High Security and Privacy in Cloud Computing Paradigm through Single Sign On

Corresponding Author: [1]Muhammad Munwar Iqbal, [2]Muhammad Salman Bashir, [3]Yasir Saleem, [4]Muhamamd Farhan, [5]Amjad Farooq, [6]Abad Ali Shah

[1, 2, 3, 4, 5,6] Department of Computer Science & Engineering, UET Lahore, Pakistan
[1]munwariq@gmail.com, , [2]salman.vu@gmail.com, [3] ysaleem@gmail.com, [4]farhansajid@gmail.com, [5]amjadfrooq@uet.edu.pk, [6]abad_shah@yahoo.com

Abstract: Cloud computing is very emerging technology and have economical computation over the current infrastructure. Cloud computing provides the services on the basis of as you pay as you go. Privacy and security is still at top level risk in cloud data management environment. Privacy of the data is affected as cloud users have not fully aware about the location of the data kept on servers. Data segregation is another problem during the storage of data. Identity management is a big issue that is faced by the cloud users. In the research paper we will propose a model to improve the data security and privacy in the cloud environment. Single Sign On uses the different identity management methods to enhance the privacy and security of the cloud users like OAuth, OpenId, and SAML etc. Securing the identity management is very effective method to secure your authorization and access management that makes surety to providing the secure cloud data management environment.
[Muhammad Munwar Iqbal, Muhammad Salman Bashir, Yasir Saleem, Muhamamd Farhan, Amjad Farooq, Abad Ali Shah. **High Security and Privacy in Cloud Computing Paradigm through Single Sign On.** *Researcher* 2012;4(9):3-13]. (ISSN: 1553-9865). http://www.sciencepub.net/researcher. 2

Key words: Grid Computing, Utility Computing, Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Cloud Computing

1. Introduction

The term Cloud Computing was coined in 2007, joint hardware and software deployment concept. From the history it is observed that although the word cloud computing is used in 2007 but the fact is that cloud computing concept established long time ago 1960, at that time John McCarthy pointed out that "computation may someday be organized as a public utility"; exactly same as fragments the characteristics and features by using different service bureaus that uses earlier in the 1960s. An interesting fact is that genuine term "cloud" is originally copied from telephony in those broadcastings & telecommunications companies, those companies which till the 1990s era mainly provided the dedicated point-to-point data circuits, initiated new services offering comparably at lower and much cheaper cost of "VIRTUAL PRIVATE NETWORK (VPN)" of almost same level of quality of service. Cloud computing does not bound the service in same borderline but they extend it up to the convers servers as well as network resources and infrastructure and then Software as a Service[11] [14], Infrastructure as a Service and Platform as a Service. Now the cloud is symbol of a publically available service and computing resources from the cloud service provider end to the cloud service user end. There many other aspects are also provides the wonderful result by using cloud computing services like economical cost, green computing etc. Cloud computing facilitate the cloud user to remote access that in independent to locations and elasticity in scalability of services. The user can get access all the cloud computing service though web browser by using the internet facility without taking the headache of managing resources.

From the (Figure 1) it can be observed some demands by the different user and established a new concept that remote access to the application and data is the main desire of every end user. Users always want maximum resources with computing power this concept leads to the Software-as-a-Service (2000) Utility Computing. On the other developer always needed the platforms that provide them the facility to different kind of applications and web services. Developer is more conscious about the different application needed during the development process of different software. While the business always demanding the infrastructure that major component for any organization to run their business. All the above concepts and demands leads towards the cloud computing through the number of steps like Personal Computer (PC) (1970), World Wide Web (1989) Grid Computing (1990), Utility Computing(2000) and Cloud Computing (2007).

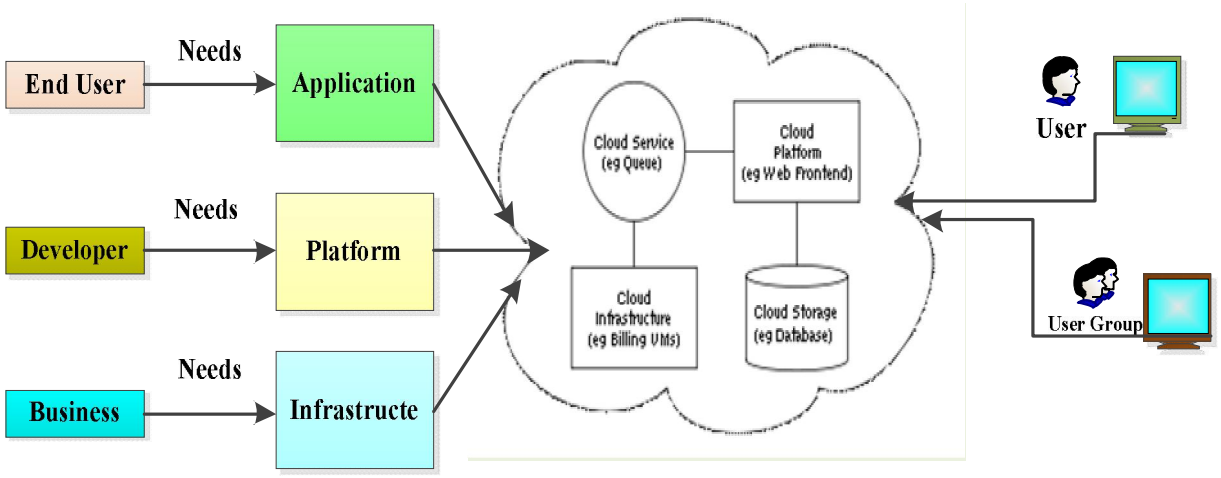

Fig: 01 Cloud Computing Environment

From the (Figure 1) it can be observed some demands by the different user and established a new concept that remote access to the application and data is the main desire of every end user. Users always want maximum resources with computing power this concept leads to the Software-as-a-Service (2000) Utility Computing. On the other developer always needed the platforms that provide them the facility to different kind of applications and web services. Developer is more conscious about the different application needed during the development process of different software. While the business always demanding the infrastructure that major component for any organization to run their business. All the above concepts and demands leads towards the cloud computing through the number of steps like Personal Computer (PC) (1970), World Wide Web (1989) Grid Computing (1990), Utility Computing(2000) and Cloud Computing (2007).

The term Cloud Computing may be defined as "Cloud computing is an emerging model of large scale computing technology that provides the different services like Platform as service (PaaS), Infrastructure as a service (IaaS) and Software as a service (SaaS) etc. through internet on demand from central remote servers to maintain data and applications typically through a measured service archetypal "pay-as-per-use [12]" business model.

Another definition by NIST [1]

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models".

Another definition by [2]

Cloud computing paradigm that is abstracted model having virtualization of resources that can be dynamically-scalable and automatically manage the computing power, this paradigm provides the different software, storage, platforms as a service. These services are delivered through internet on demand external customers at the economically "go as you pay" mode.

Cloud computing is a best promotion word intended for tool and technologies which facilitate the data access, computation power, software's and data storage services. Physical locations of the cloud service provider and system configuration are invisible to the end user.

.

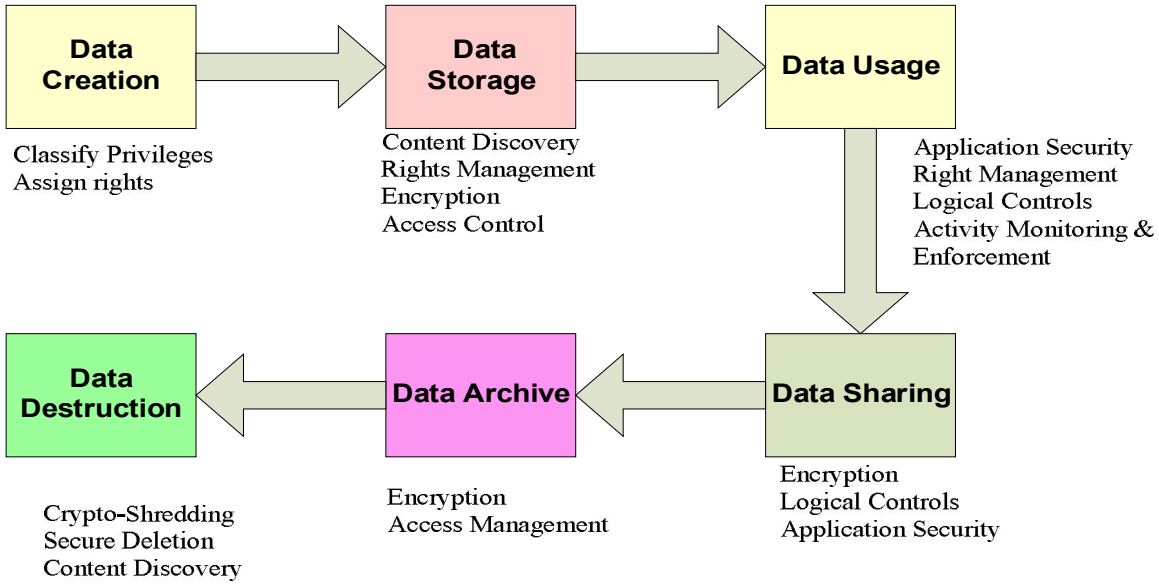

Figure 02: Data Security Lifecycle

Data is more important for company to his survival and business. Data security and privacy is the main issue in the cloud data management although cloud provides the different services to enhance the business for the companies. Cloud service providers implements the different techniques to provide the secure cloud services such as Infrastructure as a Service (IaaS), Platform as a service (PaaS), Software as a service (SaaS)[15], Communication as a Service(CaaS) and Database as a Service (DaaS) etc. Data security id needed with creation of data and continued till the data is destroys after archiving on the storage media. Data is stored and executed by using the different application services and infrastructure. By making sure the secure authentication and identity management service we can come over the most of the data security issues. Transportation of data must be only used in encryption format and using secure socket layer always over network [3].

Traditional company applications have for all time been extremely complicated as well as very costly. The amount plus variety of hardware and software and hardware necessary to run them are commonly terrifying. . Your requirement is complete team that can aware of the process of installment, configuration, running, testing, securing and update them. It is observed that when you proliferate these efforts through number of application. We infer clearly that why the companies having large and best IT sectors are not accomplishing services they required. Medium and small business doesn't take any chances on this procedure. So the better way to eliminate similar kinds of pain is "Cloud Computing".

This paper is distributed in eight sections. First section is composed of introduction and presents the brief overview and needs of the cloud computing. In Section 2 discusses the literature review and related work. Section 3 addresses the problem description in detail. Sections 4 deals with the purposed solution of said problem and discusses the different authentication methods to improve it a best solution. In the last section presented the conclusion and future work about or purposed solution.

1. Literature Review

Untrusted Storage and Computation is major concern that is faced by the organization using could computing service. Assumed that effort on conversion of solitary regular set data into alternative set which kept in the another set of procedures concerning the affiliates the first set called encryption [9] that make available a solution to computing on encoded information and data, but in cost perspective it is very expensive & costly for using in practical experiences. The literature review shows that related work is limited by space constraints. In the table data trust model and privacy models are discuss in detail.

Table 1: Trust and Data Privacy Model

Model / Feature	Full Trust	No Privacy	Compliance Based Trust	Full privacy	No trust
Encryption	No	No	Yes	Yes	Yes
Third Party Involvement	No	No	May/May Not	Yes	Yes
Sensitivity	Low	Low	Medium	High	High
Data Processing	Normal	Normal	Encrypted	Isolated Container	Isolated Container
Data Storage Format	Simple	Simple	Encrypted	Encrypted	Encrypted
SSL Transformation	Optional	Optional	Mandatory	Mandatory	Mandatory
Encryption Site	No Encryption	No Encryption	CSP End	Customer Side	Customer Side
Key Sharing	No Key	No Key	Yes	No	No

Cloud service user have the utmost level issue of data privacy and security.in the cloud computing environment the privacy of the organizational data suffer badly as client does not know the location of the data servers. Data owned by an organization is completely by the hand of third party that is cloud service provider.

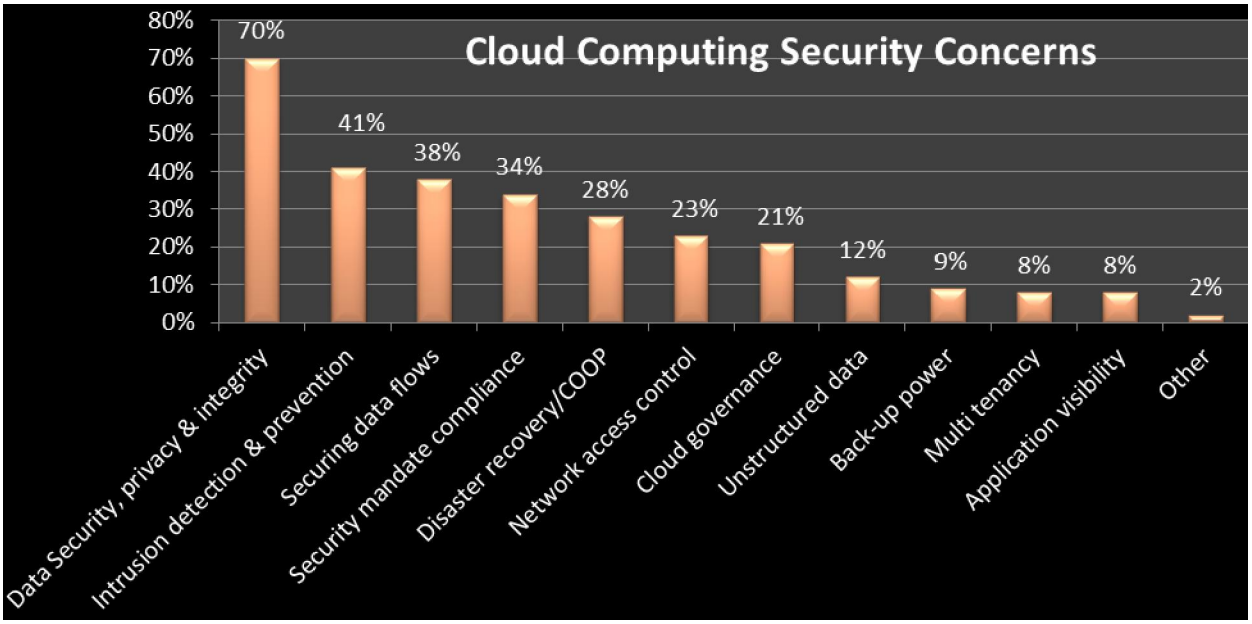

Fig 03: Cloud Computing Security Concerns

In the point view if we want to judge the security privacy and cloud computing issues it is clearly observed from the Figure 3 [5] that Cloud Computing Security mainly concerns with the data security, privacy and integrity.

Table 2: Databases Used by Different Companies

Service / Database	MySql	IBM Informix Dynamic server	BLOB	Microsoft SQL Server Standard 2005	DB2	Google Bigtable	Oracle Database	Table Storage (non-Relational)	SQL Azure,
Force.Com	✔								
IBM					✔				
CISCO							✔		
VMWARE							✔		
Salesforce.com									
GOOGLE Apps						✔			
GOOGLE AppEngine	✔		✔			✔			
MICROSOFT AZURE	✔		✔	✔				✔	✔
AMAZON EC2									
AMAZON WEB SERVICES	✔	✔	✔	✔			✔		

In this table 2 we discuss the "Databases Used by Different Companies" and some cloud service provider comp[anise may uses the more than one databases to facilitate the cloud service user. Different cloud services provider provides the facility to enable a user to store his data by different database storage service. The cloud service provider companies may also provide the Storage as a Service. These data bases may be relation databases or non-relational databases. For example, Microsoft Azure facilitate his service users to use the Storage as a Service by providing different databases like MySQL, Microsoft SQL Server standard 2005 as relational storage database and BLOB and Table Storage (Non-Relation) formats. The most of the companies that provided the cloud computing services are started their work as a cloud service provider from 2006 to 2008. We are no here to discuss their life but the purpose for the discussion is to elaborate the data remains occupied by cloud service providers after the termination of cloud services by the user. This time duration or backup is lasting form 0 to 90 days. This is also a threat to cloud user that anyone can get access to their confidential data.

2. Problem Statement

Analysis of current security management approaches shows that the most of the companies are facing the problem of user credential mangment issue and data and services privacy and security is always reaming the sword over the head of companies.

Characterstics / Security provider	Credential Management	Adaptability	Expandability	Interoperability Securit	Adoption to Security Pro	Plattform Indepent	Identity -Managem	Attribute Managem	Previlge Managem	Digital Policy Mana	IA Configuration Ma	Crypto Key Manage	IA Metadata Manag	IA Audit Managem
CA-Enterprise IT Management	0	10	10	10	10	10	10	10	10	10	0	0	0	10
Checkpoint-Software Blades	0	10	10	10	10	10	10	0	0	10	10	0	0	10
Cisco-Security Management Suite	0	10	5	5	10	0	0	0	0	10	5	0	0	10
Evidian- Identity and Access Management suite	10	10	10	10	10	10	10	5	10	10	0	5	0	5
IBM-Tivoli Suite	0	10	10	10	10	10	10	10	10	10	10	10	0	10
NetIQ- security and Compliance Management	0	10	10	5	10	0	0	0	0	0	0	0	0	10
Novell_Identity and Access Management	0	10	10	10	10	5	10	10	10	10	0	0	0	10
Oracle_Identity and Access Management	0	10	10	10	10	10	10	10	10	10	0	0	0	10
RSA- Security Suite	10	10	10	10	10	10	0	0	10	5	0	10	0	10
Sun-Identity Management	5	10	10	10	10	10	10	10	10	5	0	0	0	5
Symantec-Control Compliance suite	0	10	10	5	10	5	0	0	0	5	0	0	0	10

Legends:

0	NO
5	Partial
10	Full

Fig 4: Cloud Computing Security Concerns Implementations [13]

The above graph depicts that the credential management [13] is a very difficult task and most of the companies are not manage the credential of the cloud service users. The above diagram shows that only two companies Evidien Identity and access management suite and RSA security suite only managed the credential of the user companies. All the other companies does not support credential management.

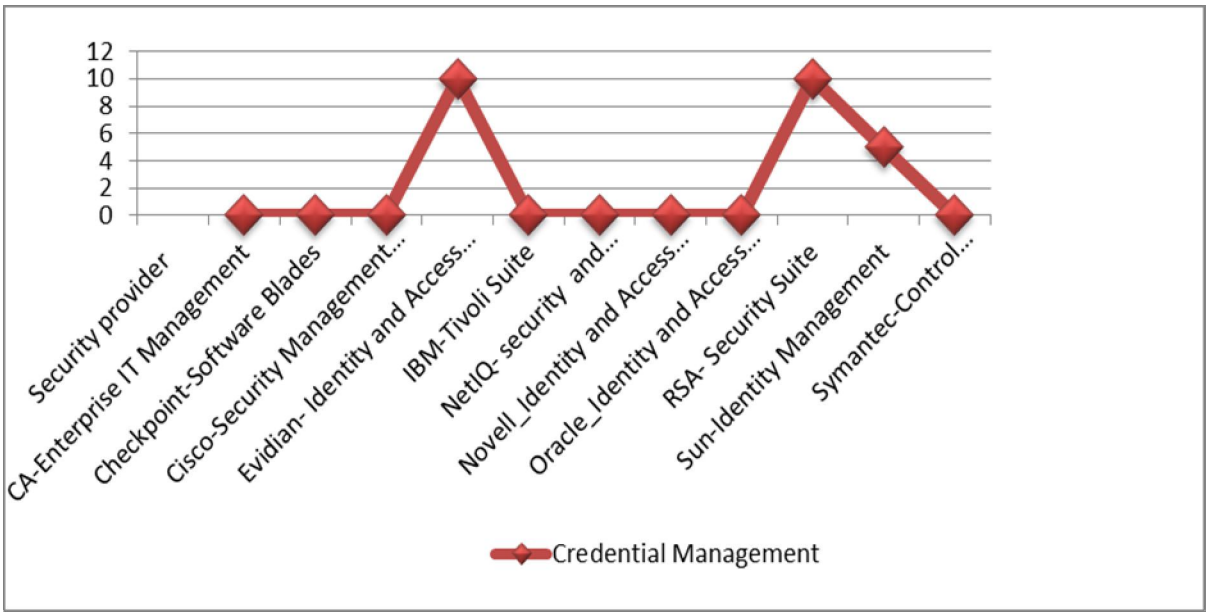

Fig 5: Cloud Computing Security Concerns Implementations

While the credential Metadata management is does not tackled by any credential management company. From above graph it very obvious that if the credentials are managed properly then IDM issue can be resolved easily. We can secure our service and database management by securing the authentication and identity management. This will also reduce the privacy and security threats. Moreover the transportation of the user credential over internet is also a big issue. We should minimize the transportation of cloud user credential over network to make sure the data privacy, data security and data management.

There is an interesting situation is occurred when a cloud user is accessing the services of Window Azure and want o connect Google Docs. There is no such service that can be availed to access the Google docs by using the same login or authentication that is already working with Window Azure. Now another problem stands that what take place if a same cloud user desires to get entrance to the different cloud services that are provides by diverse cloud provider e.g. if there is a condition in which cloud user is potentially using a service of Google docs from Google and that cloud user require to maintaining the databank using additional service facility that is make available by the other cloud service provider say Amazon simple DB or Oracle cloud. Then how user can be used in cooperation the both services commencing from the different cloud service provider? If we think then simple solution is that addressed by the problem is to subscribe the environment of cloud service provider and then be able to get the access to the required service that is facilitated by the different cloud service provider. We have discussed the scenario that is relevant to the traditional cloud service provider and traditional cloud service user exists [7].

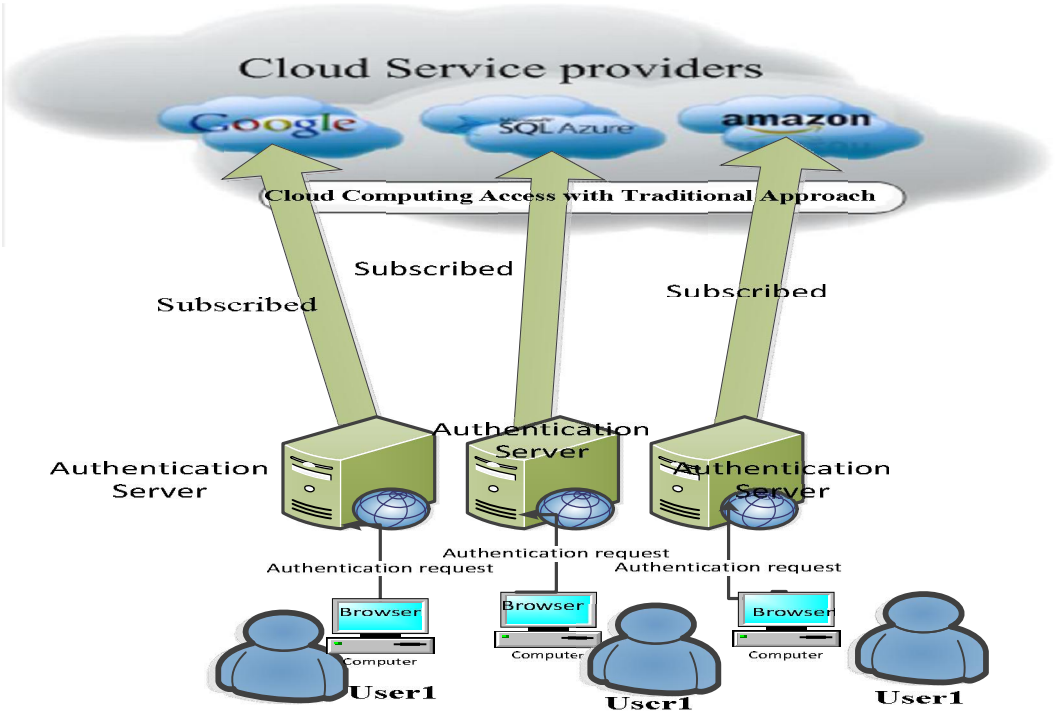

Fig 6: Cloud Computing Data and Services Access in Traditional

3. Proposed solution

The solution we are going to present is that we should use the mechanism that with subscription of the any cloud environment cloud server user can easily access the service of the other cloud service providers. In the given scenarios beyond the traditional cloud service provider environment there are different solution are existing. So in this type of scenario working with traditional cloud computing environment we explain that each cloud service provider is using the same method. The subsequent method intended for the above concern are able to be solve through building one alliance on behalf of the dissimilar cloud service providers as well as through by means of the idea of Single-Sign-On. By means of SSO facility, the users are able to utilize the diverse services which are provided through similar cloud service provider, however, users not utilize dissimilar services provided through diverse cloud services provider.

Secure Identity and Credential Management

Identity and credential management security in cloud computing environment is of great importance for secure businesses and free the cloud. It's possible only

- Eliminating password dependencies
- Centralized Account Management
- Accessing Controls
- Securing Identities

In order to achieve above goals, we need to highlight 4 A's

- Authentication: who is the user?
- Authorization: what is the user allowed to doing?
- Account management: what can the user access?
- Audit Logging: where has the user been?

Designing security around 4 A's guarantees simple and secure credentials management in the cloud and then integrates with existing Domain Controller like ORACLE (Identity Management) and Windows Server (active Directory). Technologies, security standards related to the above problems are SSO, SAML, OpenID, OAuth [16] etc.

Table 4: Comparison among SAML, Information Card, OpenID and OAuth Methods

	Identifiers Issuance	Full	Front Channel User	Back Channel without user	RP/SP Initiated	IDP Initiated	Registration	Discovery
SAML	Allows for a variety of identifier types	General XML-based syntax for communicating identity attributes	Enhanced Client Profile to supports "smarter" clients than default browsers.	Supported by the SOAP Binding, Communicate directly.	Yes	Yes	No	Optional cookie mechanism that RP/SPs discover IDPs.
Information Cards	IDPs, either self-issued or a third party	CardSpace focuses on personal profile attributes (e.g. name, email, etc.)	IMI facilitates all identity flow	No back channel	Yes	No	Manifested through the installation of managed cards into the Selector	Implicit. RP/SPs request identity attributes of CardSpace
OpenID	Users are identified by a personal URI.	OpenID SREG extension focuses on exchange of attributes typically at registration time.	OpenID authentication protocol relies on redirects and HTML Form POSTs by browser	OpenID 3.0 introduce support for direct communication.	Yes	No	No	Implicit. RP/SP discovers IDP b user URI or email.
OAuth	One-time identifier and service is identified rather than the user	OAuth token is for access to RESTful API services	OAuth's 3-legged flow allows users to approve data flow b/w services.	OAuth's 2-legged flow allows services that already authorized	Yes	Expected for OAuth v2.0	Explicit. Identity services pre-register for a consumer key and secret	Explicit. Service directly labeled and accessed.

Now we will try to explore all different ways of identity and credentials management along with their related issues and next step with the help of real world scenarios.

In first way let suppose there is an ordinary user who wants to access a web application. He/she provides identity like email address and password for access. At another situation he needs to access another web application with some other identity and so on for third web application. So, there are two major issues with respect to credentials one is the security and other one is the convenience to use. So this way will not result the above said objectives.

Above said two issues can be resolve by the help of user centric technology-Identity Provider. It's a third trustable party whose basic purpose is to manage user credentials with security and establishing a trusty relationship over the cloud.

Scenario is as under, A user wants to access a web site who requires identity, user asks Identity Provider to let it reply for access and it does. Same process for other many websites to whom he/she has access. There is a convenient to use, better security as credentials are not spreaded over different web sites. Securing identities are there but under trust relationship. Here the identity provider can also be known as Relying Party.

Identity as a Service

There is an enterprise user who needs to access cloud based application such as Salesforce, Google etc. Let's suppose he is residing at a hotel room, At first he needs to establish a connection with the corporate network to authenticate user's identity

given by Active Directory with the help of VPN. Then, throughcompany federated server gets access to cloud application by using SAML or OAuth protocols.[16]

Now the driving force for IAM as a service is, as cloud applications are available over the internet and can be accessed at anytime from anywhere, then why he/she goes to VPN into enterprise server and then go to the cloud application? Is there any direct way through which can be used to provide all the below listed characteristics related to secure credentials management.

- User Management and Provision: addition, deletion of user and use provisioning to different users.
- Authentication: better ways to authenticate users like password etc
- SSO Portal:
- Role Management:
- Compliance Reporting: Report of user who accessed service is sent to the related Enterprise.

All above characteristics can be achieved by IAM as a Service over the cloud computing environment. There is no need to go in an indirect way. Just access IAM and through this interface let them access cloud based services. The word SaaS exist with convenience, cost saving and scalability but with some tradeoffs. Because all cloud computing providers like Google, Amazon, Salesforce etc. are surprising and alarming with the lack of tools for managing user access to services. Confidentiality, Compliance requests and Auditing are top of user's concerns and it should be after all accountable to stop from firewall. We must know with certainty who access the cloud based services when and what actions are performed. It is also seen that user use a week password and convenient which is easy to remember. Enforcing strong password requires frequent support for password reset. Our concern is to set automated provisioning, SSO, string authentication, policy enforcement, monitoring, logging and auditing.

SSO Portals for Enterprises

Being a user of an enterprise that provides access to multiple web services from different cloud like Google, Salesforce, WebeX etc. Enterprise user needs to remember the user name and passwords in each case, which is difficult to remember and as already said that it's a chance of week password. So, it's a real problem that how to access these applications without providing credentials over the cloud which is a security risk, we need to have an SSO portal containing icons of different cloud applications. This SSO portal connects with Credential Manager for user authorization, authentication and access control with the help of Active directory. Now, one the main problem attach here with SSO portal to avoid unauthentic access to this page. To solve this, there is a concept of OTP (one time password) that with one or mlti factor password entries at the time of log on.

So for, we presented different ways to secure identities, credential management, accessing mechanism along with some of the flaws in these approaches has been discussed above. Last way seems to be good in order to fulfill all criteria for a satisfied user as well enterprise for better control over most critical data. Now, the environment of client/ user machine in an organization has communicated with domain controller, KTC- a granted ticket service, and ADFS (active directory Federated service). Also, there is a cloud computing environment contains SaaS, PaaA and Iaas. There is an introduction of ACS which acts as a service party as well as relying party when communicate with ADFS and web apps over cloud respectively.

Let's consider a scenario in which a user comes in the morning and access machine, machine interacts with Domain controller to prove its identity. After then, user needs to access a web application over the cloud with HOMEGRAM. Web Applications are over the cloud demands user's identification, credentials, rights and other data for access. For this that web application interacts with the ACS, Here ACS acts like an Identity provider and there is a trusty relationship between these two parties. ACS contains an HRD document that contains all those enterprises who has a trusty relationship with ACS. From where an ACS check pushes back the user's request to ADFS server. ADFS uses KTC for authentication. Ticket Granting Ticket interacts with Domain controller and sends some feedback in the form of ticket. A link has been established among TKT, User machine and ADFS. Domain controller generates an ST and send to KTC from where it reached to ADFS through client. It's a SAML token containing user's credentials and identity. Now this SAML token is signed by ADFS and send to its trusty relationship ACS. ACS validates the signature and removes the signature of ADFS and attaches its own signature and further redirects the user to again send to web application. As soon as web application receives ACS signatory SAML document, access rights are given to user. In this whole procedure, it is evident that all users related information remains centralized. There is no spreading of user's credentials in an unsecure manner. Fine grained Access Management and securing identities.

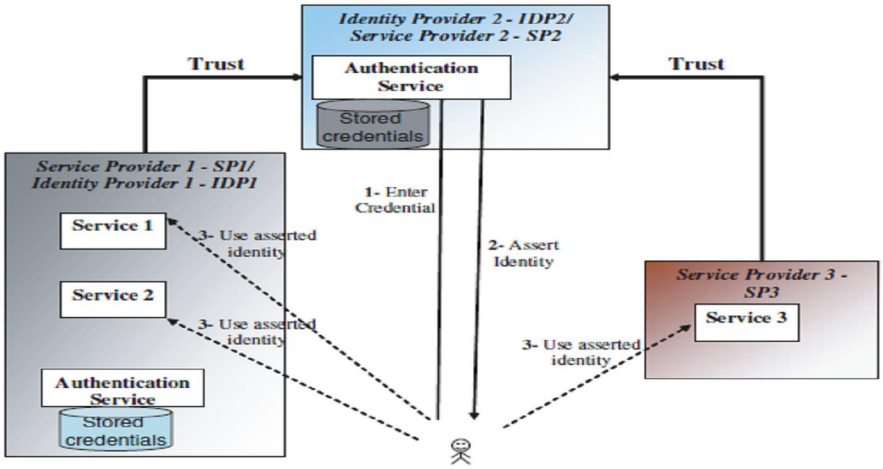

Fig 5: Federate Identity Management [16]

The previously sated problems are able to be solved through developing a federation having customary cloud service providers that offer diverse services as diverse cloud service providers. By the means of supporting Single Sign On procedure, every user is able to get the access to entire services those offered through diverse cloud service provider that are associate with federation alliance. The ways out of customary cloud computing setting are able to be resolve through formulating a universal open cloud federation. The offers solution those are able to be observed as given below. As revealed in above diagram, we are taking an instance of the majority well-known cloud service provider of current time which is Amazon, Google as well as Microsoft SQL Azure. All of these 3 cloud service suppliers are associate with cloud federation, then they can be offer the entire services to e client those are listed as cloud computing alliance. For example we have assessed the matter of customary cloud setting that major part of this cloud federation is offering SSO among the user as well as diverse cloud suppliers those are the official members in this federation.

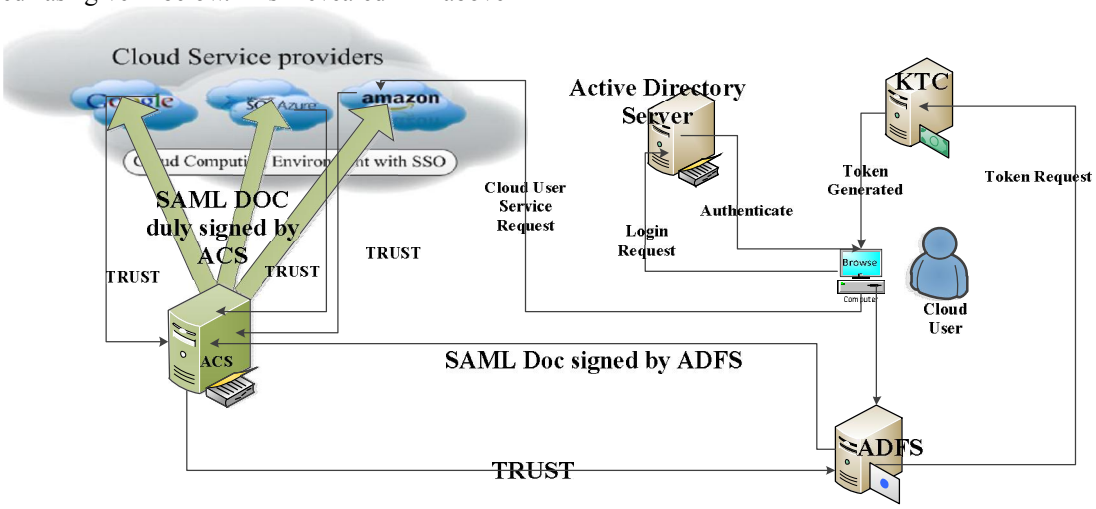

Fig 4: Cloud Computing Access with SSO

Security Issues Related to Cloud Computing federation

There are important security issues that require to must be tackled when recognizing moving serious applications as well as critical data to public plus joint cloud computing settings. Cloud providers have to develop enough panels and controls to provide either similar or better rank security as compared to business. This cloud computing association offers huge conception for distributing services as of diverse cloud service providers through immediately Single Sign On procedure. The diverse models intended for cloud service release (, PaaS IaaS, SaaS) may hazing dissimilar necessities of the client when

it comes to security. Recognizing that who is accountable for what is very important earlier affecting something of value to a cloud [10], [7].

4. Conclusion and future work

Our proposed model will be secure through using different authentication methods like SAML, OpenId and OAuth. Single Sign On provides the secure Identity management mechanism by using the new secure proposed model. The cloud data management is more secure less risky if we use the secure IDM and Authentication services and application through data is managed and execute by Single Sign On. Our idea about formulating a well-organized plus extra precise cloud computing federation alliance which is take away the complication of cloud client in a customary cloud situation. Through utilizing same kind of federation alliance be a worldwide method to offer diverse cloud services by single position as well as user could not require sign-on for diverse geographically and services level cloud for reason that of bringing in the Single-Sign-On federation as well as probing among clouds. Our proposed solution is focused for high-quality federation as well as spotlight on other area of this solution. The problem relating the implementation of safety standard and risk free federation is our future concern.

References

[1]. NIST SP 800-145, "A NIST definition of cloud computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf : Retrieved on Saturday 11 May 2012

[2]. Ian Foster,Yong Zhao, Ioan Raicu, Shiyong Lu (2008), Cloud Computing and Grid Computing 360-Degree Compared, Grid Computing Environments Workshop, 2008. GCE '08, Digital Object Identifier: 10.1109/GCE.2008.4738445, pp:1-10.

[3]. Cloud Security Alliance December 2009 http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf: Retrieved on Saturday 11 May 2012.

[4]. S. Cantor and N. Klingenstein. Understanding shibboleth. Guideline, last edited 2007. [http://spaces.internet2.edu/display/shib], last viewed 23 January 2009. Retrieved on Saturday 11 May 2012, from http://www.ca.com/~/media/Files/IndustryResearch/lockheed-martin-cyber-security_238215.pdf

[5]. E. Damiani, S. D. C. di Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati. Balancing Confidentiality and Efficiency in Untrusted Relational DBMS. CCS, 2003.

[6]. Arvind D Meniya, Harkishan B Jethva (2012) International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1, Jan-Feb 2012, pp:891-895

[7]. R. Gennaro, C. Gentry, and B. Parno. Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers. STOC, 2010.

[8]. Arvind D Meniya, Harkishan B Jethva (2012) International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1, Jan-Feb 2012, pp:891-895

[9]. B. Thompson, S. Haber, W. G. Horne, T. Sander, and D. Yao. (2009) Privacy-Preserving Computation and Verification of Aggregate Queries on Outsourced Databases. HPL-2009-119.

[10]. W. Itani, A. Kayssi and A. Chehab. (2009) Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures; Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Department of Electrical and Computer Engineering, American University of Beirut, Beirut Lebanon.11, 07, 2020.

[11]. J. Viega, McAffee, (2009) Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.

[12]. G. Reese, (2009)"Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.

[13]. M. Kretzschmar and S. Hanigk (2010) "Security Management interoperability challenges for Collaborative Clouds", 2010 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management. pp. 44-48. 2010.

[14]. Wang, Q., et al., (2009) Enabling public verifiability and data dynamics for storage security in cloud computing. Computer Security–ESORICS 2009, 2009: pp. 355-370.

[15]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, Provable data possession at untrusted stores, in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

[16]. White paper: Internet-Scale Identity Systems: An Overview and Comparison. Ping Identity Corporation pp 1-17. Retrieved on Saturday 04 May 2012, from https://www.pingidentity.com/unprotected/upload/wp_internet_scale_identity_systems.pdf.