Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 3360 – 3371

SPI Transactional Database Using Secure Elastic Cloud Access with OOB

M.Sumathi*[1], N.G.S.Parameswaran[2]

*1Associate Professor, Department of Computer Science, Sri Meenakshi Govt. Arts College for Women, Madurai, Tamilnadu, India
sumathivasagam@gmail.com

2 Assistant Professor, Department of Computer Applications, VHNSN College, (Autonomous), Virudhunagar, Tamilnadu, India
parames@eswardhas.pro

Abstract

Security is the major issue in cloud computing that connects electronic media of diversified location. It is accessed by the privileged and authenticated user as the recent cloud computing trends proceeds towards server access which make the security concept more vital. Another factor considered in cloud access is the cloud virtualization that entirely depends on server along with the concept of distributed computing. This work focus on cloud authentication mechanism using Out of Band (OoB) mechanism that is used in cloud SPI model. In order to make the authentication mechanism stronger the proposed method takes the challenge of handling storing authentication mechanism for SPI cloud model instead of using two phase authentication model.

Index terms: SPI model, two phase authentication, Out of Band, Privileged cloud

Introduction

The cloud model comprises of SPI model that includes Software, Platform and Infrastructure as its services. Every application used in cloud or taken from the cloud services referred as cloud application that is accessed from the cloud server. The access of application taken from the cloud server needs strong authentication mechanism [Choudhury, Amlan Jyoti, 2011]. It assists the user to gain stronger authentication access to gain momentum of the cloud access. As the cloud server may present anywhere so as the user, the authentication mechanism need to be stronger for providing access grant to the user. It also provides greater flexibility of the cloud server access to the user for all its Software, Platform, and Infrastructure.

The different categories of cloud access are its Public, Private and Hybrid cloud access. As the cloud access are updated frequently the new version has more features for sharing information, its access using the concept of virtualization, scalability, utilization of its software, platform, and infrastructure as a services, in distributed approach. While addressing the impact of security issues by the cloud performance [K.Xiong and H.Perros, 2009] that is evaluated using cloud resource utilization, and its security concern in cloud virtualization in distributed cloud approach is addressed with two phase authentication system. Though there is an impact of various authentication mechanisms like single phase and two phase authentication system to access the cloud indefinitely. More research is going in phase to balance the security breaches for accessing cloud due to user accessing internet as it is openness access.

Whenever there is a flaw in openness network that mainly targets distributed network, as the cloud also work on distributed architecture. It leads to security breach as the cloud is accessed illegally by unauthenticated user for gaining cloud access. What is needed is strong authentication mechanism to provide vital access to cloud model that is used only by legitimate user. Two phase authentication mechanism though provides vital authentication mechanism and suits for transactional cloud access.

Different kinds of threats in cloud access affect the scalable performance of cloud. Cloud scalable performance is affected by its utility service that comes from the third party access. Generally the security can be incorporated to the cloud server as it’s accessed by the third party. It involves security measures to its services which is tedious process.

The organization of this work addresses the impact of security in cloud access using Out of Band model. It is compared with the existing two phase authentication model with a scenario. In extend all the security breaches and its countermeasures are addressed with Out of Band cloud access model.

Literature survey

The survey addresses few existing work that deals with authentication system. The system focuses on password security mechanisms that can be used to any system for ensuring security in the system. In detailed conventional and traditional work of Lamport uses password table as access. It uses authentication by password combination taken from the table in different combination level. The recent authentication system uses biometrics authentication which is more secure instead of keying password.

Every secure scheme [H.Y. Chien et.al, 2002] is proposed in subsequent attempt and every prediction possibilities are addressed in the work of [M.-S. Hwang et. al, 2001]. All such traditional attempts are broken in widespread including smart cart authentication system [V. Shoup et.al, 1996] by understanding its secure mechanism and its organization.

In order to strengthen the system the concept is supported with few metrics that controls intruder with never comprising techniques. Generally such system uses two phase authentication system as it provides security for third party access. The third party access is addressed in the work of [G.Yang et.al, 2008]. This work provides solution for third party access for smart card approach.

The overall challenge for invoking authentication schemes is taken to cloud computing access. As the cloud computing techniques adapts both client server and distributed system. It also uses boundless infrastructure that need strong authentication system. The cloud authentication system was proposed by [Lee et.al, 2012] using two phase authentication schemes. The password used by both the parties can be trapped by the intruder as the password does not involve any crypto system.

Moreover the cloud computing uses boundless network and this system is not viable for cloud computing for ensuring secure.

The works of [S. A. Almulla and C. Y. Yeun, 2010] address various challenges in cloud computing security to address its scalability and integrity approach. The concept of confidentiality is addressed with cloud access mechanism to provide security for third party access that makes flawless connection between users. Such mechanism will ensure security in the overall cloud system but doesn’t ensure security to cloud data.

The authentication systems not only provide security to cloud system but also need to indulge security in SaaS, PaaS, IaaS (SPI) cloud approach. This security scheme is also extend to cloud model for ensuring security in cloud approaches. The security scheme is made as a prototype but not for cloud access control. It is proposed in the work of [A. Celesti et.al, 2010].

The survey shows the secure authentication scheme to ensure security to cloud data by not with access control. This work involves overall secure authentication scheme for cloud that includes both the data as well as its access control.

Secure cloud model

SPI model makes fully functional cloud mechanism including both its software and hardware. The secure cloud mechanism used in its software and hardware ensures effective delivery of cloud application. It is enhanced with flexible mechanism to access cloud Any Where Any Time (AWAT) mode using secure cloud procedures. [J. Abadi, 2009] The ACID property is well addressed, processed and accessed to create virtual cloud store. The virtual cloud store is accessed using platform independent mode to utilize its infrastructure. However such mechanism is not free from issues.

Generally issue arises in many aspects like cloud mechanism, performance, and its transaction. Among these the most addressable issues is the cloud security. The cloud security is addressed with the cloud access mechanism. The secure mechanism is supported with the identity mechanism which helps to identify its individual mechanism. Both the identity and security cloud mechanism are considered to be more vital in cloud architecture.

The function of cloud architecture is to invoke SPI services with its accessibility and security services. However security lies vital to be addressed for providing effective cloud services. More security mechanism prevails in cloud architecture but it differs based on the access mechanism. Diverse secure strategies are used in various cloud functionalities. It works based on cloud access mechanism. Despite indulging various secure mechanisms the cloud is not totally free from threats.

Secure mechanism used in SaaS

SaaS in cloud service deals with third party software as a service. It requires valid authentication mechanism for ensuring reliability and trust while accessing those services through cloud. The cloud third party services embed with valid authentication mechanism that helps in balancing third party service requirements.

Data sharing in cloud third party service covers information and its security, its architecture, data security within services, accessing exact information, and its data central access. The security methodology used in data sharing covers the security measures taken for both system and network security. Hence security in SaaS includes both data and the system security.

Ensuring security in cloud data center focus on the application used in cloud along with its sharing policies. Such policies address the security breaches and avoid direct access of the application beyond the SaaS boundary. The procedures for ensuring security in cloud data center enforce certain procedures along with the policies to change the application access control.

Whenever there is security flaw in application access mechanism the security procedures looks into its policies to overcome from these issues. [C.Wang et. al, 2010] The other key areas to look into regarding security implementation in cloud data center are its authentication mechanism, access rights, level of encryption, data transferred and back up cloud store.

In SaaS accessing user profile is done as individual task and ensuring security policies terms were done as separate task. Both cannot be done simultaneously as both task need special attention from cloud data center and also it involves various other supporting tasks. In an extension boundary in cloud data store plays the key role for implementing secure cloud data store.

Secure mechanism used in PaaS

Security in PaaS uses both public and private cloud that uses different platform setup. The software installed in cloud and been used by the different user profile using SaaS depend on hybrid cloud stack. The cloud application created by SaaS model includes the security level of PaaS for ensuring security both in system and application level.

Fig 1 shows the level of security and access control mechanism in cloud data center combining SPI architecture all together. The cloud data store combines all the level of SPI in order to provide access rights for full-fledged cloud application. Security, authentication process is done using SaaS and PaaS mechanism and successful combination of such mechanism provide better access right control for all the applications deployed in cloud platform.

The cloud boundary is another parameter to be considered while providing valid authentication and access rights to cloud application. The cloud boundary and its parameters are its provider, user, admin, cloud resource, and cloud boundary. The cloud boundary is subdivided into within and out of boundary as within cloud boundary addresses cloud infrastructure and out of boundary is defined by Out of Band (OoB) [Choudhury, Amlan Jyoti, 2011].

The cloud boundary along with the access rights principles are addressed by the combination services of PaaS and IaaS. It deals with the cloud infrastructure support towards access rights mechanism. The cloud boundary is extended based on the accessing mode extension as different location of services tends to enjoy cloud privilege access. Hence cloud boundary extension is possible as cloud architecture support OoB operation.

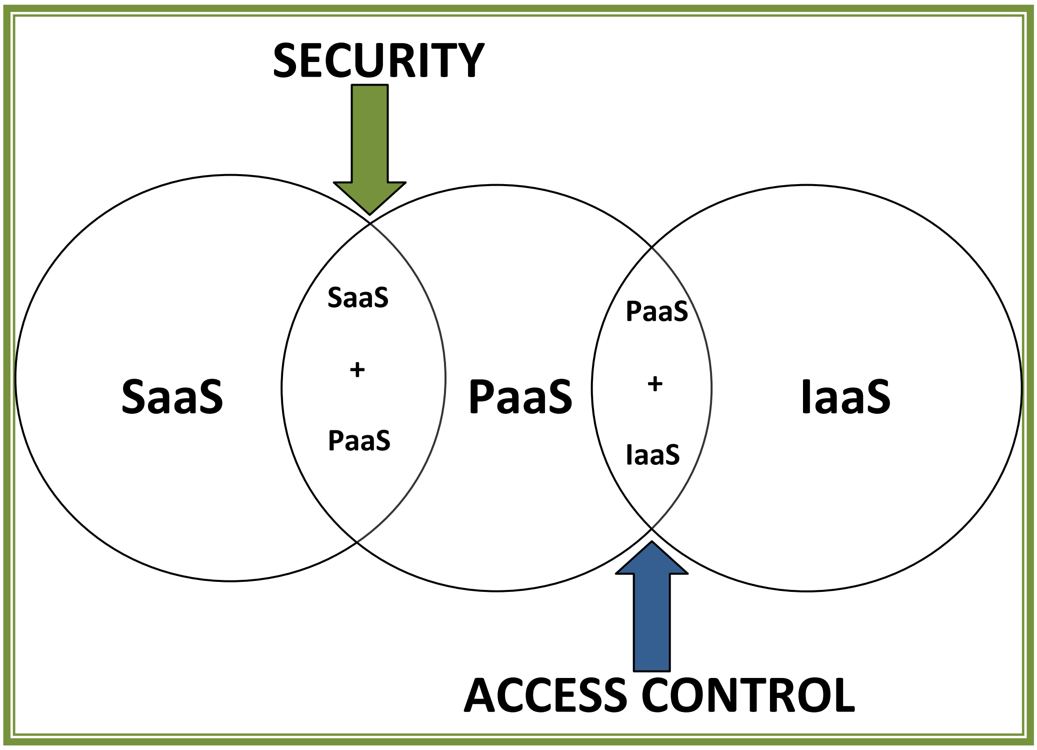

Fig 1: Cloud Data Store access control

Fig 2 represents cloud boundary extension and its access rights control. When cloud access gets into authentication mode, cloud boundary is set with the valid cloud access authentication. The step by step functionality for extending cloud access beyond boundary is done by the following measures.

Algorithm 1: Two Phase Authentication

Step 1: Cloud provider is enhanced and set in the new location.

Step 2: User authentication mode is set for cloud access.

Step 3: Cloud service provider is set on the location for validating the cloud authentication cloud.

Step 4: Cloud admin is deployed on the location for granting the cloud access.

Step 5: Cloud resources are classified and provided with the access rights.

Step 6: The cloud infrastructure boundary is defined and set for cloud access on distinct locations.

Step 7: The cloud trust boundary is set for extending the cloud services beyond the boundary and creates elastic cloud.

Algorithm 2: Foreign Cloud

Step 1: Cloud provider is enhanced and set in the new cloud location termed as foreign cloud.

Step 2: User authentication mode along with native access is set for foreign access.

Step 3: Valid foreign Cloud service provider is set on the location for validating the authentic cloud.

Step 4: Cloud admin is deployed on the foreign location for granting the cloud access.

Step 5: Native cloud resources are classified based on the cloud locations are provided with the access rights.

Step 6: The cloud infrastructure boundary is defined and set for cloud access on distinct locations.

Step 7: The cloud trust boundary is set for extending the cloud services beyond the boundary and creates elastic cloud.

Step 8: Valid two phase cloud authentication is extended for elastic cloud.

Secure mechanism used in IaaS

Security mechanism in IaaS covers two important cloud models viz public and hybrid cloud. Despite using these two models for explaining cloud security in IaaS which addresses the deployment of cloud model like Virtual cloud and inter cloud.

The major security breaches in IaaS security are its flexibility and adaptability. Flexibility is addressed when the valid cloud access is taken beyond the boundary, setting new cloud provider and accessing cloud resources. The cloud environment is made highly adaptable when such cloud process is automated. While during the course of automatic cloud resource access it keeps tracks of application transaction and maintaining the transaction become tedious. [Sudipto et.al, 2009] Hence transactional database are maintained to address these issues.

The solution for the above problem creates virtual private cloud controlled by the organization and cannot be extended further. While extending the cloud, OoB is set and the cloud provider service is extended. The cloud provider extension keeps the track of changes done in virtual cloud and in parallel updates transactional database to maintain its default changes.

In order to ensure security in virtual cloud the configuration of Virtual firewall, Virtual IDS is all set to prevent intrusion.

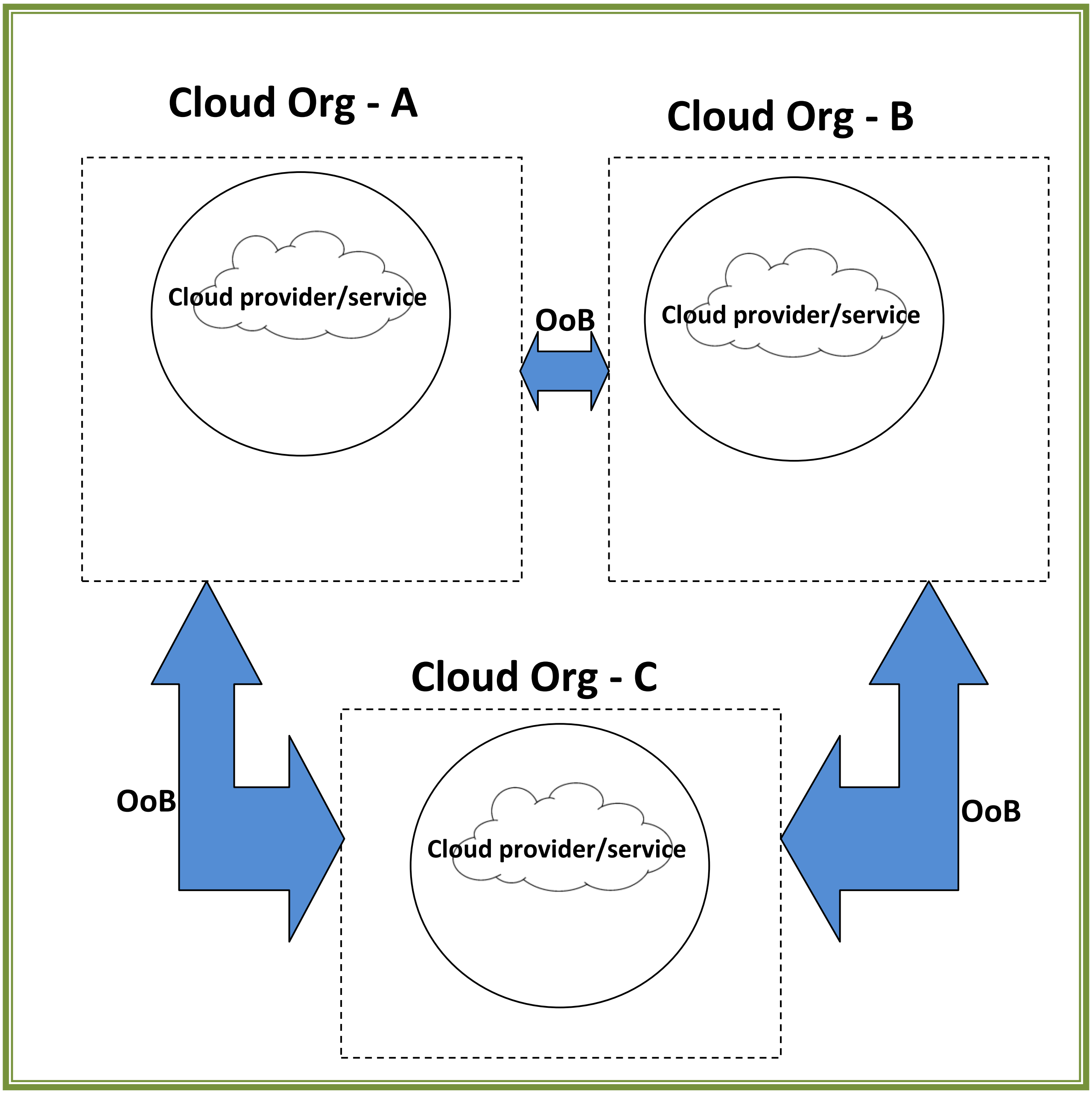

Fig 2: Cloud boundary extension using OoB

Two phase authentication

In earlier work, the Two Phase authentication is proposed for secure resource access from the elastic cloud [N.G.S. Parameswaran and M. Sumathi, 2016]. The extension of the work uses Two Phase authentication with Out of Band (OoB) for secure resource access in foreign cloud. Two phase authentication mechanisms extend it security to cloud software, platform, and its infrastructure. The cloud extension deals with cloud elasticity along with the transactional database access. Security in cloud transactional database has a massive threat and it is address with secure cloud elasticity.

Two phase authentication is introduced in cloud elasticity to ensure security measures in every transactional service. In our earlier work two phase authentication mechanisms is addressed with authentication as one phase and transaction validation is done with other phase. This mechanism ensures scalability and consistency in every transactional cloud services.

This situation works well in deployed cloud boundary and the security concern has to be tightened as the cloud boundary is extended to convert itself as virtual cloud. Adapting two phase authentications in virtual cloud extends its cloud boundary using Out of Band (OoB). Fig 3 represents two phase authentication mechanisms.

The virtual IP is taken as first level of authentication for identifying every system that connects with cloud services. The successful completion of authentication phase is followed by the next level of validation phase that comes from cloud provider. The cloud provider validates virtual IP and granting its access using virtual firewall. Virtual IDS is enabled for providing valid secure access to cloud resources.

Two phase authentications will fail when cloud is extended beyond the boundary despite providing valid access to its resources. To address these issues OoB concept is introduced for extending cloud services and its resources. OoB accounts the functionality of cloud provider and its services for every resources that invokes cloud mechanism.

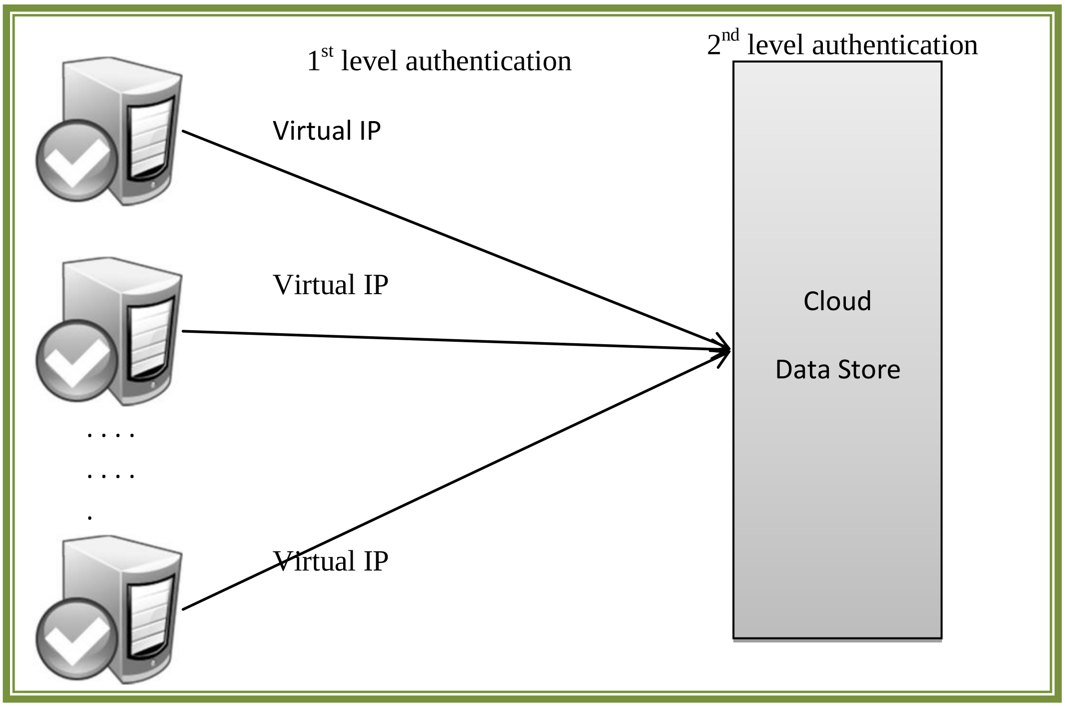

Fig 3: Two phase authentication

Existing model

Group of researchers from the faculty of engineering of Messina University (Italy) proposed a three-phase cross-cloud federation model in order to support the establishment of cloud resource federation [A. Celesti et. al, 2010]. This model facilitates management of so called “Horizontal Federation” of cloud resources. One cloud service provider, lacking in internal resources, can cooperate with another cloud service provider in order to supplement required resourced my means of external ones.

The model consists of three phases: discovery of available external cloud resources, match-making selection between discovered cloud providers, and authentication for trust context establishment with selected clouds. The main focus of this model is authentication phase, which is named Cloud Single Sign-on (SSO) Authentication. Through Cloud SSO a cloud provider authenticates itself with other heterogeneous cloud providers regardless of their implemented security mechanism and accesses all needed external cloud resources. In order to establish trust relationship between home and foreign clouds, an IdP (trusted third party) is represented in this model which verifies digital identities of clouds and provides SAML authentication assertions. A new SAML profile was designed which is called Cross-Cloud Authentication Agent SSO (CCAA-SSO) SAML Profile. Figure 3 shows the sequence diagram of the authentication process between home and foreign clouds through the IdP. For this authentication procedure two software layers are participating in each cloud site: Cloud Manager layer and Virtual Infrastructure (VI) Manager layer. The Cloud Manager layer contains Cross-Cloud Federation Manager (CCFM) software module that performs all the phases of this model by means of three software agents: discovery, match-making and authentication. The interaction between participating entities is accomplished through SAML request-response messages. First the authentication agent of the home cloud sends a SOAP request for some virtual resources to the peer agent located at the foreign cloud, which, in turn, responds with a SAML authentication request message. The home authentication agent authenticates itself to the IdP using a SSO service. Then the obtained SAML response message containing an identity assertion is passed to the VI Manager agent of the home cloud which, in turn sends the message to its peer at the foreign cloud. The VI manager of the foreign cloud, with the help of the authentication agent, verifies the SAML assertion and contacts its peer at the home cloud providing access mechanism to the requested resources.

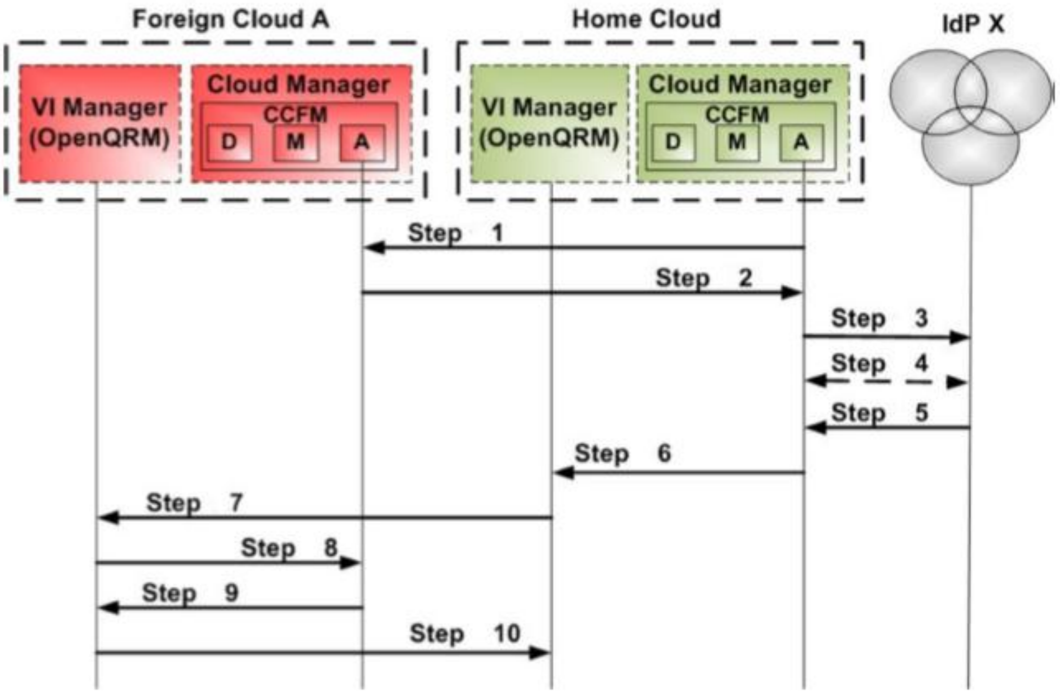

Fig 4: CCAA-SSO approach [A. Celesti et. al, 2010]

Secure authentication Scenario

Fig 1 shows the different cloud service models and how they relate to security and user control over resources. Typically, as you move up through the layers from IaaS to SaaS, there are fewer security risks for the user and provider but at the cost of less control by the user. Each layer serves a different purpose to internet users, as well as developers.

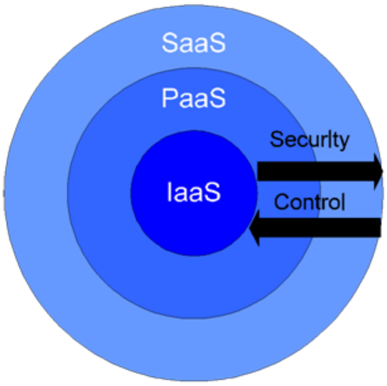

Fig 5: Cloud Security approach and its control

Attack possibilities and prevention mechanism

	Google App Engine	Microsoft Windows	GroundOS
Availability	No SLA and no mention of guaranteed uptime.	Provided by SLA	Problem of user
Integrity	Encryption Authentication	Encryption Authentication	Problem of user Encryption
Confidentiality	Privacy policy Encryption Authentication	Privacy policy Encryption Authentication	Problem of user Encryption
Authentication	Single---sign on Username and password	Username and password	Username and password
SLA	No	Yes	No

Table 1: Cloud attack possibilities

The clouds used for the analysis of the security mechanisms, namely Microsoft Windows Azure (MWA), Google App Engine (GAE) and GroundOS (GOS) are all examples of PaaS clouds. MWA and GAE are proprietary clouds whereas GOS is an open source cloud. [B.P. Rimal et. al, 2009] These three clouds were selected to provide insight into what current cloud providers have to offer in terms of general cloud offerings and security in their clouds. In order to be able to compare apples with apples, the clouds were all chosen to be PaaS clouds. Also, PaaS clouds are interesting for developing a WPS that takes advantage of the scalability capabilities of a cloud. Table 1 shows the five most important aspects of security that a cloud should address.

Availability is usually stipulated in an SLA. This is considered by many providers as the place to address availability and some SLAs consist of issues on availability only. Availability, which is often called uptime, can be defined as how long a service (i.e. the cloud) will be available or online. Availability is largely provided by reliable software and reliable scalability under pressure.

Encryption in GAE is available through programming language libraries. MWA and GAE require the developer to handle encryption and decryption when storing sensitive data; data is not encrypted by default. MWA, GAE and GOS provide network communication encryption through SSL, which has to be set up by the developer. Protection of user data is stipulated in privacy policies, which detail the conditions under which someone is considered to be violating privacy. MWA and GAE both provide an automated failover system, which will relocate a user’s data to another data center if the current data center were to fail by some disaster (Google Apps 2007, Microsoft Windows Azure 2009). While cloud providers generally provide redundant backups it is recommended that users make personal backups regularly.

Confidentiality and integrity of data stored in the cloud is mainly provided by encryption and password security, ensuring that only authorized users get access to data. MWA provides authentication to the entrance of its developer web portal (interface) and also standard SQL authentication and authorization practices to their database through logins and GRANT / DENY / REVOKE commands (Microsoft Windows Azure 2009).

GAE provides authentication though its web portal and single-sign on authentication for first time registration. Single-sign on allows a generated password to be used only once. Upon sign-up to use GAE and request for a domain name a password is generated and sent to the user’s cellular phone. This generated password can then be used to activate the user’s account, after which the password cannot be used again.

Conclusion

This paper process two phase authentication for native cloud access and thus launches elasticity in all the cloud native location. The native cloud location is secure with two phase authentication for cloud data store and proposes OoB concepts for every cloud transaction made in native cloud location. The flexibility is achieved using elastic cloud concepts and accessibility is done using OoB methods. This concepts proven to be secure as the native cloud is secure with two phase authentication for native cloud store to result in virtual cloud.

References

[1]. Choudhury, Amlan Jyoti, et al. "A strong user authentication framework for cloud computing." *Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific*. IEEE, 2011.

[2]. Xiong, Kaiqi, and Harry Perros. "Service performance and analysis in cloud computing." *Services-I, 2009 World Conference on*. IEEE, 2009.

[3]. Lamport, Leslie. "Password authentication with insecure communication." *Communications of the ACM* 24.11 (1981): 770-772.

[4]. Chien, Hung-Yu, Jinn-Ke Jan, and Yuh-Min Tseng. "An efficient and practical solution to remote authentication: smart card." *Computers & Security* 21.4 (2002): 372-375.

[5]. Shen, Jau-Ji, Chih-Wei Lin, and Min-Shiang Hwang. "A modified remote user authentication scheme using smart cards." *IEEE Transactions on Consumer Electronics* 49.2 (2003): 414-416.

[6]. Shoup, Victor, and Avi Rubin. "Session key distribution using smart cards." *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1996.

[7]. Yang, Guomin, et al. "Two-factor mutual authentication based on smart cards and passwords." *Journal of computer and system sciences* 74.7 (2008): 1160-1172.

[8]. Li, Xiong, et al. "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards." *Journal of Network and Computer Applications* 35.2 (2012): 763-769.

[9]. Almulla, Sameera Abdulrahman, and Chan Yeob Yeun. "Cloud computing security management." *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on*. IEEE, 2010.

[10]. Celesti, Antonio, et al. "How to enhance cloud architectures to enable cross-federation." *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*. IEEE, 2010.

[11]. Abadi, Daniel J. "Data management in the cloud: Limitations and opportunities." *IEEE Data Eng. Bull.* 32.1 (2009): 3-12.

[12]. Wang, Cong, et al. "Toward publicly auditable secure cloud data storage services." *IEEE network* 24.4 (2010).

[13]. Das, Sudipto, Amr El Abbadi, and Divyakant Agrawal. "ElasTraS: An Elastic Transactional Data Store in the Cloud." *HotCloud* 9 (2009): 131-142.

[14]. Parameswaran, N. G. S., and M. Sumathi. "Forecasting Response Time in Elastic Cloud for Secure Resource Access in Transactional Database using Two Phase Authentication System." *Indian Journal of Science and Technology* 9.31 (2016).

[15] Rimal, Bhaskar Prasad, Eunmi Choi, and Ian Lumb. "A taxonomy and survey of cloud computing systems." *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on*. Ieee, 2009.