Reaping Cloud by Ensuring Data Storage Security

Ms.Khushboo Sandhi

PG student (IT), L.D. Engineering College, Ahmedabad- Gujarat
khushboo.sandhi@gmail.com

Abstract **- The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.**

Index Terms **- Cloud Computing, Secret Sharing , Software as a Service, Cloud Service Provider.**

I. INTRODUCTION

Cloud sources should address privacy and security issues as a matter of high and vital priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the opportunity that there are malicious insiders in the single cloud. In current years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds". As data and information will be shared with a third party, cloud computing users want to keep away from an untrusted cloud provider. Defending private and significant information, such as customer details and a patient's medical records from attackers or malicious behaviour is of serious importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and and multi-clouds in cloud computing is surveyed.

II. RELATED WORK

National Institute of Standards and Technology(NIST) describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources like networks, storage, servers, applications, services and that can be rapidly provisioned and released with minimal management effort or service provider interaction".

2.1 Cloud Computing Components

The cloud computing model consists of three delivery models, five characteristics, and four deployment models. The five input characteristics of cloud computing are: location-independent resource pooling, on demand self service, rapid elasticity, deliberate service and broad network access. These five characteristics represent the first layer in the cloud environment architecture.

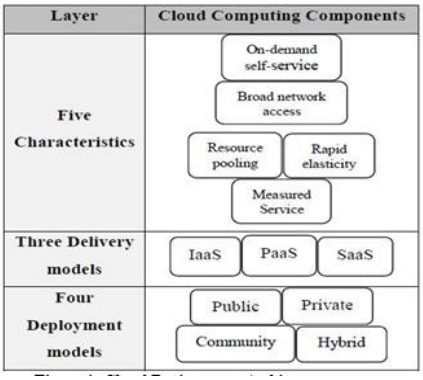

Fig. 1: Cloud Environment Architecture

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, information storage space and computing services. It is the delivery of computer infrastructure as a service. A model of IaaS is the Amazon web service. In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service. An example of PaaS is GoogleApps. Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS. A Model of SaaS is the Salesforce.com CRM application this model represents the second layer in the cloud environment architecture.

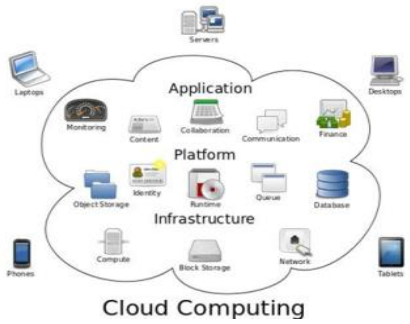

Fig. 2: Cloud Applications Structure

Cloud deployment models contain public, community, private and hybrid clouds. A cloud environment that is available for multi-tenants and is accessible to the public is called a public cloud. A private cloud is accessible for a particular group, even as a community cloud is modified for a specific group of customers. Hybrid cloud communications is a composition of two or more clouds. This model represents the third layer in the cloud environment architecture.

Fig. 3: Cloud Types

2.2 Cloud Service Providers Examples

In the commercial world, various computing needs are provided as a service. The service providers take care of the customer's requirements by, for illustration, maintaining software or purchasing luxurious hardware. For example, the service EC2, created by Amazon, offers customers with scalable servers. There are many features of cloud computing. First, cloud storages, such as AmazonS3, MicrosoftSkyDrive, or NirvanixCLoudNAS, authorize consumers to access online data. Second, it offers computation resources for users such as Amazon EC2. Third, Google Apps or versioning repositories for source code are examples of online collaboration tools.

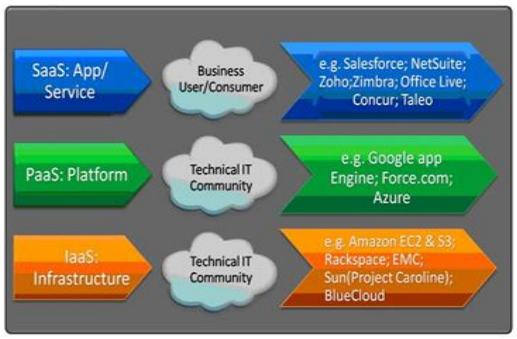

Fig. 4: Cloud Computing Providers

2.3 Layers of Cloud computing model

There are five layers in cloud computing model, the Client Layer, Application Layer, Platform Layer, Infrastructure Layer and Server Layer. In order to address the security problem, every level should have security implementation.

Client Layer : In the cloud computing model, the cloud client consist of the computer hardware and the software that is totally based on the applications of the cloud services and basically designed on such way that it provides application delivery to the multiple servers at the same time, as some computers making use of the various devices which includes computers, phones, operating systems, browsers and other devices.

Application Layer: The cloud application services deliver software as a service over the internet for eliminating the need to install and run the application on the customer own computers using the simplified maintenance and support for the people which will use the cloud interchangeably for the network based access and management of software by controlling the activities which is managed in the central locations by enabling customers to access the application remotely with respect to web and application software are also delivered to many model instances that includes the various standards that is price, partnership and management characteristics which provides the updates for the centralize features.

Platform Layer : In the cloud computing, the platform services provides the common computing platform and the stack solution which is often referred as the cloud infrastructure and maintaining the cloud applications that deploys the applications without any cost and complexity of the buying and managing the hardware and software layers.

Infrastructure Layer : The Cloud infrastructure services delivers the platform virtualization which shows only the desired features and hides the other ones using the environment in which servers, software or network equipment are fully outsourced as the utility computing which will based on the proper utilization of the resources by using the principle of reusability that includes the virtual private server offerings for the tier 3 data centre and many tie 4 attributes which is finally assembled up to form the hundreds of the virtual machines.

Server Layer : The server layer also consist of the computation hardware and software support for the cloud service which is based on the multi-core processor and cloud specific operating systems and coined offerings.

2.4 Cloud Computing Attacks

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors criminals may attempt include:

a. **Denial of Service (DoS) attacks :** Some security professionals have argued that the cloud is more vulnerable to DoS attack, because it is shared by many users, which makes DoS attack much more damaging.

b. **Side Channel attacks :** An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

c. **Authentication attack :** Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has or is. The mechanism used to secure the authentication process and the methods used are a frequent target of attackers.

d. **Man in the middle cryptographic attacks :** This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

e. **Inside-Job :** This kind of attack is when the person, employee or staffs who is knowledgeable of how the system runs, from client to server then he can implant malicious codes to destroy everything in the cloud system.

2.5 Security Requirements

Security measures assumed in the cloud must be made available to the customers to gain their trust. There is always a possibility that the cloud infrastructure is secured with respect to some requirements and the customers are looking for a different set of security. The important aspect is to see that the cloud provider meets the security requirements of the application and this can be achieved only through 100% transparency. Open cloud Manifesto exerts stress in transparency in clouds, due the consumer's apprehensions to host their applications on a shared infrastructure, on which they do not have any control in order to have a secured cloud computing deployment, we must consider the following areas, the cloud computing architecture, Governance, portability and interoperability, traditional security, business continuity and disaster recovery, data centre operations, incident response, notification and remediation, Application security, Encryption and Key Management, identity and access management. One of the reasons why users are very anxious of the safety of their data being saved in the cloud is that they don't know who is managing it while in the server of the cloud computing service provider. Typical users who uses the cloud computing service like storing their files in the sever to access it anywhere they want through internet, don't bother much about the security of their files, those documents are common files that don't need to be secured. But in the case of big companies which have very important information to take care of, they need to have secured cloud computing system.In order to have secure cloud system, the following aspect must be considered:

Authentication:
Is the process of verifying a user or other entity's identity. This is typically done to permit someone or something to perform task. There is variety of authentication system, some are stronger than others. A strong authentication system ensures that the authenticators and messages of the actual authentication protocol are not exchanged in a manner that makes them vulnerable to being hijacked by an intermediate malicious node or person. That is, the information used to generate a proof of identity should not be exposed to anyone other than the person or machine it is intended for.

Authorization:
Is when the system decides whether or not a certain entity is allowed to perform a requested task .This decision is made after authentication the identity in question. When considering an authentication system for a particular application, it is crucial to understand the type of identifier required to provide a certain level of authorization.

Confidentiality:
Confidentiality is needed when the message sent contains sensitive material that should not be read by others and therefore must not be sent in a comprehensible format. A loss of confidentiality is the unauthorized disclosure of information. Confidentiality, as it relates to security and encryption techniques can be obtained by encrypting messages such that only intended recipient are able to read them.

Integrity:
Integrity is ensuring that the data presented are true and valid master source of the data and includes guarding against improper information modification or destruction to ensure information non-repudiation and authenticity. A loss of integrity is the unauthorized modification, insertion, or destruction of information.
One way of ensuring of data integrity is by using simple checksums which prevent an attacker from forgoing or replying messages. Checksum is usually implemented when the channel between communication parties is not secure and ensure that the data has reached its destination with all bits intact, if bits have been modified, that the modification will not go unobserved.

Non-Repudiation:
Non repudiation is ensuring that a traceable legal record is kept and has not been changed by a malicious entity. A loss on non-repudiation would result in the questioning of the transaction that has occurred. A simple example of non-repudiation is signing contract. The signer cannot claim they did not agree a contract because there is an evidence that they did agree. The difference is that a signature can be forger but good encryption cannot.

III. SECURITY RISKS IN CLOUD COMPUTING

In different cloud service models, the security responsibility among users and providers is different. According to Amazon network, their EC2 addresses security control in relation to physical, and virtualization security, environmental, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data.

Data Integrity
It is not an easy task to securely maintain all essential data where it has the need in many applications for clients in cloud computing. To maintain our data in cloud computing, it may not be fully trustworthy because client doesn't have copy of all stored data. We have to begin new proposed system for this using our data reading protocol algorithm to check the integrity of data before and after the data insertion in cloud. Here the security of data earlier than and following is checked by client with the help of CSP using our "effective automatic data reading protocol from user as well as cloud level into the cloud" with truthfulness.

Data Intrusion
The importance of data intrusion detection systems in a cloud computing environment, We find out how intrusion detection is performed on Software as a Service, Platform as a Service and Infrastructure as Service offerings, along with the available host, network and hypervisor based intrusion detection options. Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security.

Service Availability
Service availability is most significant in the cloud computing security. Amazon previously mentions in its authorizing agreement that it is possible that the service might be unavailable from time to time. The user's web service may conclude for any reason at any time if any users files break the cloud storage policy. In accumulation, if any damage occurs to any Amazon web service and the service fails, in this casing there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.

IV. MULTI-CLOUD COMPUTING SECURITY

DepSky System: Multi-Clouds Model
The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were introduced by Vukolic. These terms suggest that cloud computing should not end with a single cloud. Using their design, a cloudy sky incorporates unlike colors and shapes of clouds which lead to different implementations and administrative domains. In the proposed system Bessani present a virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-

clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, combining Byzantine quorum system protocols, cryptographic secret sharing and erasure codes.

DepSky Architecture and Data Model

The DepSky architecture consists of four clouds and every cloud uses its own particular interface. The DepSky algorithm exists in the client's machines as a software library to communicate with each cloud. These four clouds are storage clouds, so here no codes to be executed. The DepSky library authorizes reading and writing operations with the storage clouds. The use of diverse clouds requires the DEPSKY library to deal with the heterogeneity of the interfaces of each cloud provider. An aspect that is especially important is the format of the data accepted by each cloud. The data model allows us to ignore these details when presenting the algorithms.

DepSky Data model

As the DepSky system contract with various cloud providers, the DepSky library deals with various cloud interface providers and as a result, the data format is acknowledged by each cloud. The DepSky data models consist of three abstraction levels: the conceptual data unit, a generic data unit, and the information unit implementation.

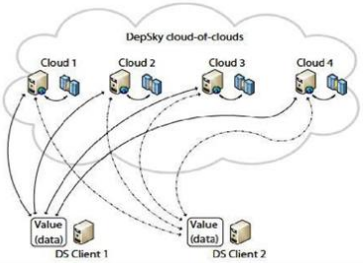

Fig. 5: DepSky Architecture

The DEPSKY data model with its three abstraction levels. In the first (left), there is the conceptual data unit, which communicates to the basic storage object with which the algorithms work a register in distributed computing. A data unit has a exclusive name, a version number, verification data and the data stored on the data unit object. In the second level (middle), the theoretical data unit is implemented as a generic data unit in an abstract storage cloud. Each basic data unit, or container, holds two types of files: a signed metadata file and the files that store up the data. Metadata files hold the version number and the verification data, jointly with other information's that applications may demand. Notice that a data unit can store more than a few versions of the data, i.e., the container can hold several data files. The name of the metadata file is simply metadata, while the data files are called value<Version>, where <Version> is the version number of the data (e.g., value1, value2, etc.). Finally, in the third level (right) there is the data unit implementation, i.e., the container translated into the specific constructions supported by each cloud provider.

V. ALGORITHM USED

Secret Sharing Algorithms

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the 2012 45th Hawaii International Conference on System Sciences file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.

VI. EXISTING SYSTEM

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds".

Disadvantage of Existing System

1. Cloud providers should address privacy and security issues as a matter of high and urgent priority.
2. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

VII. PROPOSED SYSTEM

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an un-trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance.

In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed.

7.1 Advantage of Proposed System

1. Data Integrity
2. Service Availability
3. The user runs custom applications using the service provider's resources
4. Cloud service providers should ensure the security of their customer's data and should be responsible if any security risk affects their customer's service infrastructure.

7.2 Modules

Module Description

Data Integrity:

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers.
One of the solutions that they propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al. State that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al. Claim that using the Byzantine fault tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place.

Data Intrusion:

According to Garfinkel, another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

Service Availability:

Another major concern in cloud services is service availability. Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers.

DepSKy System Model:

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Bessani et al. explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

VIII. CONCLUSION AND FUTURE WORK

Now a days the use of cloud computing has speedily increased and cloud computing security is still measured the major issue in the cloud computing atmosphere. Customers do not want to misplace their private data as a consequence of malicious insiders in the cloud. The loss of service availability has caused many problems for a large number of customers in recent times. Additionally, data intrusion leads to many troubles has caused many problems for a large number of customers in recent times. Additionally, data intrusion leads to many troubles for the users of cloud computing. The principle of this work is to survey the recent research on single clouds and multi- clouds to address the security risks and solutions. The research has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area if security. We maintain the immigration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user. For future work, we intend to offer a framework to supply a secure cloud database that wills assurance to avoid security risks facing the cloud computing community. This structure will be relevant multi-clouds and the secret sharing algorithm to decrease the risk of data intrusion and the loss of service accessibility in the cloud and ensure data integrity.

REFERENCES

[1] Sapthami, P.Srinivasulu, B. Murali Krishna. "A Novel Approach to Cloud Computing Security over Single to Multi Clouds"Int. Journal of Engineering Research and Application Vol. 3, Issue 5, Sep-Oct 2013. pp.636-640

[2] Cong Wang, Qian Wang, and Kui Ren gy Wenjing Lou "Towards Secure and and Dependable Storage Services in Cloud Computing". Institute IEEE Transactions on Cloud Computing Date of Publication: April-June 2012 Volume: 5.
[3] Sajjad Hashemi1 International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.
[4] Johannes Braun Alexander Wiesmaier Johannes Buchmann " On the Security Of Encrypted Secret Sharing" 2013 46th Hawaii International ty on System Sciences.
[5] K Chandra Moulnali and U Sesadri " Single to Multi Clouds for Security in cloud computing by using Secret Key Sharing" International journal of computers and technology Aug 15th,2013.
[6] Kapila Sharma1, Kavita Kanwar1, Chanderjeet Yadav, "Data Storage Security in Cloud Computing" International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013
[7] Maulik Dave " Data Storage Security in Cloud Computing" Volume 3, Issue 10, October 2013 International Journal of Advanced Research in Computer Science and Software Engineering.
[8] Hyun-Suk Yu, Yvette E. Gelogo, Kyung Jung Kim. "Securing Data Storage in Cloud computing" Journal of Security Engineering 9th March 2012.
[9] B.Arun S.K.Prashanth "Cloud Computing Security Using Secret Sharing Algorithm"VCE, Hyderabad India Volume : 2 Issue : 3 March 2013.
[10] Priyanka Pareek "Cloud Computing Security from Single to MultiClouds using Secret Sharing Algorithm" International Journal of Advanced Research in Computer Engineering & Technology Volume 2, Issue 12, December 2013
[11] K.Valli Madhavi R.Tamilkodi R.BalaDinakar "Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed" International Journal of Electronics Communication and Computer Engineering Volume 3.
[12] Mohammed A. AlZain, Eric Pardede ,Ben Soh , James A. Thom. "Cloud Computing Security: From Single to Multiclouds" 2012 45th Hawaii International Conference on System Sciences.
[13] Deepanchakaravarthi Purushothaman1and Dr.Sunitha Abburu "An Approach to Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.