Identity Management in Cloud Computing: Issues, Incidents and Solutions

Ashanpreet Kaur, Ramandeep Singh

Abstract: Cloud computing refers to computing over the internet. Here internet refers to as cluster of clouds. Cloud computing provides its customers with a virtual cloud. The World Wide Web is casted to a single virtual computer by the cloud. Cloud computing is a very vast term. It has grown in the recent past a lot. Due to the immense advantages of cloud came the limitations too. The major hurdle is the security in the cloud. To keep the customer in your grip you need to make them sure that the data stored over the cloud is absolutely in safe hands. But the user is still in shadow of doubt, is my data safe? What if it lands into the wrong hands? How about tempering of data by unauthorized person? What if the culprits find where my data is kept? God knows what all questions will be haunting the customer. Also this paper proposes the use of user identity to manage the data saved on the cloud. This will help to achieve a safe distance from security threats. This paper will help all those in traumas to narrow out different security models and ideas in thus to secure cloud computing.

Keywords: Cloud computing, data storage, user identity management, security threats, secure cloud computing

I. INTRODUCTION

Cloud computing simply refers to computing over the internet [1]. The internet here means cluster of clouds. The cloud provides us with a lot of advantages. With the help of internet the cloud provides these advantages. It helps people to avail the facilities online may be from anywhere in the world or at any span of time; say Leeds, Greece, Seattle, Mozambique, Christchurch etc. The cloud recast's the complete World Wide Web into a virtual computer. The cloud is a vast term. It is very much different from a desktop. The desktop is physical, you may touch it. Yet the cloud is imaginary, but still it is for real although you may not be able to touch it. The cloud is cheaper than any other application. The cloud has zero maintenance cost. The customer is free from any maintenance and management responsibilities. The cloud is a self healer. With this solitary feature it is termed as "utility computing" or "IT on demand" [1]. Other applications might focus on the hardware, but the cloud is something different. It does not lay emphasis on the hardware but does on the code. Examples could be: Google apps provided by Google and Microsoft apps. Generally, in cloud operations are managed by using virtual cloud [2]. Let's explain cloud computing in a simpler way. A person wants to travel from city Calgary, Alberta, Canada to Cross-field, Canada which is exactly 43 kilometers or 27 miles. The person would prefer taking a bus. He gets onto the bus reaches the destination and pays for his ticket. Here he pays for the service he uses rather than purchasing the complete bus. This is what exactly is cloud computing in simple terms. You pay only for the services you would be using. Another example could be an electric bill that arrives at our homes every single month. The units of electricity that we used for our household purposes we pay only for it, not for the complete thermal power plant's expenses'.

The reasons due to which cloud computing became popular are: scalability, Instant, save money and time.

Scalability can be explained as how easy is it to grow or to shrink the network according to the demand. Instant means available anytime. If the need goes down, turn it off. If there's ample amount of demand, keep it high. Also it feels comfortable and reasonable to pay for only the amount of services you use. The more you'll use the more pay. It's directly proportional to the increase or decrease in the demand.

A. Service models of cloud computing: [3]

1) Infrastructure-as-a-service (IaaS): It is the most comprehensive cloud computing platform. It is mainly used by full time developers or large scale customers. They provide infrastructure to develop, run and store the apps on the cloud. Example: Amazon E2.

2) Platform-as-a-service (PaaS): They help us run the application with a specific environment. The app is eventually locked to the platform that was used for its creation. It gives you the ability to make your own app. This is very much available to a vast audience. Example: Facebook.

3) Software-as-a-service (SaaS): It is the basic form of cloud computing. It allows the usage of cloud apps. There is no third party development or resource from the user, but these may offer powerful tools right from the web-browser. Example: Google account.

B. The cloud platform is further divided into three parts:[4]

1) Public cloud: These are the ones in which the services are available over the internet to the public at a very vast area. In public cloud a service provider makes resources such as applications and storage.

2) Private cloud: It is typically a private network that is being used by one consumer for whom data security and privacy is the foremost concern. The disadvantage of private cloud is that the customer has to take huge amounts of cost for setting up the network and maintaining it all alone.

3) Hybrid cloud: Hybrid is when a customer has mixed sorts of demands, both for dedicated server and cloud hosting. It is used when an organization need more processing-power than its available in house and obtains extra requirement on the cloud. This is termed as "Cloud Bursting". Also it is used when a customer wants to move completely from a private cloud to completely public cloud.

C. Benefits of Cloud Computing

1) Access to resources

It is the greatest advantage of cloud computing. It provides access to the processing power of multiple remote computers [5]. This enables customers to take advantage of greater computation speed and larger storage capacity than fraction of the cost.

2) Mobility

Customers can access the services from almost any location in the world because the services are web- based and because of the advent of mobile devices. This can enable employees to access important business tools while they are on the move. For example an employee can fill a form while being on a train, providing rest of the business with access to that data in real time.

3) Easily scalable

Both the monthly subscription and pay as you use charging models make it easy for the amount of service being provided to be increased or decreased. The supplier simply provides access to additional users or increases the storage space available in exchange for higher money payments by the customer. The scalability aspect of cloud computing a model makes it's extremely attractive to grow organizations with varying levels of demand for computer resources.

most organizations can provide on their premises and at a

4) Data security and storage capacity

Data security is of particular importance as lapses in procedure can cause severe financial and reputational damage. For the majority of organizations the data security and data storage capacity offered by data centers is far superior to that which can afford in house.

5) Cost saving

Cost savings are encouraged as of the policy pay as you use. This very much decreases the cost of the customers and in return enhances the customer usage. This means that there is no upfront payment as there would be with the purchase of license in orthodox software license model. Although there may be an initial step or configuration fee, that is usually very low. The pay as you use system benefits the organizations with peaks and troughs in its demand for computing resources. It is cheaper than paying for exclusive use of resources to meet peak demands. Cloud computing services do not represent a capital expenditure.

6) Maintenance support

The suppliers will usually offer ongoing support services. However remote hosting of the services makes the process of maintaining and supporting the services less intrusive for the customer. The supplier can handle backups, updates and upgrades automatically and remotely without visiting the

customer's site. This will generally mean that maintenance and support can be carried out more quickly.

7) Environmental friendly

It has been suggested that data centers are a green alternative to in house computing and this is shortly debated topic. This is because servers in very large data centers typically run at around eighty percent while an in house server might run at five percent capacity. I t is probable that the existence of cheap and more easily accessible cloud computing architecture has increased the overall demand for computation, outstripping the energy efficient gains that have been made in the data centers.

8) Free trails

Some suppliers offer the opportunity to trial a product for their period without charge. This is made easier by the supplier's ability to terminate access at the end of the period and provides them with the opportunity to hook the customer. This business model is sometimes referred to as 'free-mium'.

D. Disadvantages of Cloud Computing

1) Internet reliability

IT services provided over the internet have lack of internet access or slow connections that will hinder access to those services. Where such kinds of services are business critical and that can be a major problem. As the internet access improves this should be a diminishing concern. Also we should remember that there is no guarantee of uninterrupted services even with locally hosted software.

2) Dependence on supplier

In cloud computing the customer is dependent on the supplier for day-to-day access for the IT services rather than just for support and maintenance. If the supplier is in financial trouble, its ability to provide the services may be effected. However dependence on the supplier is a common for most organizations and the usual risk assessment can be carried out to mitigate the risk. Due diligence checks on the supplier may reveal that whether it is a financial trouble and references can be passed for existing or past customers whether the supplier has a reliable history or not.

3) Security

Corporations will have up will raise red flags. The usage of thin clients could possibly be high-jacked if people careless with data. Also SLA's will need to have provisioning within them that directly specifies how cloud computing providers plan on protecting data [6].

4) Little or no reference

Because of privacy concerns, cloud vendors for most of the part are unable or unwilling to present case studies about companies that are currently using their services. As a matter of fact there are very few large companies that are publicly reporting their usage of cloud computing at large scale. This leaves many organizations feeling shy about usage of cloud computing resources as of yet even though it has become a popular terminology in the tech world. Other two disadvantages of this technology are computing along with the fact that very few companies are reportedly using the technology because the entire cloud movement has some problems. It may be possible that the small start-up companies will have to take advantage of come larger ones before they begin to adopt cloud computing.

The cloud actually needs a connection for its working, if it is down the services are not able to perform that much. Even if the service providers keep a close eye on the connection still the risk prevails. Software capabilities are another problem. Connecting wireless can be difficult when it comes to personal devices.

Another big issue can be if you have plenty of data to deal with. As there is no specific answer to the user's question "who owns the data?" so onto this basis the user sets his set of terms and conditions that sometimes are hard to maintain. Many of the disadvantages of cloud computing are due to the fact that the technology is still relatively new. In other words they will be addressed in time, as more and more users adopt cloud computing.

Being able to keep important data secure has always been an issue in IT's. But with a technology that takes information outside of the virtual secure walls most

II. OVERVIEW

In this section, the author has discussed security and Identity management system.

A. Security

Security is one of the major factors in cloud computing. Hackers and malicious intruder may hack into cloud accounts and steal sensitive data stored in cloud systems [7]. Many methods of providing security would be cryptography, security algorithms [8]. But how to make sure the information stored on the cloud by the user is still secure enough that it can't be accessed by an unauthorized user. Cloud promises its users confidentiality, integrity and availability. Security is not a feature; it is a property of a system [9]. All this study leads to use of identity management.

B. Identity Management

Identity management deals with the identification such as a system in a country. [10]. IDM systems are the policies that define which devices are used or which ones are allowed on the network. IDM in cloud has to manage and control virtual devices, service identities, control points etc. IDM has become an important part of cloud these days. Now cloud providers need to control usernames, passwords and other information that is used to identify, authenticate and authorize the users for various applications [11].

Examples: Policy definition, reporting, alerts and alarms. Unauthorized users try to log in the alarm and the alarm goes on. Some systems offer dictionary integration support for both wired and wireless systems. Models of IDM and security challenges [12] are shown in table 1.

IDM and SSO model	Advantages	Disadvantages	Security Challenges
Independent IDM Stack	• Easy to implement • No separate integration with enterprise directory	• The users need to remember separate credentials for each SaaS application	• The IDM stack should be highly configurable to facilitate compliance with enterprise policies; e.g., password strength, etc.
Credential Synchronization	• Users do not need to remember multiple passwords	• Requires integration with enterprise directly • Has higher security risk value due to transmission of user credentials outside enterprise perimeter	• The SaaS vendor needs to ensure security of the credentials during transit and storage and prevent their leakage
Federated IDM	• Users do not need to remember multiple passwords • No separate integration with enterprise directory • Low security risk value as compared to credential synch	• Relatively more complex to implement	• The SaaS vendor and tenants needs to ensure that proper trust relationships and validations are established to ensure secure federation of user identities

Table 1: IDM models

Identity management involves not only presentation of self but a response to a range of threats arising from the proliferation of personal information online [13].

Following are the two, out of many, incidents related to identity theft and data breach in major cloud service providers.

- *Apple*

Recently there was a bad time for the Apple. The hacking of personal photographs of famous personalities was quite a rumor, which turned true. The hacking was from the iCloud at a worst time when apple's new technology phones were

about to be launched. The customers are blaming the company whereas Apple says the theft has been a result of brute-force. Brute-force is a technique when the hacker tries to crack all the possible passwords until and unless he succeeds. The ones with weak passwords were the ones to be taken down at first. This downfall affected the Apple's sale, but they say it should have been the responsibility of the customers to take of their own personal stuff.

- *Yahoo*

There have been cases for theft of yahoo mail accounts. The passwords and usernames have been collected from the databases that were owned by third party that have been compromised. The company then was then sending notifications to all their affected users to change their existing passwords to new ones. The ones that were affected received messages from the company about the loss.

III. OBJECTIVES

- Provide Security at various levels of user's sign-on.
- Classifying data according to the security levels and apply various encryption schemes to protect classified data.
- Refreshing of keys after a specific span of time.

The data that gets to be stored in the cloud will be systematically arranged according to their sensitivity. This actually means the data that needs a lot of security will be saved at a high security level. The data for example your Swiss account's password can be provided with Z security. The user's need to sign in their account in which the data is to be stored, have to answer some security questions. They need to fill in their passwords to access the data. A lot of security checks will be provided at this level so in case not to lead the important information to the culprits hands. The data with medium sensitivity will be stored at a medium security check. Example: The information of all of your bank accounts and the money stored in them, also to whom who want to assign your will, such kinds of data will be stored on this level. The security check here is the security questions that the user will have to answer in order to gain access to their stored data. The ones left with least data security will normally be provided by user-id and password login. The data here could be the social networking site's accounts.

Various encryption techniques will be applied to the stored data in case they can't be accessed by unauthorized users. If a person fails to pass the security check may be even at one base point, he or she will not get the authority to use the data stored at the cloud. The classified data will not be accessed by the person even if they pass the level of security questions, because a very effective method at the security check is present. Another amazing scenario present here is the refreshing [14].

IV. OUTCOME

The outcome is a system that provides cloud security i.e. security of the data that is stored on the cloud with the help of identity management system. The data entered has been secured with the assistance of various encryption algorithms and using the identity of an individual. Security checks are supporting every level where the data needs to be stored. The confidential level helps the data be at a bay from culprits with the help of finger print scans and security questions that might not be easy to cross. The second level is for the internal use, that data which needs medium sort of security. Such security is provided with the help of security questions those are not same as the ones with tight security or level one. The third kind of security check is normal like any social-networking site. You fill in your username and password and you may have access to your account.

Main reason that makes this system different from other systems is the use of identity of a person. This is explained with the use of fingerprint scans that are not easily prone to attacks. Another sort of security provided with this system is the refreshing of keys or passwords after a particular span of time. This helps the system be protected from attacks such as brute force.

VI. REFERENCES

[1] Farhan Bashir Shaikh and Sajjad Haider, "Security Threats in Cloud Computing", IEEE, 6th International Conference on Internet Technology and Secured Transactions, December 2011.

[2] Shigeaki Tanimoto, Manami Hiramoto, Motoi Iwashita, Hiroyuki Sato and Atsushi Kanai, "Risk Management on the Security Problem in Cloud Computing ",IEEE, 1st ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, 2011.

[3] Wang Meiyan, "Analysis to the Weakness and safety in Cloud Computing", IEEE, 3rd International Conference on Intelligent System Design and Engineering Applications, 2012.

[4] Safiriyu Eludiora, Olatunde Abiona, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime and Lawrence Kehinde," A User Identity Management Protocol for Cloud Computing Paradigm", Published Online, March 2011.

[5] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE, 2011.

[6] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", IEEE, 2012.

[7] Rajkumar Chalse, Ashwin Selokar and Arun Katara, "A New Technique of Data Integrity for Analysis of the Cloud Computing Security", IEEE, 5th International Conference on Computational Intelligence and Communication Networks, 2013.

[8] Ann Cavoukian, "Privacy in the clouds", Published Online, Identity Journal Limited, December 2008.

[9] Ruth Halperin and James Backhouse, "A roadmap for search on identity in the information society", Published Online, Identity Journal Limited, December 2008.

[10] Ardi Benusi, "An Identity Management Survey on Cloud Computing", Int. Journal of Computing and Optimization, Vol. 1, 2014, no. 2, 63-71, Albania.

[11] Anu Gopalakrishanan, "Cloud Computing Identity Management", SETLabs Breifings Vol. 7, No. 7, 2009.

[12] D. Barnard-Wills and D.Ashenden,"Public sector engagement with online identity management", Springer Cranfield University, Shrivenham, Swindon SN6 8LA, UK.

[13] Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo Yan," Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 6, June 2013.

[14] "Data classification for cloud readiness", Microsoft Trustworthy Computing".

Ashanpreet Kaur
Department of Computer Science
Lovely Professional University, Jalandhar, India
ashansidhu88@gmail.com

Ramandeep Singh
Department of Computer Science
Lovely Professional University, Jalandhar, India
ramankhosa@gmail.com