IJDCST @November Issue- V-1, I-7, SW-90
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Security in Multiple Codes Using Distributed Depsky System

[1] J. Madan Mohan, [2] Bandla Srinivasa Rao

[1] PG Scholar, Dept. of CSE, VRS & YRN College of Engg. & Technology, Chirala, AP.

[2] Professor & HOD, Dept. of CSE, VRS & YRN College of Engg. & Technology, Chirala, AP.

Abstract: Cloud computing holds the potential to eliminate the requirements for setting up of high-cost computing infrastructure for IT-based solutions and services that the industry uses. Cloud computing provides many benefits in terms of low cost and accessibility of data. This would allow multi-fold increase in the capacity and capabilities of the existing and new software. 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. The entire data resides over a set of networked resources, enabling the data to be accessed through virtual machines. 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. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. 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. Our work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

Keywords: Cloud Computing, IaaS, PaaS , Single Cloud.

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing includes various types of services such as: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS, where a customer makes use of a service provider's computing, storage or networking infrastructure; PaaS, where a customer leverages the provider's resources to run custom applications; SaaS, where customers use software that is run on the providers infrastructure. Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware.

Internet has been a driving force towards the various technologies that have been developed since its inception. Cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its users and providers. The advantages of using cloud computing include: a) reduced hardware and maintenance cost b) accessibility around the globe and c) flexibility and highly automated processes wherein the customer need not worry about mundane concerns like software up-gradation.

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In such an environment users need not own the infrastructure for various computing services. 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. Now a day there has been

a move towards "multiclouds", "intercloud" or "cloud-of-clouds".

Our work focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, the cloud computing users want to avoid an untrusted cloud provider. 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.

II. RELATED WORK

NIST describes that the Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Components of the Cloud Computing:

The cloud computing model consists of five characteristics, three delivery models, and four deployment models. The five characters are:

- Location-independent resource pooling
- On-demand self-service
- Rapid elasticity
- Broad network access
- Measured service

All these five characters are in the first layer of the environmental architecture.

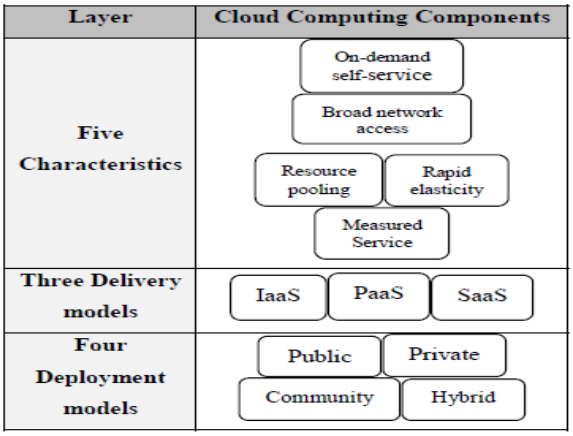

Figure 1: Cloud Environment Architecture.

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, data storage and computing services. 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. Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS. Cloud deployment models include public, private, community, and hybrid clouds. Cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud. Private cloud is available for a particular group, while a community cloud is modified for a specific group of customers. The hybrid cloud infrastructure is a composition of two or more clouds. This model represents the third layer in the cloud environment architecture. The infrastructure that is owned and managed by users is in the private cloud. The data that is accessed and controlled by trusted users is in a safe and secure private cloud. Whereas the infrastructure that is managed and controlled by the cloud service provider is in a public cloud.

Examples of the cloud service providers

Services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a cloud services provider. A cloud service can dynamically scale to meet the needs of its users and because the service provider supplies the hardware and software necessary for the service.

We can certainly apply the age-old proverb: The more things change, the more they stay the same. The raft of new technologies delivered over the past year or two has enticed many larger IT shops to launch their first private, hybrid and public clouds and served to make or break the fortunes of small and large cloud competitors alike. A few sharks -- known to us as telecommunications companies -- have seen the opportunity to enter the tank and gobble up hot

cloud services vendors. We know lists such as this invite healthy debate among readers as to who and, perhaps more importantly, who isn't named. So be sure to let us know what you think. Examples of cloud services include online data storage and backup solutions, Web-based e-mail services, hosted office suites and document collaboration services, database processing, managed technical support services and more. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure. Reliability and availability are other benefits of the public cloud, in addition to low cost.

III. Security risks in cloud computing

Security risks play a major role in the cloud computing environment although cloud service providers can offer benefits to users. Users of online data sharing or network facilities are aware of the potential loss of privacy. According to a recent IDC survey the top challenge for 74% of CIOs in relation to cloud computing is security. The protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance. Moving databases to a large data centre involves many security challenges such as privacy and control issues related to data accessed from a third party data loss or theft, accessibility vulnerability, virtualization vulnerability, confidentiality and integrity.

In [4], authors present some fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources. The security responsibility between users and providers is different in different cloud service models. According to [5] the way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. Cloud providers are more responsible for the security and privacy of application services than the users in SaaS. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. Users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others in PaaS. Users are responsible for protecting operating systems and applications in IaaS, whereas cloud providers must provide protection for the users' data.

The impact of security issues in the public cloud is greater than the impact in the private cloud. Any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. The physical infrastructure that is responsible for data processing and data storage can be affected by a security risk in the cloud environment. Resources in the cloud are accessed through the Internet; consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. Internet security problems will affect the cloud with greater risks due to valuable resources stored within the cloud and cloud vulnerability. Technology used in the cloud is similar to the technology used in the Internet. The encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. The data intrusion of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients.

Data Integrity

One of the most important issues related to cloud security risks is data integrity. Data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Example of breached data occurred in 2009 in Google Docs, which triggered the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's Cloud Computing Services. When multiple clients use cloud storage or when multiple devices are synchronized by one user, it is difficult to address the data corruption issue. Solutions that propose is to use a Byzantine fault-tolerant replication protocol within the cloud. This solution can avoid data corruption

caused by some components in the cloud. 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. Although this protocol solves the problem from a cloud storage perspective, they remain concerned about the users' view due to the fact that users trust the cloud as a single reliable domain or as a private cloud without being aware of the protection protocols used in the cloud provider's servers.

Data Intrusion

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. Hence 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. There is a possibility for the user's email to be hacked, 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. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. 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. Most of the companies seeking to protect services from such failure need measures such as backups or use of multiple providers. If a delay affects payments from users for cloud storage, the users may not be able to access their data. 45% of stored client data was lost in LinkUp as a cloud storage provider, due to a system administrator error. Data authentication which assures that the returned data is the same as the stored data is extremely important. Organizations should use HMAC technology or a digital signature to ensure data is not modified by Amazon S3. Hence, these technologies protect users from Amazon data modification and from hackers who may have obtained access to their email or stolen their password.

IV. Security in Multi cloud computing

The migration of cloud computing from single to multi-clouds to ensure the security of the user's data.

Preliminary

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were introduced. These terms suggest that cloud computing should not end with a single cloud. A cloudy sky incorporates different colors and shapes of clouds which lead to different implementations and administrative domains by using the illustration. Recent research has focused on the multi-cloud environment which control several clouds and avoids dependency on any one individual cloud. We identify two layers in the multiclouds environment:

- Inner-cloud
- Inter-cloud

Byzantine Protocol

In cloud computing, any faults in software or hardware are known as Byzantine faults that usually relate to inappropriate behavior and intrusion tolerance. Much research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction. Although BFT research has received a great deal of attention, it still suffers from the limitations of practical adoption and remains peripheral in distributed systems. The relationship between BFT and cloud computing has been investigated and many argue that in the last few years. BFT has been considered one of the major roles of the distributed system agenda. Many describe BFT as being of only "purely academic interest" for a cloud service. This lack of interest in BFT is quite different to the level of interest shown in the mechanisms for tolerating crash faults that are used in large-scale systems. BFT protocols are not suitable for single clouds. One of the limitations of BFT for the inner-cloud is that BFT requires a high level of

failure independence as do all fault-tolerant protocols. If Byzantine failure occurs to a particular node in the cloud it is reasonable to have a different operating system. Different implementation and different hardware are to ensure such failure does not spread to other nodes in the same cloud.

DepSky System: Multi-Clouds Model

A virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-clouds. 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.

a. Architecture

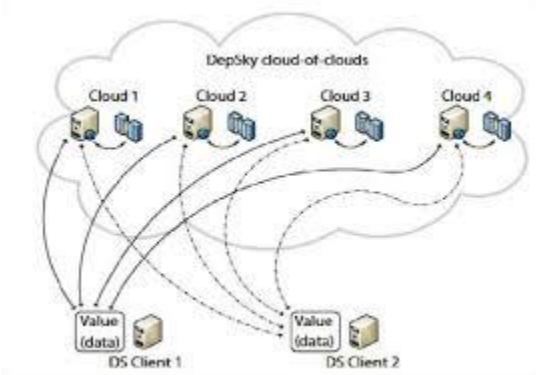

Figure 2: DepSky Architecture

It consists of four clouds and each cloud uses its own particular interface. DepSky algorithm exists in the clients' machines as a software library to communicate with each cloud as shown in the figure 2. The DepSky library permits reading and writing operations with the storage clouds.

b. Data model

As the DepSky system deals with different cloud providers, the data format is accepted by each cloud, the DepSky library deals with different cloud interface providers and consequently. The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

c. System Model

The DepSky system model contains three parts: readers, writers, and four cloud storage providers Readers can fail arbitrarily whereas, writers only fail by crashing. For example, they can fail by crashing; they can fail from time to time and then display any behavior.

Measure for security risks

In order to reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud. Using a hash function is a good solution for data integrity by keeping a short hash in local memory. In other words, authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data. If the amount of data is large, then a hash tree is the solution.

Many storage system prototypes have implemented hash tree functions. Although the previous methods allow consumers to ensure the integrity of their data which has been returned by servers, they do not guarantee that the server will answer a query without knowing what that query is and whether the data is stored correctly in the server or not. The Proofs of Retrievability (PORs) and Proofs of Data Possession (PDP) are protocols to ensure high probability for the retrieval of the user's data. Computing resources are required in this approach and not only storage in the cloud, whereas if only storage service is available by using Byzantine Disk Paxos and using at least four different clouds in order to ensure users' atomicity operations and to avoid the risk of one cloud failure. The loss of availability of service is considered one of the main limitations in cloud computing and it has been addressed by storing the data on several clouds. Loss of customer data has caused many problems for many users such as the problem that occurred in October 2009 when the contacts, photos, etc. of many users of the Sidekick service in Microsoft were lost for several days.

Data encryption is considered the solution to address the problem of the loss of privacy. All they argue that to protect the stored data from a malicious insider, users should encrypt data before it is stored in the cloud. The DepSky system stores the cryptographic keys in the cloud by using the secret sharing algorithm to hide the value of the keys from a malicious insider. Data is replicated in four commercial storage clouds is not relayed on a single cloud, this avoids the problem of the dominant cloud causing the so-called vendor lock-in issue in the DepSky system.

Storing half the amount of data in each cloud in the DepSky system is achieved by the use of erasure codes. Followed by that, exchanging data between one provider to another will result in a smaller cost. DepSky system aims to reduce the cost of using four clouds to twice the cost of using a single cloud. DepSky uses a set of Byzantine quorum system protocols in order to implement the read and write operations in the system. So it needs only two communication round trips for each operation to deal with several clouds.

Limitations

The problem of the malicious insider in the cloud infrastructure which is the base of cloud computing is considered. IaaS cloud providers provide the users with a set of virtual machines from which the user can benefit by running software on them. Traditional solution to ensure data confidentiality by data encryption is not sufficient due to the fact that the user's data needs to be manipulated in the virtual machines of cloud providers which cannot happen if the data has been encrypted.

Administrators manage the infrastructure and as they have remote access to servers then he can gain access to the user's data. Although cloud providers are aware of the malicious insider danger, they assume that they have critical solutions to alleviate the problem. The attackers outlined in their work have remote access and do not need any physical access to the servers. Another solution is to monitor all access to the servers in a cloud where the user's data is stored. This mechanism is beneficial for monitoring employee's behavior in terms of whether they are following the privacy policy of the company or not, but it is not effective because it detects the problem after it has happened.

We classified four types of attacks that can affect the confidentiality of the user's data in the cloud. It could occur when the malignant insider can determine text passwords in the memory of a VM and other confidential data. They argue that the recent research mechanisms are not good enough to consider the issue of data confidentiality and to protect data from these attacks. Some of the solutions are mechanisms and are used as part of cloud computing solutions while different types of solutions focus on solving the whole data confidentiality issue intrinsic to cloud computing. The idea of replicating data among different clouds has been applied in the single system DepSky. The limitations of this work which occurs due to the fact that DepSky is only a storage service like Amazon S3 and does not offer the IaaS cloud model. This system provides a secure storage cloud, but does not provide security of data in the IaaS cloud model. This is because it uses data encryption and stores the encrypted key in the clouds by using a secret sharing technique. Security risk issues in cloud computing have attracted much research interest in recent years. Multi–clouds can address the security issues that relate to data intrusion, service availability, data integrity in multi-clouds. Providing a cloud database system, instead of normal cloud storage is a significant goal in order to run queries and deal with databases.

V. Future Work

We aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. The framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. We want to distribute the data into three different cloud providers and we apply the secret sharing algorithm on the stored data in the cloud provider. The intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. We have used this technique in previous databases-as-a-serves research.

Hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud. If the attacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider to know the secret which is the worst case scenario. Replicating data into multi-clouds by using a multi-share technique may reduce the risk of data intrusion and increase data integrity. It will decrease the risk of the Hyper-Visor being hacked and Byzantine fault-tolerant data being stolen from the cloud provider.

VI. CONCLUSION

Cloud computing security is still considered the major issue in the cloud computing environment in the rapid increase in use of the clouds. Customers do not want to lose their private information as a result of malicious insiders in the cloud. The loss of service availability has caused many problems for a large number of customers recently. Data intrusion leads to many problems for the users of cloud computing. This work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

VII. REFERENCE

[1] Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", Hawaii International Conference on System Sciences, 45th Conference, 2012, pp. 5490-5499.

[2] (NIST), http://www.nist.gov/itl/cloud/.

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptograpy and data security,2010, pp. 136-149.

[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[5] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[6] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[7] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.

[8] I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.