



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com

A Efficient and Secure Dynamic Multi Dimensional Cloud Confidence

Vijaya.A, Daphne D

Senior Assistant Professor, Department of Applied Science, New Horizon College of Engineering, India

UG Student, Department of CSE, JNN Institute of Engineering, Chennai, India

ABSTRACT: The term cloud (in the context of computing systems) refers to systems and applications that integrate and manage sharing of resources and services distributed across multiple administrative domains. Performance with scalability, optimum utilization of resources, efficient management and reliability and virtualization are some of the advantages of cloud applications. Most of the existing research on cloud security is focussed on authentication. Access control and authorization is a relatively less explored area, although very important for cloud security. The potential of access control as a security mechanism in grids is one of the major motivating factors behind this work. Design and development of new models for access control and authorization, specific to cloud environment and its security requirements forms the core of this thesis work. The thesis proposes models for representing various access control components of cloud security and suggests algorithms to show the association between these components.

Our study on the access control and authorization requirements of cloud systems helped us to identify the core cloud security issues as cloud-wide access control and authorization, indirect authorization for the geographically spread users and resources, dynamic authorization of the cloud resources. Since a cloud-wide mechanism to secure the cloud resources does not exist, we proposed an multi-level authentication framework. This framework includes one time password, team level and user level password generation authorization architectures. Multi dimensional password generation algorithms govern the working of this architecture. We implemented the cloud authorization model for team level and user level enforcement of access control. We implemented the models using programming techniques and inference mechanisms.

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. It delivers 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 is delivery of computing platforms and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud 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.

II. CLOUD SECURITY THREATS AND MITIGATION

Does cloud computing exacerbate security threats to your application? Which emerging 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 API for OWASP Top 10 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.

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.

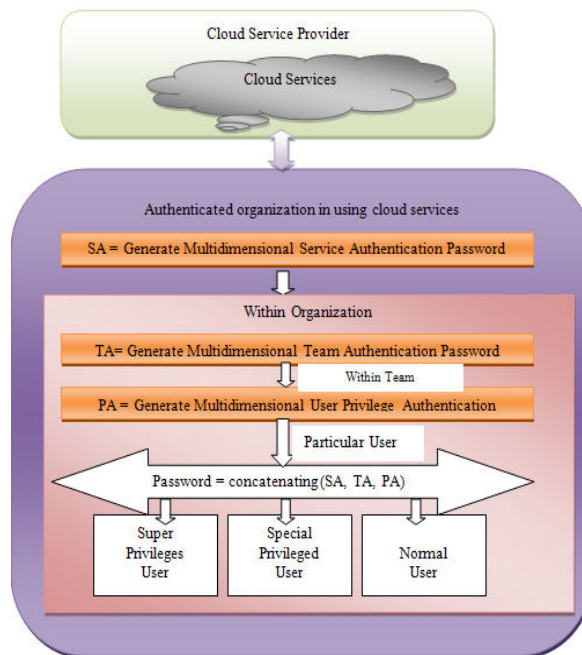


Fig:Multidimensional Password Generation

III. 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:

$HOTP(K,C) = \text{Truncate}(HMAC\text{-SHA-1}(K,C))$

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

After calculating the HMAC value it is truncated 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.

else goto 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]. NIST Definition <http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc>
- [3]. CA Technologies cloud authentication system <http://www.ca.com/us/authentication-system.aspx>
- [4]. X. Suo, Y. Zhu, G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annual Computer Security Application.
- [5] 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.
- [6] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "Three-Dimensional Password for More Secure Authentication," IEEE, <http://ieeexplore.ieee.org>., Last Updated – 6 Feb 2008
- [7] Cloud Computing services & comparisons <http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services>.

- [8] A User Identity Management Protocol for Cloud Computing Paradigm Safiriyu Eludiora¹, Olatunde Abiona², Ayodeji Oluwatope¹, Adeniran Oluwaranti¹, Clement Onime³, Lawrence Kehinde Apered in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163
- [9] Nandini Mishara, Kanchan Khushwaha, Ritu Chasta, Er. Abhishek Choudhary, "Technologies of Cloud Computing – Architecture Concepts based on Security and its Challenges, International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Volume 2, Issue 3, March 2013
- [10] Michael Miller, "Cloud Computing, Web-Based Applications That Change the Way You Work and Collaborate Online", Pearson, Eighth Impression, 2013.
- [11] Atif Alamri, Wasai Shadab Ansari, Mohammad Mehedi Hassan, M. Shamim Hossain, Abdulhameed Alelaiwi, M. Anwar Hossain, "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
- [12] Anu Rathi, Yogesh Kumar Anissh Talwar, "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
- [13] 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



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details