A Survey on Designing a Framework for Improving Security for Cloud using Inter-cloud Identity Management

Snehal Gaikwad
Department of Information Technology
Nagpur, Maharashtra

Pragati Patil Bedekar
Department of Computer Science
Nagpur, Maharashtra

ABSTRACT
To achieve operational excellence in today's IT platform continuous to become even more difficult. The security of the data amongst which suffers the most or can say is very vulnerable to the attacks. Also the storage space of the particular data these days also is becoming the major issue in current scenario. So to maintain the Integrity of the data or the work of the user need to be made maintain, these days it is seen that the lot of storage in cloud which gives, a chance of using Cloud technology in good way, but also it need to ensure the security in this part. So to maintain the confidentiality of the data in this paper the sharing of files using the cloud technology is useful. Which is done by the proper Authentication of the users as well as the Availability of the stored data at the cloud storage? Also there are many ways to improve the security in the inter-cloud to achieve the secured sharing and to maintain the identity of the data of different users at one single place.

Keywords
Authentication, Availability, Cloud Computing, Confidentiality, Identity, Integrity Management.

1. INTRODUCTION
In cloud computing what happens is the resources which are provided to each and every customer are provided as a type of service over the Internet, which can be used by the customer whenever the need arises. These services which are computable can be made available through the data centers and the particular services can be access from anywhere, so by this it can say that the cloud can be considered as the single access point which includes all the tools that can be addressed to the clients need for the computing purpose. For the data storage and the data processing if the cloud is characterized by large scale the thing gets complex, also the delivery of the software's as the service provided by the online as well as the service of levered connection to the wireless devices with the applications which are provided by the online promise systematic, disciplined and the economic change in the business. As the cloud computing services can be access or rented by the customers and they generally do not own it. This minimizes the total capital expenditure and also lowers the barriers for entry. The cloud computing helps the users to use the computing tools irrespective of the physical location, by this the users can access the data and systems regardless of geography or available media.

2. CLOUD MANAGEMENT
By seeing what is available today, it is very important for the cloud consumers and also the providers to align the things on the Graduated SLAs and also the corresponding pricing model to conduct the business within the cloud. This also includes maturing the cloud capabilities in more advance offerings, like the virtual supply chains, needs the fully abstracted interaction across clouds. Now what becomes more challenging is that it will become for the providers to properly make the model, extend the given and the added policies as well as expose these policies in order to provide the integrated services across distributed and different business process and infrastructure. To eliminate various risks from security, privacy and regulatory the data needs to be managed in disciplines manner which is related to these business and the infrastructure.

To deliver a proper future state architecture which captures the Promise of Cloud Computing, architects need to understand the primary benefits of Cloud computing:
• Decoupling and separation of the business service from the infrastructure needed to run it (virtualization).
• Flexibility to choose multiple vendors that provide Reliable and scalable business services, development environments, and also the cloud infrastructure which can be calculated out of the box and can be billed based on the usage with no long term contracts.
• Also on the criteria of more demand the infrastructure can be both allocated as well can be dis allocated in large area using the resources for the business basis.
• Cost allocation flexibility for customers wanting to Move Capital exchange into Operational exchange.
• Reduced costs due to operational efficiencies, and more rapid changes in new business services. These Cloud computing infrastructures can also be allowed to achieve more efficient use of the given IT hardware and software investments in clouds.

This can be done by breaking down the physical barriers which are typically inherited from the isolated systems and initialing the management of the group of systems as a single entity. An ultimate example of this virtualized system is none other than the cloud computing, with the new evolution of the data centers which employees automated system management, balancing of workload and virtualization techniques. This infrastructure model results in being cost efficient model for delivering different information services, reduction in IT management's complexity , innovation promoting increase in response in real time work load balancing.

2.1. Essential Characteristics in cloud computing

2.1.1 Rapid Elasticity
Elasticity can be defined as to both up and down the resources as per the need. Due to which the consumer looks the cloud as

the infinite material and can borrow or buy the data as per ones need. This is one of the important characteristic of cloud computing.

2.1.2 Measured Service

The cloud service are controlled and monitored by the cloud provider, this is what happens in the measured service. This is very important for billing, access control, optimization of resources, planning of capacity and many other tasks.

2.1.3 On-Demand and Self-Service

The on-demand and self-service aspects of cloud computing includes that consumer can always use cloud services as needed without any human interaction with the provider of cloud.

2.1.4 Ubiquitous Network Access

Ubiquitous network access means that the cloud distributor's capabilities are available over the given network and can be reached and accessed through standard mechanisms by both big and small clients.

2.1.5 Resource Pooling

In resource pooling a cloud service provider will allow its clients to serve via a multi-tenant model. The physical and virtual resources which are assigned and reassigned by the consumer demand. The consumer does not have a sense of the provider or the detailed knowledge of the provider's exact location. But it can be specified the disturbers exact location at the higher level of abstraction. In short the security will be the key challenging in feature for the exploring of the cloud computing benefits.

3. OVERVIEW

In this part the security and the IDM issues of cloud computing environment are discussed along with the particular steps which need to be taken by the cloud providers and the consumers.

3.1 Security

Security turns to be the most essential part of the total solution and which requires end-to-end security practices. From an identity and access perspective in cloud, the enterprise will provide an identity authentication service for its working employees regardless of where the service is provided, either internally or in the outer cloud computing environment. The company will own and manages the employee's identity individually and does not share these identities with any other entity. The company provides a single central point in managing an employee's identity, which includes password preset/reset/and many other changes. The company will enhance the identity and security protection by which protecting an employee's confidential and credential information, because the identity federation approach allows the enterprise to manage its employee's access control policy—determining where single sign on (SSO) occurs, asserting trust sufficiently, and then sharing acceptable attributes between the identity provider and the service provider. From an end user's perspective, remote access can reinforce security by using advanced authentication mechanisms (such as strong authentication or multifactor authentication) to prevent identity stealing over the Internet, or to leverage the Host Checker to verify allowed hardware, thereby ensuring a secured environment.

3.2 Information Security

Security is a well-deserved property of a well-designed system. The term information security is nothing but protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidence, integrity and availability for different users.

***Confidentiality*:** Preserving authorized restrictions on

Access and secrecy, which includes means for protecting Personal privacy and proprietary information.

***Integrity*:** To Guard against improper information and modification or destruction; what includes ensured information non-repudiation and authenticity.

***Availability*:** The ensuring timely and reliable access.

And use of information to the consumers, Security is not a characteristics; it is a property of a particular system. It results from deep analysis of security requirements, sound architecture and design, and secure coding practices. Personnel security also enhance these features, organizations need to follow rules and regulations laid down by the cloud service providers for the cloud Customers.

3.3 Personnel Security

The majority of questions relating to personnel will be similar to those one would have asked his own IT personnel. As with most ways, there is a balance between the risks and the cost.

• What kind of policies and procedures does one have in place?

Also when one is hiring IT administrators or others with system access?

It should include:

▪ pre-employment checks (identity, nationality or status, employment history and references, criminal convictions, and vetting).

• Is there any different policies depending on where the needed data is stored or applications are run? Consider For example, hiring policies in one region may be totally different from those in another.

▪ All practices need to be regular across regions.

▪ It should be noted that sensitive data is stored in one particular place with appropriate personnel.

• What kind of security education program does one run for all?

• Is there a particular process of continuous evaluation?

▪ This is occurred how often?

▪ Further interviews

▪ reviews on security access and privileges

▪ reviews on Policy and procedure.

3.4 Security Issues of Cloud Computing

Despite many beauty of Cloud computing application service, as described before, Cloud service subscribers, particularly for larger enterprises will corporate information security policies which need to be enforced from time to time, they may want to consider getting a security assessment from a neutral third party before dealing to a Cloud vendor. Cloud computing is fraught when security risks and seven specific security issues were brought to the attention of Cloud service subscribers that they should raise them with the distributes before actually selecting them:

Privileged user access—we must ask the providers to provide us specific information for the hiring and oversight of privileged administrators, and the control over their access, because outside services usually ignores the "physical, logical and personnel security controls" which gets over inside programs.

Regulatory compliance—the providers who refuse to undergo these steps are "giving the hint that consumers can only use them for the most important functions", as consumers are ultimately responsible for the security and integrity of their data even when it is held by a provider.

Data location—we must asks the providers if they will "give a word to store and process data in specific jurisdictions and if they will make a contractual commitment to follow local privacy requirements on behalf of the consumers".

Data segregation— the subscribers' data should be catered with data from other customers as the Cloud is typically a shared place. The service providers should provide data encoding as options and proof on the corresponding encoding schemes which will be designed and properly tested by the specialists.

Recovery—the providers if have applied and tested any disaster recovery procedures (DRP) which provides them "the ability to do a complete restoration" and mostly, "how long it will take" to execute the DRP. Security attributes of cloud computing are discussed, so that the whole system is reliable and accessible to the consumers.

3.5 User Identity Management

To know whether an application runs outside the cloud or in the cloud, it typically needs to know something about its consumers. Toward this end, the application commonly wants that each and every consumer should provide a digital identity, or a set of bytes that describes that consumer. Based on what these bytes contain and how these are evaluated, the application can determine the things such as the identity of the user and what they're allowed to do.

Many outside cloud applications depend on an outside cloud infrastructure service, such as Active Directory, which provides this identity information. When a user accesses any cloud application, however an on-premises identity usually won't work. And then the question arises that what about an application built on a cloud foundation? From where does it get its identity information? An identity service in the cloud can solve these problems. Because it gives a digital identity that can be used by an individual, by outside cloud applications, a cloud identity service will be applied in many different environments. The kind of identity service is the number of cloud identity services available today is only important .For example the Accessing Amazon cloud services such as EC2 or S3 require presenting an Amazon-defined identity, for instance, while using Google App Engine if it requires a Google account. The Microsoft will provide Windows Live ID, which can be further used for Microsoft applications and others, while BizTalk Services also offers its own identity service, which can be federated with others.

3.6 Identity and Access Management

The below steps can be applied to control the cloud provider's identity and to access the management systems (those are under their control).

3.6.1 Authorization

• Any account must have system-wide privileges for the entire cloud system and, if they have so, for what operations do they do (read/write/delete)?

• How will the accounts with the highest level of privilege are authenticated and managed by the cloud?

• In what way the most critical decisions (e.g., simultaneous de-provisioning of large resource blocks) are authorized (single or dual, and by which roles in the organization)?

• One must see if any high-privilege roles are allocated to the same individual? Does this particular allocation break the segregation of? Given duties or the least privilege rules?

• The thing which needs to be noticed is to see whether you use role-based access control (RBAC)? Also in this case is the principle of least privilege is being followed?

• What is changed, if any, when change is made to administrator?

Privileges and these roles are allowed for extraordinary access in the time of an emergency?

• One must also see if there is an "administrator" role for the customer? For example, does the customer administrator have a role in including the new users (but without allowing him to change the existing storage!)?

3.6.2 Identity Provisioning

- What all things are examined on the identity of the user accounts at the time of registration? If any particular standards are followed? For example, they follow e-Government Interoperability Framework?

• Different levels of identity checks must be there based on the required resources.

• Processes should be in the particular place of de-provisioning credentials.

•The credentials must be provisioned and de-provisioned both together throughout the cloud system, or if there are any risks in de-provisioning them across the multiple geographically distributed locations?

3.6.3 Management Personal Data

- When the data is stored and protection controls is applied to the given user's directory (e.g., AD, LDAP) and when is it accessed?

•The user's directory data should be exportable in an interoperable format?

• It is needed-to-be known what are the basis for the access to the customer's data within the cloud distributor?

3.6.4 Key Management

Particular steps need to be followed to keep the control on the cloud provider:

• Are the security controls in correct place for input and output of those keys? For example, if there are strong password policies, the particular keys must be stored in a separate system, there must be hardware security modules (HSM) for the root certificate keys, smart card must be based on the authentication, direct shield must be accessed to storage, short key should have particular lifetime, etc.

• Are the security controls in its place for using those same keys to sign and code the data?

• Are the procedures in place in the program of a key compromise?

For example, let's see the key revocation lists.

•Are the given keys revocation able to deal with issues for multiple sites in simultaneous manner?

•Do the customer system images protected or encoded?

3.6.5 Encryption

- We all know that the Encryption can be used in number of places—so where exactly is it used?

▪ In the transmition of data.

▪ At the resting of data.

▪ Do the processer or the memory contain the data.

▪ Are they in the Usernames and passwords?

• Is there a particular system for what should be coded and what should exactly not be coded?

• Access key is controlled by whom?

• How the protection of these keys takes place?

3.6.6 Authentication

• What types of authentication are used for operations which require high rely? This can also include the login for management interfaces, the key creation, and access to the multiple-user accounts, along with firewall configuration, and remote access, etc.

•Are the two-factor authentication process is used to manage the important components within the infrastructure, like the firewalls etc.?

3.7 Identity and Access Management Systems Offered to the Cloud Customer

For the use and control by the cloud customer the following points will be applied to the identity and access management systems which will be offered by the cloud customer.

3.7.1 Identity Management Frameworks

• Do the systems allows for a federated IDM infrastructure which will be interoperable both for high assurance (OTP systems, where required) and low assurance (e.g. username and password)?

• The third party should be cloud provider interoperable identity providers?

• There must be the ability to incorporate single sign-on?

3.7.2 Access Control

- Do the client credential system is allowed for the separation of roles and responsibilities and for multiple domains (or a single key for multiple domains, roles and responsibilities)?

• How will we manage access to the customer system images-and ensure that their authentication and cryptographic keys will not be contained within in them?

3.7.3 Authentication

• How will the cloud provider will identify itself to the customer (*i.e.*, is there mutual authentication)?

▪ Do the customer sends API commands?

▪ Do the customer logs in the management interface?

• Is the federated mechanism for authentication is being supported.

The end Users will be needed to access certain resources in the cloud and should be well aware of these access agreements such as their acceptable use or their conflict of interest. End user signatures may be used to confirm if anyone is committed to such policies. The client side organization should run mechanisms to find the vulnerable code or rules at entry points like firewalls, servers, or mobile devices and to upload patches on the local systems as well as they are found at any instance. Thus, this approach ensures the end users are secured on the cloud.

Moreover, the cloud has to be secured from any user with suspicious intent that may try to gain control to take the information or stop a service to be delivered. For this reason, the cloud should involve a denial of service (DOS) protection. One only way of apply DOS protection is by improving the infrastructure with more bandwidth and better computational strength which the cloud has in large amount. It involves filtering certain packets that have same IP source addresses or server requests. The issue concerning the cloud provider to end users is transmission uniqueness. A simple way of implementing integrity is by using secure socket layer (SSL) or transport layer security (TLS) to ensure that the sessions are not being changed by an individual in the middle of the attack. At a lower level, the network can be made secure by the usage of secure internet protocol (IPsec). Finally, the middle point between end users and the cloud is confidential transmission.

3.8 Related Works

Identity federation is nothing but the evolution to meet business globalization strategies, enterprise and cloud service which is provided by the providers and the providers are looking for best practices which is related to the cloud computing environment. In many paper, the various authors

demonstrated that how remote access, identity management, and security can made to work together to enable, secure, and integrate the cloud computing services. Amongst which four patterns were proposed and they were also implemented. With the use of these integration patterns and ways, the whole of the enterprise can effectively design identity federation solutions in a hybrid and complex cloud environment for different use types specific to the particular type of business. Our main study focuses on the proposed patterns which enable us to draw our own conclusion that this work will give another beneficial solution for credential compromise. Also adoption of IDM in cloud computing environments results in many challenges. The difficulties that may be experienced by any enterprise in the management of ID can couple with the other factors which have overhead costs. According to IDM IaaS user's centric identity management is being considered as a complete all-round solution in addressing all possible problems of cloud IDMs. The authors keep the opinion that it should be outsource to other companies that can effectively handle them. Our opinion on this work is that IDM IaaS may not be enough to address the given security challenges, because the particular paper will not consider the other models like for example PaaS and SaaS. These two models will require sufficient IDM. Since cloud computing environment will require holistic security, privacy and trust approach to meet the earnest benefits which is derived from the cloud computing.

4. CONCLUSION

In the particular paper it has been discussed that the core working concept of cloud computing identity management which also focuses in the issue which is related to the authentication and authorization along with the integrity, non-repudiation and de-provisioning of an application and regular compliance of the cloud framework includes both the providers and the consumer's point of view. Also the future scope can be the better usage of security algorithms like ECE and RC6 for data storage can be done, but that will increase the storage cost of the cloud environment, so some solutions can be proposed in that direction as well.

5. REFERENCES

[1] D. Chappell, "A Short Introduction to Cloud Platforms an Enterprise—Oriented View," Chappell and Association, San Francisco, 2008, pp. 1-13.

[2] T. B. Winans and J. S. Brown, "Cloud Computing: A Collection of Working Papers," Deloitte Consulting LLP, New York, pp. 1-27.

[3] Stratus Technologies, "Server Virtualization and Cloud Computing: Four Hidden Impacts on Uptime and Availability, "A White Paper by Startus Technology, June 2009

[4] Oracle, "Architectural Strategies for Cloud Computing," An Oracle White Paper in Enterprise Architecture, August 2009

[5] G.Boss, P.Malladi, D. Quan, L. Legregni and H. Hall, "Cloud Computing," IBM Corporation, New York, August 2007.

[6] NIST, January 2010. http://www.nist.gov/

[7] P. Mell and T. Grace, "Effectively and Securely: Using the Cloud Computer Paradigm, "NITS, Information Technology Laboratory, Boulder, and December 2009."

[8] The European Network and Information Security Agency (ENISA), "Cloud Computing: Benefits, Risks and Recommendations for Information Security," November 2009.

[9] Juniper Networks, "Implementation Identity Federation in a Hybrid Cloud Computing Environment Solution Guide," October 2009.

[10] P. Bryden, D. C. Kirkpatrick and F. Moghadami, "Security Authorization: An Approach for Community Cloud Computing Environments White Paper, November 2009.

[11] Gartner, "Assessing the Security Risks of Cloud Computing,"2009.

[12] S. So, "Cloud Computing and Information ecurity,"Info-Security Project, No. 3, May 2009.

[13] G. Treu, F. Fuchs and C. Dargatz, "Implicit Authorization for Social Location Disclosure," Journal of Software, Vol. 3, No. 1, 2008, pp. 18-26.

[14] M. E. Whiteman and H. J. Mattord, "Principles of Information Security," 2nd Edology, Massachusetts, 2005.

[15] P. Venkataram and B. S. Babu, "An Authentication Scheme for Ubiquitous Commerce: A Cognitive Agents Based Approach," Proceedings of IEEE Workshops on Network Operations and Management Symposium Workshops, Salvador da Bahia, 7-11 April 2008, pp. 248-256.

[16] A. Gopalakrishnan, "Cloud Computing Identity Management, "SET Labs Briefings, Vol. 7, No. 7, 2009 pp. 45- 54.