ISSN 2319-2720

Volume 3, No.3, July – September 2014

International Journal of Computing, Communications and Networking

Available Online at http://warse.org/pdfs/2014/ijccn01332014.pdf

A SURVEY ON SECURED STORAGE OF DATA AND CONSEQUENT ISSUES IN CLOUD COMPUTING

T. Esther Dyana[1], S. Maheswari[2]
[1]PG Student, Nandha Engineering College (Autonomous), Erode, estherdyana20@gmail.com
[2]Associate Professor, Nandha Engineering College (Autonomous), Erode, maheswarinec@gmail.com

ABSTRACT

The term cloud is analogical to the “Internet”. The cloud is coming into sharper focus as more people adopt cloud services and gain experience that can be shared with others. As uses of cloud computing have extended, so has industry expertise in harnessing its prospective. In addition to serving as an underlying infrastructural pillar of the internet, the cloud now supports a collection of services and applications. A number of benefits are regularly mentioned by cloud providers and customers, including reduced capital costs, economies of scale, time savings, flexibility, and scalability. Yet, organizations that consider cloud computing have also expressed a number of security concerns. In multiple studies over the past years, security and privacy are commonly cited as top concerns and the advantage of moving from single cloud to multiple clouds are analyzed and the comparison table of different cloud tools is studied in this paper.

Key Words: Privacy preserving, Multicloud, Security, cloud tools.

1. INTRODUCTION

Cloud Computing is a synonym for distributed computing over a set of connections, and means the ability to run a program or application on several connected computers at the equivalent time. It can provide software, platform, infrastructure, devices and everything as a service needed by the cloud users. Cloud has public, private, hybrid, community clouds as deployment models. The customers do not possess the physical infrastructure fairly they rent the usage from a third party provider. Since the single cloud is not so efficient for multiple customers it has motivated to the multicloud environment. Although cloud computing offers many services there are also some security issues such as data privacy, integrity, recovery, accountability, malicious insiders and attacks due to the lack of knowledge of where the data- centers are located.

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. Cloud computing offers many benefits, but is vulnerable to threats. Many underlying challenges and risks in cloud computing that increase the threat of data. To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology. This paper focused on various attacks to cloud in section II and various privacy preserving mechanisms and authentication techniques and some encryption algorithms to protect the confidential data of the cloud users are discussed in section III, pros and cons of single cloud computing in section IV, advantage of moving towards multicloud computing are discussed in section V and VI, challenges in the deployment of multicloud in section VII, and in section VIII the pursue of multicloud and various tools that support cloud computing are shown.

2. ATTACKS IN CLOUD

Cloud computing have suffer from some of the following attacks and that can be explained as follows

2.1 Data theft attack- The Fog Computing is the technology used to launch disinformation attacks against the malicious insiders preventing them from distinguishing the real sensitive customer data from fake worthless data. By combining user behavior profiling and decoy technology [6] it improves detection accuracy.

2.2 Loss of Data- Data can lost due to a fire or natural disaster or data can be accidentally deleted if a provider of cloud services does not introduce right backup measures. While encrypt the data before upload them to the cloud, suddenly lost the encryption key. By using Attribute Based Encryption (ABE) and Proxy Re-Encryption(PRE) [7] the integrity and confidentiality is preserved and provide secure storage backup for sensitive data

2.3 Service Traffic Hijacking- In a cloud environment attacker could use the stolen login information to intercept, forge or give faint information to redirect users to malicious sites [15] and a two-factor authentication to reduce the risk.

2.4 Denial of Service- The cloud can be made attacks such as denial of service (DoS) and distributed DOS, which can block the cloud usage [20].For example, attackers can launch DoS-attacks on asymmetric application layer by exploiting vulnerabilities in the Web-servers, databases, or other cloud resources. Twitter suffered a devastating DoS attack during 2009.

2.5 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 [18].

2.6 Authentication attacks – Authentication is a fragile point in hosted and virtual services and is commonly targeted by the attackers to break the password by using different methods [15].

2.7 Man-in-the-middle cryptographic attacks – In this attack, the whole conversation is controlled by the attacker by placing himself between two victims and can intercept all messages [8].

These attacks should be identified and rectified at the early stage to avoid such vulnerabilities and the different kinds of attack, vulnerabilities and security solutions are discussed in [13]. The state-of-art and various security issues are discussed in [19].

3. SECURITY CONCERNS

3.1 Privacy Preserving Techniques

- **Privacy-preserving auditing protocol-** It has three phases namely Owner initialization, conformation auditing and sampling auditing [1]. These phases ensure the cloud customer that their data had stored securely on the server. And it also designed to support dynamic data updates.
- **Anonymous ID Assignment algorithm-** It is used to share private data among number of parties. It is built on top of secure sum data mining operation with Newton’s identities and Sturm’s theorem [5] to protect data and provide security in cooperative communications.
- **Robust cheating detection-** The output from authentic cloud server should be successfully verified by the customer and no output from cheating cloud server can pass the verification with non-negligible probability [2].
- **Automatic Blocker-** It is used to prevent the unauthorized data access for preserving data integrity by checking the parameters of new and existing customers and the system accepts only the validate user[11].
- **Merkle Hash Tree-** For authentication and ensuring the integrity of data storage in cloud and Bilinear aggregate signature technique for the efficient handling of multiple tasks [3].
- **Seed Block Algorithm-** It helps users to gather information from any remote location in the absence of network connectivity and also recover the files if the cloud gets destroyed. The remote data backup server ensures integrity, security and confidentiality [17].
- **Update Checker-** It improves the security of virtual machines to identify outdated packages and Online Penetration Suite scans virtual machine for software vulnerabilities [16].
- **Multi-level security-** It takes the workflow and a security requirement as input and generates as output the set of valid partitions with cost and is implemented in Haskell [14].

3.2 Privacy as a Service

PasS is a set of security protocols to ensure the privacy. It allows for the secured storage and processing of the users confidential data by leveraging tamper-proof capabilities of cryptographic coprocessor to provide a secure execution domain in computing cloud that is physically and logically protected from unauthorized access. And this is achieved by implementing data privacy mechanism and user-configurable software protection mechanism [4]. It has the following three steps:

- **Data and software transfer protocol** – executed by the cloud customer to add privacy structure to software and data before transferring them to computing cloud.
- **Software execution and Data processing protocol** – executed by the crypto coprocessor and the main server hosting the coprocessor to safely execute the customer cloud software and it ensure the privacy.
- **Privacy feedback protocol** – inform users of the different privacy mechanism applied on users data and make them aware of any data leaks or risks.

C. Encryption Techniques

- **The Homomorphic encryption and secure multiparty computation** are used by cloud servers to perform regular computation on encrypted data without access to decryption keys. [9] Uses the core of Domain-Specific Language (DSL) for secure cloud computing and secrecy preserving and to prevent control-flow leakage.
- **Ranked Searchable Symmetric encryption system** is used for the effective utilization of outsourced, encrypted cloud data and it prevent the cloud server from learning plaintext of either data files or searched keywords and is achieved by Order Preserving Symmetric Encryption Scheme(OPSE)[12].

4. PROS AND CONS OF CLOUD COMPUTING

In today's economy, companies are looking at any cost saving measures, and the bottom line is that cloud computing provides much greater flexibility than previous computing models. The advantages and disadvantages can be described as follows and it is represented in Figure 1.

A. Pros of Single Cloud

The benefits of cloud computing are many. They are listed below.

- Reduced cost since you pay as you go.
- Portability of the application is that users or employees can access information anywhere they are.
- The ability to free-up IT workers who may have been occupied performing updates, installing patches, or providing application support.
- Scaling and Cost.

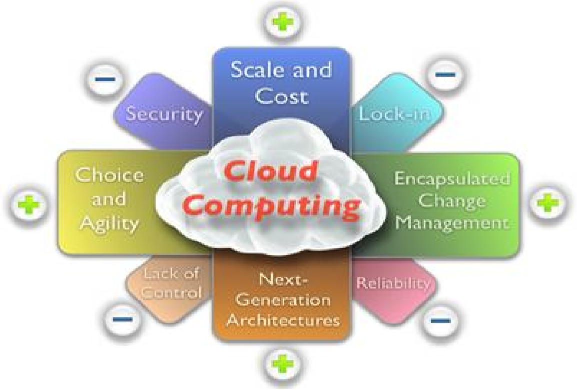

Figure 1: Pros and Cons of Cloud

B. Cons of Single Cloud

The disadvantages of using single cloud are as follows

- Inflexibility.
- Software implementations and upgrades much more difficult
- Security.
- Lower System performance.

5. TOWARDS MULTI-CLOUD

Since the evolution of cloud computing grows in importance, the advancement of multiple clouds will also become increasingly commonplace, and it is therefore very important that the applications deployed in different clouds can communicate with each other and to those of partners and customers. A multi-cloud approach is one where an enterprise uses two or more cloud services, therefore minimizing the risk of widespread data loss or outage due to a component failure in a single cloud computing environment.

The industry is moving towards a future where organizations use multiple clouds. It brings benefits such as additional infrastructure needed for fault tolerance and gives customers a choice to use clouds that are better suited than others for a particular task.

Many cloud users are using AWS [Amazon Web Services] as their starting point, and as soon as they have a handful of applications running, they start thinking about the potential of running some of those workloads elsewhere – either a private cloud or another public cloud.

Over the last year, as enterprise awareness of the cloud has increased, further many enterprises outsource their workload deployments to the cloud, in most cases to a single cloud provider or vendor.

But the market is rapidly changing with more and more options becoming available from a variety of public IaaS providers, including Amazon, HP, IBM, RackSpace as well as private offerings such as Openstack and VMware.

The novel deployment options make it possible to mix and match platforms and cloud providers, as well as to set up hybrid clouds to store some of the resources in on-premises datacenter or private cloud while migrating parts of workload to one or more public clouds.

6. BENEFITS OF MULTICLOUD

It brings benefits such as additional infrastructure necessary for fault tolerance and gives customers a choice to use clouds that are better suited than others for a particular task. Open standards are a key benefit of open source cloud computing. Open source cloud platforms such as OpenStack enable collaboration between clouds and help businesses avoid provider lock-in.

By choosing an open cloud service, businesses avoid being locked in to one technology and gain the liberty to move their data and applications between, public, private and hybrid cloud models. Rackspace has been found well suited for open standards that was cited as the main benefit of using open source cloud computing platforms.

- **Autonomy** – The ability to deploy your applications on different cloud providers has the clear advantage of reducing dependency on a single vendor. The lower level of lock-in improves the position in negotiating with vendors for better SLA and/or costs. The capability to easily exchange vendors means that you can take advantage of the most attractive offers available at any given time.
- **Integrity** – In multicloud storage, the integrity of the clients' data is maintained by Cooperative Provable Data Possession (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. The security is provided by multiprover zero-knowledge proof system and can satisfy completeness, knowledge soundness and zero-knowledge properties. And also it minimize the computation costs of clients and storage service providersby selecting optimal parameter values [10].
- **Hybridity** – Some applications are kept on-premises and others on one or more public clouds, based on a diversity of considerations, such as security, performance or cost optimization. This will provide faster service, even if the cloud customers are located in different countries. Deploying your applications on a cloud will result better response time and performance.
- **Extended capabilities** – Different cloud providers support different platforms and offer constantly changing packages of capabilities. Some features, for example, Database as a Service, might not be supported by all cloud providers. It might be a good idea to shop around, comparing the various cloud offerings to identify which providers offer the best fit for you. You might prefer to pay more for specific deployments if it means you get special capabilities, while continuing to take advantage of lower costs offered by a different provider for resources where those capabilities are not relevant.

7. DEPLOYMENT CHALLENGES

While using multicloud the cloud vendors and users have some strategies to overcome.

- **Management overhead –** Multi-cloud requires a higher level of expertise. This brings with it an increase in overall management overhead, including investments in establishing connections and monitoring. The accomplishment of different platforms requires skill in a more diverse range of subjects.
- **Interoperability** – It is to make the application set up work on different platforms and clouds. A specific tool called Ravello, can be used to achieve seamless deployment on different external cloud providers.

Managing multiple security schemas introduces complexity and risk and can require additional resources to monitor and manage. Single sign-on capabilities among disparate cloud providers may require additional third-party services or create additional complexities on developers. Security managers may incur additional overhead for enforcing security policy and meeting compliance requirements.

A. Overall complexities

- Administrate the resources across several providers for server and application monitoring, access controls and policy enforcement.
- Auditing on multiple clouds to meet requirements.
- Several contracts and business relationships should be controlled.
- The enforcement of service-level agreements should be satisfied.
- The establishment of network connections should be managed to obtain high performance and security.
- Maintenance of several network management schemas.
- Employ with numerous Application Program Interface to make integration with the applications.
- Deal with multiple charges on using multicloud.
- To monitor the cause of issues and provide alternate solutions

8. PURSUE MULTI-CLOUD

Even though there are many challenges and complexities in the deployment of multicloud computing, specifically there are two main reasons to pursue it. They are

8.1 Reduced hazards

While adopting a multi-cloud strategy, by running your cloud-based deployments on multiple cloud suppliers, redundancy may move to the next new level. By choosing information centers from completely different suppliers to host our cloud servers, we are able to effectively eliminate the danger related to the business continuity of the infrastructure supplier, furthermore as risks associated with different "data center" problems, since every cloud supplier can sometimes operate individually.

A multi-cloud approach can conjointly reduce different risks related to having one supplier: for instance somebody discovers vulnerability on the virtualization platform that the current infrastructure provider uses. It will have very little impact when this multicloud has been deployed.

The following graph - Figure 2 shows that the percentage of multi-cloud deployment of cloud customers had greatly increased with better quantity and quality in the enterprises rather than using the single cloud.

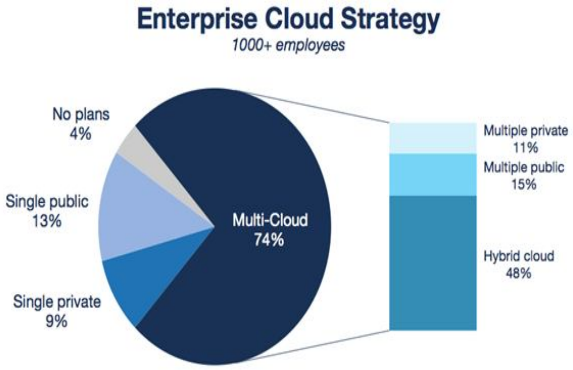

Figure 2: Single Vs Multicloud strategy

8.2 Effective control

The adoption of a multi-cloud strategy was tedious over a past few years. Cloud suppliers operated on proprietary closed architectures that created migration a headache: you would have to be compelled to effectively transfer no matter knowledge you had, make your virtual machine from scratch on another supplier, and so transfer everything back once more.

To enable the interoperability of existing corporate data centers with their own public infrastructure, cloud providers are facilitate the upload and download of complete virtual machines, so that copying your VMs from one provider to another is easier than ever. There are data migration solutions that allow you to move data from one service provider to another with no difficulty. There are even cloud-based service providers, such as Cloudability, that can manage multiple cloud providers at the same time.

On the cloud computing strategy there are significant differences between providers:

- Some will offer better support.
- Some will propose better SLA terms.
- Some will provide services at lower prices.
- Some will have improved APIs and so on.

The upcoming trends on multi-cloud computing would surely create a center of attention to both the cloud vendors and cloud users to deploy it in a secured and effective way to store and retrieve huge amount of data without any struggle. The following Table 1 shows about the comparison of different tools used under different categories.

Table 1: Comparison Table for Different Cloud Tools

S.NO	PRODUCT	COMPANY	CATEGORY	DESCRIPTION
1	Cloudability	Cloudability	Cloud Cost Analytics	Financial management tool for monitoring and analyzing all cloud expenses across an organization
2	S3 Life-Cycle Tracker, EC2 Reservation Detector, RDS Reservation Detector	Cloudyn	Cloud Optimization	To help corporate IT from over-buying Amazon cloud resources and shows detailed information on all of their virtual machine instances, databases and storage
3	AtomSphere	Dell Boomi	Cloud Integration	To integrate their various cloud based applications with each other and with on-premise applications
4	Enstratius	Enstratius	Cloud infrastructure management	Provides cross-platform cloud infrastructure management for public, private and hybrid clouds security and it have single login to manage all cloud resources
5	Informatica Cloud Spring 2013	Informatica	Cloud data integration	Long-time data integration vendor, reduces the risk of data breaches during application development and testing
6	CloudHub	MuleSoft	Cloud integration service	Open source technology to provide quick, reliable application integration without vendor lock-in
7	RightScale Cloud Management	RightScale	Cloud Management	Provides configuration, monitoring, automation, and governance of cloud computing infrastructure and applications

9. CONCLUSION

Thus the paper concludes many security issues, challenges and attacks in the cloud computing environment and addresses some of the issues with their solutions. The emergence of cloud computing greatly be a focus for most of the organizations to deploy it for the effective and secured storage of data. The latest trend in cloud computing move towards the multi-cloud deployment model for their effective access to resources, scalability, flexibility and provides users to choose their cloud that are well suited for their task. Though there are some complexities occur it can be a preferable choice to many organizations to pursue cloud computing.

REFERENCES

1. Kan Yang, Xiaohua Jia. **An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing**, IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 9, September 2013.
2. Cong Wang, Kui Ren, Jia Wang, Qian Wang. **Harnessing the Cloud for Securely Outsourcing Large –Scale Systems of Linear Equation**, IEEE Transactions on Parralel And Distributed Systems, Vol. 24, No. 6, June 2013.
3. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. **Enabling Public Auditability and Data dynamics for Storage in Cloud Computing**, IEEE Transactions on Parallel and Distributed System, Vol.22, No.5, May-2011.

4. Wassim Itani Ayman Kayssi Ali Chehab. **Privacy as a Service:Privacy-Aware Data Storage and processing in Cloud Computing Architectures**, International Conference On Dependable Autonomic And Secure Computing 2009.
5. Larry A. Dunning, and Ray Kresman, **Privacy Preserving Data Sharing with Anonymous ID Assignment**, IEEE Transactions on Information Forensics And Security, Vol. 8, No. 2, February 2013.
6. Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis. **Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud**, IEEE Symposium On Security And Privacy Works, 2012.
7. Sanjay Tiwari, Chandresh Bakliwal, Chitra Garg. **A Unique Approach to Element Management and Secure Cloud Storage Backup for Sensitive Data**, International Journal Of Engineering Research And Applications (IJERA), ISSN: 2248 9622 Feb2013
8. G. Jai Arul Jose, C. Sajeev. **Implementation of Data Security in Cloud Computing**, International Journal Of P2p Network Trends And Technology, ISSN: 2249-2615 July to Aug Issue 2011.
9. John C. Mitchell, Rahul Sharma, Deian Stefan, and Joe Zimmerman. **Information-flow control for Programming on Encrypted Data**, IEEE Computer Society, Ieee 25th Computer Security Foundations Symposium**,** 2012.
10. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, and Mengyang Yu. **Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage**, IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 12, December 2012.
11. K.Kiran Kumar, K.Padmaja, P.Radha Krishna. **Automatic protocol Blocker for Privacy-preserving public Auditing in Cloud computing,** International Journal of Computer Science And Technology(IJCST) Vol. 3, Issue 1, Spl. 5, ISSN : 2229-4333, Jan. - March 2012.
12. Cong Wang, Ning Cao, Kui Ren, Wenjing Lou. **Enabling Secure and Efficient Ranked Keyword Search over Outsourced cloud Data**, IEEE Transactions on Parallel and Distributed Systems, Vol.23, No.8, Year 2012.
13. Nitesh Shrivastava, Ganesh Kumar. **A Survey on Cost Effective Multi-Cloud Storage in Cloud Computing**, International Journal of Advanced Research in Computer Engineering and Technology, Vol. 2, Issue. 4, ISSN: 2278-1323, April 2013.
14. Paul Watson, **A Multi-level Security Model for Partitioning Workflow over Federated Clouds**, Watson Journal of Cloud Computing: Advances, Systems and Applications 2012, **1**/1/15.
15. Nelson Gonzalez, Charles Miers, Tereza Carvalho, Mats N¨aslund and Makan Pourzandi. **A Quantitative Analysis of Current Security Concerns for Cloud Computing**, Gonzalez Et Al. Journal Of Cloud Computing: Advances, Systems And Applications 2012, **1**:11.
16. Roland Schwarzkopf, Matthias Schmidt, Christian Strack, Simon Martin and Bernd Freisleben. **Increasing Virtual Machine Security in Cloud Environment**, Schwarzkopf Et Al. Journal of Cloud Computing: Advances, Systems and Applications 2012, **1**:12.
17. Kruti Sharma, Kavita R Singh. **Seed Block Algorithm: A Remote Smart Data Back-up technique for Cloud Computing**, International Conference on Communication Systems and Network Technologies 2013.
18. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen. **Security and Privacy Enhancing Multicloud Architectures**, IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.
19. Mohiuddin Ahmed1, Abu Sina Md. Raju Chowdhury2, Mustaq Ahmed3, Md. Mahmudul Hasan Rafee. **An Advanced Survey on Cloud Computing and State-of-the-art Research Issues**, International Journal Of Computer Science Issues(IJCSI), Vol. 9, Issue 1, No 1, January 2012, ISSN (Online): 1694-0814
20. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham. **Security Issues for Cloud Computing**, International Journal Of Information Security And Privacy, 4(2), 39-51, April-June 2010