significantly improve the service quality by reducing the resource provisioning time while maintaining a low cloud overhead.

KEYWORDS: service, encrypted, attacks, planning

I. INTRODUCTION

Cloud computing technology is an open standard, service-based, Internet-centric, safe, convenient data storage and network computing service. Cloud computing is an internet-based model for enabling convenient, on-demand network access to a shared pool of configurable computing resources.It provides various services over internet such as software, hardware, data storage and infrastructure. Cloud computing providers deliver the applications via internet, which are accessed from web browsers, desktop and mobile apps. Cloud Computing Technologies are grouped into 4 sections: they are, SaaS, DSaaS, IaaS and PaaS. **SaaS (Software as a Service)** is an on-demand application service. Itdelivers software as a service over the Internet. It eliminates the need of installing and running the application on the customer's own computers. **PaaS(Platform as a Service)** is an on-demand platform service to host customer application.

PaaS isdelivery of computing platforms and/or solution stack as a service, often consuming cloud infrastructure and sustainingcloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. It improves the flexibility in having multiple platforms in business environment. **DSaaS (Data Storage as Services)** is an on- demand storage service.Cloud computing provides internet- based on demand back up storage services to a customer. In this service, customers can keep their data backup remotely over internet servers. These backup data maintenance is taken care by DsaaS service Provider. Cloud DsaaS service providers are responsible for keeping the customer data confidential. Here customers need not worry on setting up the large discs array to keep their huge amount of data. **IaaS (Infrastructure as a Service)** is an on- demand infrastructure service. It delivers the computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients can buy those resources as a fully outsourced service.

DOI: 10.15680/IJIRSET.2014.0312141

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Cloud Security Threats and Mitigation:

Does cloud computing exacerbate security threats to your application? Whichemerging threats are relevant? Which traditional threats are amplified or muted? Answers to these questions are dependent on the combination of cloud service deployment and operational models in play. The following table illustrates the dependencies which should be taken into consideration when architecting security controls into applications for cloud deployments:

	Public/Hybrid Cloud –Threats	**Private Cloud -Threats**	**Mitigation**
IaaS	OWASP Top 10 Data leakage (inadequate ACL) Privilege escalation via management console misconfiguration Exploiting VM weakness DoS attack via API Weak protection of privileged keys VM Isolation failure	OWASP Top 10 Data theft (insiders) Privilege escalation via management console misconfiguration	Testing apps and AP for OWASP Top 1 vulnerabilities Hardening of VM image Security controls including encryption, multi-factor authentication, fine granular authorization, logging Security automation - Automatic provisioning of firewall policies, privileged accounts, DNS, application identity (see patterns below)
PaaS	[In addition to the above] Privilege escalation via API Authorization weakness in platform services such as Message Queue, NoSQL, Blob services Vulnerabilities in the run time engine resulting in tenant isolation failure	[In addition to the above] Privilege escalation via API	

In addition to the aforementioned threats to information confidentiality and integrity, threats to service availability need to be factored into the design. Please remember that the basic tenets of security architecture are the design controls that protect confidentiality, integrity and availability (CIA) of information and services.

Cloud service providers request customers to store their account information in the cloud, cloud service providers have the access to these information. This presents a privacy issue to the customer's privacy information.

Many SLAs have specified the privacy of the sensitive information, however, it is difficult for customers to make sure the proper rules are enforced. There is a lack of transparency in the cloud that allows the customers to monitor their own privacy information.

When a customer decide to use multiple cloud service, the customer will have to store his/her password in multiple cloud, the more cloud service the customer is subscript to, the more copy of the user's information will be. This is a security issue for the customers and the cloud service providers.

The multiple copies of account will lead to multiple authentication processes. For every cloud service, the customer needs to exchange his/her authentication information. This redundant action may lead to an exploit of the authentication mechanism.

DOI: 10.15680/IJIRSET.2014.0312141

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Cloud service providers use different authentication technologies for authenticating users, this may have less impact on SaaS than PaaS and IaaS, but it is present a challenge to the customers.

Multi-level password generation:
This can be used for a wide range of systems including websites, servers, VPN and many other networking solutions. According to the RFC the best possible attack is the brute force attack. As a result this is a suitable solution for most systems.

First level password generation:A one-time pad is a password used only once. Schemes based on a one time pad have been described but are rarely deployed due to the need to supply a new password (or 'pad') for each authentication.
Schemes which use a grid-card are not one-time pads, and are akin to requesting a selection of characters from a password *known* by the user (albeit a password written down). As such, they only protect against re-play attacks (as the same selection of characters can't be sent) and not against duplication of the entire grid (or the building up of a duplicate answer grid over time).

Second level password generation: This level is a team level password generation to authenticate the team for particular service. Example team needs to enter the team name, team id, team thumb image and sign. First all images get added and convert into number data. This data gets concatenate with textual inputs. The resultant output will be a TA (multidimensional team authentication) password.

Third level password generation: This level is a user level password generation. It authenticates the user privileges. User need to enter user name, age, phone number, id and DOB to generate his/her password. Algorithm will process these inputs and generate the PA(multidimensional privilege authentication) password. Organization password alone is not sufficient to access any cloud service. Organization password helps to move authentication into Intranet. Team password helps to move intra team and privilege password helps to access the cloud service for particular user.

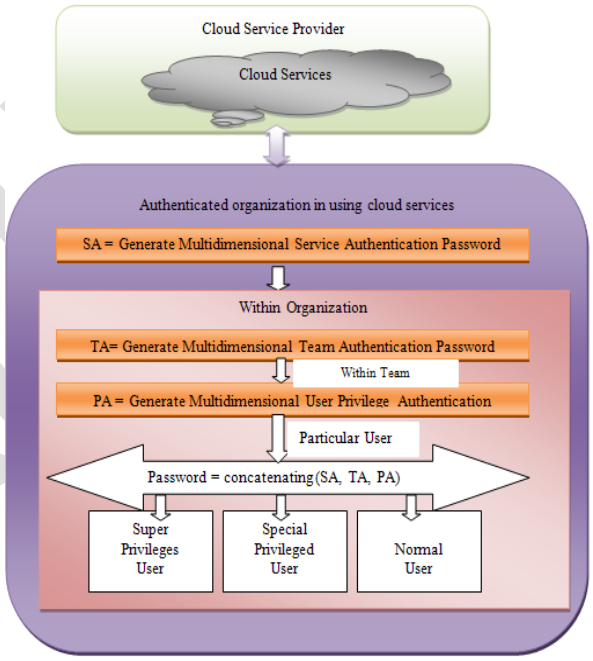

Fig: Multidimensional Password Generation

DOI: 10.15680/IJIRSET.2014.0312141

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Algorithm:

One time pads:

The solution is based on RFC 4226 (HOTP: An HMAC-Based One-Time Password Algorithm) and uses time as the moving factor.

The HOTP algorithm is defined as:

HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

here K is a secret key and C is the moving factor.

After calculating the HMAC value it tstrancated to a shorter human friendly key.

So we need two parameters here key (K) and time based moving factor (T=C). The key can be created using a good random number generator. This key must be stored securely. It should be decrypted only when required and decrypted value should be removed immediately after it is no longer required for computation. Also access to the key must be granted on need basis to the applications required to validate or generate one time passwords.

The RFC recommends the default time step size to be 30 seconds. So we can create one password every 30 seconds.

Multidimensional Password Generation:

Step 1: Start

Step 2: Read input values such as Name, Age, Gender,
Address, Phone Number, Department, Mobile Number

Step 3: Extract image feature

Step 4: Apply Encryption Algorithm

Step 5: Combine image features with input texts in a pre-defined sequence to generate Organization or Service Authentication (SA) Password

Step 6: Combine image features with input texts in a pre-defined sequence to generate Team Authentication (TA) Password

Step 7: Combine image features with input texts in a pre-defined sequence to generate User or privilege Authentication (PA) Password

Step 8: Authentication check : Multifactor Authentication Technique

If Service authentication is successful

Then

check Team level authentication

If Team Authentication is successful

Then

check Privilege level Authentication

If password for privilege level is successful then provide access to cloud environment.

elsegoto step 9

Step 9: Stop

REFERENCES

[1]. IEEE - The Application of Cloud Computing in Education Informatization, Modern Educational Tech... center Bo Wang, HongYu Xing.

[2]. Kiran B., Kareem S.A., Illamani V., Chitralekha S., "Case of Phthiriasis palpebrarum with blepheroconjunctivitis", Indian Journal of Medical Microbiology, ISSN : 0255-0857, 30(3) (2012) PP. 354-356..

[3] NIST Definition http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc

[4] Singamsetty P., Panchumarthy S., "Automatic fuzzy parameter selection in dynamic fuzzy voter for safety critical systems", International Journal of Fuzzy System Applications, ISSN : 1562-2479 , 2(2) (2012) PP. 68-90..

[5].CA Technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx

[6]. Suresh V., Jaikumar S., Arunachalam G., "Anti diabetic activity of ethanol extract of stem bark of Nyctanthes arbor-tristis linn", Research Journal of Pharmaceutical, Biological and Chemical Sciences, ISSN : 0975-8585, 1(4) (2010) PP.311-317.

[7]. X. Suo, Y. Zhu, G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annual Computer Security Application.

[8] Babu T.A., Joseph N.M., Sharmila V., "Academic dishonesty among undergraduates from private medical schools in India. Are we on the right track?", Medical Teacher, ISSN : 0142-159X, 33(9) (2011) PP.759-761.

DOI: 10.15680/IJIRSET.2014.0312141

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

[9] T. Neetha, CH. Sushma, "Security for Effective Data Storage in Multi Clouds", International Journal of Computer Applications Technology and Research, Volume 2, Issue 1, 16-17, 2013
[10] Kamatchi P., Selvaraj S., Kandaswamy M., "Synthesis, magnetic and electrochemical studies of binuclear copper(II) complexes derived from unsymmetrical polydentate ligands", Polyhedron, ISSN : 0277-5387, 24(8) (2005) PP.900-908.
[11] S. Wiedenbeck, J. Waters, J.-C.Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Proc. Human-Comput. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005.
[12] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,"Three-Dimensional Password for More Secure Authentication,"IEEE, http://ieeexplore.ieee.org., Last Updated – 6 Feb 2008
[13] Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.
[14] A User Identity Management Protocol for Cloud Computing Paradigm SafiriyuEludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehindeapered in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163
[15] NandiniMishara, KanchanKhushwha, RituChasta, Er. AbhishekChoudhary, "Technologies of Cloud Computing – Architecture Concepts based on Security and its Challenges, International Journa of Advanced Research in Computer Enginering and Technology (IJARCET), Volume 2, Issue 3, March 2013
[16] Michael Miller, "Cloud Computing, Web-Based Applications That Change the Way You Work and Collaborate Online", Pearson, Eight Impression, 2013.
[17] AtifAlamri, WasaiShadab Ansari, Mohammad Mehedi Hassan, M.ShamimHossain, AbdulhameedAlelaiwi, M.AnwarHossain, "A Survey on Sensor-Cloud: architecture, Applications, and Approaches, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, Article ID 917923, 18 pages, 2013
[18] AnuRathi, Yogech Kumar AnisshTalwar, "Aspects of Security in Cloud Computing", International Journal of Engineering and Computer Science ISSN: 2319-7242, Volume 2, Issue 4, April 2013, Page no. 1361-1363
[19] Dr.G.Brindha, A Study on Quality of Work Life of the Employees at Baxter (INDIA) Private Ltd., Alathur, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,612-615, Vol. 2, Issue 3, March 2013
[20] Dr.G.Brindha, An Analytical Study of the Proposed Voluntary Retirement Scheme in Bharat Sanchar Nigam Limited, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 2707-2712, Vol. 2, Issue 7, July 2013
[21] Dr.G.Brindha, BEYOND THE JUNGLE Strategic Information Systems Theory in 'Low –Competitive' Contexts, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 1446-1450, Vol. 2, Issue 6, June 2013
[22] Dr.G.Brindha, Mergers and Acquisitions, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp1446-1450, Vol. 2, Issue 11, November 2013
[23] Dr.G.Brindha, Building Competitive Advantage through Links with Science, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 1154-1164, Vol. 2, Issue 4, April 2013
[24] Dr.G.Brindha, Article on Portfolio Management, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 2182-218, Vol. 2, Issue 6, June 2013

DOI: 10.15680/IJIRSET.2014.0312141