Vicissitudes of Security and Privacy (Visp) in Cloud Computing: A Study on Multi-Cloud Data Sharing Issues

P.Kanimozhi, T. Aruldoss Albert Victoire

Abstract :Many computing environments have been transfigured by cloud computing with its resources performing remote data management, reliability, vendor lock in, automation etc. This exemplar swing raises a range of privacy and security issues that must be taken into concern. Bandwidth cost, Migration Issues, Data Breaches, shared technology vulnerabilities, Denial of service ,Abuse and nefarious use of cloud services, insufficient due diligence, Advanced Persistent Threats(APTs) are key challenges in cloud computing security environments. This paper studies the rampant technologies and a wide array of both earlier and contemporary projects on cloud security and privacy. Also the paper classifies data sharing challenges in multi-cloud environment.

Index terms: Cloud Security, Malicious Files, Data sharing, and Multi-cloud

I. INTRODUCTION

The momentum of cloud computing is increasing every year, demanding every IT industry to have a cloud strategy or risk losing fund. A 55% increase in net sale in 2016 of Amazon Web Services (AWS) creates a grander space for Cloud infrastructure among every industry. Comparing earlier methods of information processing, cloud computing environments provide substantial profits, such as the tools for automating reconfiguration of cloud, accumulating resources, connecting with right resources, virtualizing resources that are all in demand. These demands make every organization to deploy cloud services, which eases the process of achieving their business goals and needs.

Yet, the swing in paradigm that convoys the espousal of cloud computing is gradually giving upswing to security and privacy considerations relating to aspects of cloud computing such as multi-tenancy issues, trust, loss of control and accountability [1].

Therefore cloud systems that handle complex information are required to arrange technical methods and organizational precautions to avoid data protection collapses that might result in massive and exorbitant damages.

Revised Manuscript Received on December 22, 2018.

P.Kanimozhi, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, India, chandrankani@gmail.com.

T. Aruldoss Albert Victoire, Department of Electrical and Electronics Engineering, Anna University Regional Campus, Coimbatore,India, t.aruldoss@gmail.com

II. KEY CONCEPTS AND TECHNOLOGIES

It is real-world and cost effective to use cloud computing in the way, there can be issues with security when using systems that are not provided intramural. To mien into these and find suitable solutions, there are several key concepts and technologies that are widely used in cloud computing that need to be unstated, such as virtualization agent snapshot mechanisms, varieties of cloud services, Grid computing ,Utility computing ,Autonomic computing and “container” technologies.

A. Virtualization Agent Snapshot Mechanisms

A hypervisor or virtual machine monitor (VMM) is a key component that resides between VMs and hardware to control the virtualized resource [4]. The Snapshot Mechanism of the Virtualization is as follows:

A memory snapshot epitomizes the memory state of the profiled application at the beat it was captured. It contains information about all CPU, Memory, and about references between objects. The key benefit of snapshot is to support atomic multi-word read operations that produce a consistent view on a large dataset. With snapshot, concurrent programs read a large dataset atomically and work with a consistent process it concurrently in multithreading environment. The snapshot image is isolated from further memory updates, shared by multiple threads, and accessed with normal load/store instructions snapshot image of the dataset without synchronization code. A snapshot to read a multi-word dataset atomically and to.

B. Grid Computing

An ancestor to cloud computing, where heterogeneous resources will be collected together to achieve one common goal. The system involves large number of files for computations, which can be presumed as distributed system with non-interactive workloads. Each and every node in grid is set to perform different applications.

When compared with cluster computing, the systems in grid are loosely coupled, which are geographically disseminated. The standard used in grid computing is open one and nontrivial QoS.

Retrieval Number:F13030476S519/19©BEIESP

Published By:
BlueEyes Intelligence Engineering
& Sciences Publication

C. Utility Computing

A pay and use model, where a user gets a service only when they needed by the service provider. When compared with other on-demand computing, utility computing maximizes the resources utility and minimizes its associated cost. Utility is the bag of the computing resources such as storage and its associated services, computing and fining abilities as a hire service. This bag of computing services laid the foundation for the idea of "On Demand" Computing and Cloud Computing. Utility computing also envisaged a way to the idea of "Virtualization", where multi-server concept has been the backend of this envision.

D. Autonomic Computing

A Computing power which is used to address a complexity a problem with the help of technology to manage the technology. It is a self-managing system which solves many computation problems without the intervention of humans, which helps the IT Professional to concentrate on the business improvement. Self-managing capabilities in a system accomplish their functions by taking an appropriate action based on one or more situations that they sense in the environment. The function of any autonomic capability is a control loop that collects details from the system and acts accordingly [9]. Some of the attributes of the self-management of autonomic computing are self-configuring, self-healing and self-optimization.

E. Cner Technologiesontai

It is an OS level Virtualization technique, which is used for installing and running distributed applications deprived of commencement of an entire Virtual machine for each application. As a substitute, multiple isolated systems, called containers are run on a single control host and access a single kernel. Because containers share the same OS kernel as the host, containers can be more efficient than Virtual machine, which requires separate OS instances. Containers hold the components necessary to run the desired software such as files, environment variables and libraries [10].

III. CLOUD COMPUTING CHARACTERISTICS

Table 1, describes the various the cloud service Models with its examples and their use-cases.

Service Models	Functions	Examples	Use-Case
PaaS	Makes the development, testing ,and deployment of applications quick, simple and cost effective.[11]	Apprenda, Heroku,Force.com, Apache Stratos	Increases developer productivity and utilization rates while also decreasing an application's time to market[11]
IaaS	A self-service Model for accessing, monitoring and managing remote datacenter infrastructure, such as compute, storage, networking and networking services [11].	Amazon Web Services, Cisco Metapod, Microsoft Azure, Google compute Engine, Joyent	Extends current data center infrastructure for temporary workloads [11].
SaaS	Applications can be directly run by web browser without any installations except some plugins [11].	Cisco WebEx, Google Apps, Concur, Citrix Go To Meeting	Replacing Traditional on-Device software [11].

A. Cloud Security Challenges

Some of the areas that one can apply security features are as follows:

B. Infrastructure Security

The infrastructure security in cloud will be of three different levels;

- The Application Level Infrastructure Security (ALIS)
- The Network Level Infrastructure Security (NLIS)
- The Host Level Infrastructure Security (HLIS)

The Application Level Infrastructure Security (ALIS)

Any security program will be of crucial, when it becomes to secure the software or application developed. Still many organizations with their high secured programs yet to come out with the security in application or software level, which is the foremost one in this information era. As there are thousands of applications has been developed and deployed in cloud platform, where every IT industries are in a position to reexamine their current security practices and its standards. The continuum of application security ranges from standalone system to the multi-user system. Some of the various levels of application level security are:

- Application level security in cloud models and its types
- Cloud end-user application security

By means, the infrastructure security can be only realized with service provider provisions for providing security [15].

Identity & Access Management

Identity management concept is important in cloud computing which involves securing the identity of a cloud user.

Retrieval Number:F13030476S519/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. SECURITY FACTORS AND ITS SOLUTIONS

A. Identity Provisioning

Generally users are allowed to create an account by filling up their identities such as name, username, email-id, password etc. Based on the account creation in cloud, the user's identity will be created in some structured fashion. The system where the user creates account will be responsible for avoiding replicas, and the user will be given provision for choosing their identity, with the availability of the system. Then the trust value has become crucial in both cloud and user's perspective.

B. Cryptosystem

The identity and credentials of the user will be only maintained by the user itself or by some network administrator, which is stored in an isolated storage location. The value of the information should be highly intense in order to upsurge the strength of identity stored and the system where it is stored. The stored information should be managed by a cloud administrator as a cryptosystem, which involves cryptographic algorithms and its key for managing it.

C. Physical Communication Channel

Identity Management system will make sure that the user's identities are in encrypted form to be decrypted. The strength of the communication security will be depends on the type of encryption algorithm used.

The Host Level Infrastructure Security (HLIS)

The delivery models of Cloud computing such as IaaS, PaaS, and SaaS along with the cloud deployment models such as Public and Private should be taken into account for the assessment of cloud security and its associated risks. Practically, IaaS end users will be responsible for fortifying the hosts in the cloud computing, rather the security responsibilities in SaaS and PaaS will be taken care by the respective cloud service provider itself[14].

The Network Level Infrastructure Security (NLIS)

In the case of NLIS, it is vital for any end user or service provider to differentiate services availed in private and public clouds, in order to understand the security issues prevailed. If the user uses the private cloud, there will be less vulnerability or risks, since 74 the security topology of the cloud system has been defined based on the customers specification of the particular organization constraints. But if the user uses the public cloud, its not possible for individual to customize the topology as it will change the entire network topology, which will in turn disturbs other users in the cloud[11][12][13].

V.MULTI-CLOUD TENANCY VS SINGLE CLOUD TENANCY

Common Cloud Security Factors	Description	Example	Solutions
Authorization	A Security factor which is used to verify the user's true permissions and rights to access the requested resources.	Dialed Number Identification Service(DNIS)	-
Data Integrity	Unauthorized modification of information leads to data integrity	Data loss or manipulation, Untrusted remote server performing computation on behave of user	Third party Auditor, Provable data Possession, Proof of Retrievability, Proof of ownership[12]
Data Availability	A security factor which makes sure that the data is available for the customer at any point of time.	Back -up server, Multiple Virtual Servers	Depsky[13],HAIL[14]

A. Multi-Tenant Cloud

It is a Multi-Tenant Software as a Service Architecture, in which several corporates store their information in the same instance or platforms. The instance will be divided or partitioned that prevents the industries from accessing each other's stored information. This is like construction or making of Matki (earthen pots), where the making plans are same, but minor changes can be made to every individual pot to differentiate. Significant changes to individual pot leads to high in cost. The primary reason for any company to move to cloud is to reduce cost, which is achieved by multi-cloud computing rather than single cloud computing[18][19].

Single Plan=Many Pots
Single Architecture=Many clouds

Retrieval Number:F13030476S519/19©BEIESP

Published By:
BlueEyes Intelligence Engineering
& Sciences Publication

B. Single-Tenant Cloud

A Hosted Software as a Service (SAAS), where every company has its own cloud infrastructure and its supporting tools. Ponder like a neighborhood pots developed by same potter, where each pots has the ability to get modified as desired. By having a single hosted cloud, the buyer can twist and customize the cloud to meet their organization requirements[20].

My cloud –My Rights

Now we have reached the destination of defining exact definitions of single and multi-tenant cloud by comparing all their benefits and drawbacks in terms of real time scenarios.

- ✓ If the customer decided to have their own cloud, then the customer has to bear the cost of whole cloud deployed.
- ✓ A Multi-Tenant cloud provides cost effective solution when compared to single tenant cloud.

- ✓ A resource of single tenant cloud is not used efficiently, unless or otherwise it's fully unplugged. For each single cloud, the core software such operating system and its related libraries have to update every time to cover the exploitable codes.

C. Right Side of Multi-Tenant Cloud

- ✓ **Economy of Hardware & Power:** An ultimate benefit of Multi-tenant cloud comparable to single tenant cloud is of economical. With the nature of pooling of resources, there are some finite savings in terms of hardware and its supporting environments along with the consumption of its power.
- ✓ **Ease in Upgradation:** If the customer is using multi cloud tenancy, he/she will not be in a position to upgrade a software of cloud ,rather it's a forced and automated one, which in turn all the cloud together will be upgraded instantaneously. Simply the mediation of customers in upgradation of software will not be required[22].
- ✓ **Redundancy with Backups:** A backing up of data in a single cloud requires stringent effort as compared to the multi-tenant cloud.

Other Side of Multi-Tenant Cloud

- ✓ **Can't meet individual organizations Specific needs:** As thousands of industries run their business on same database of multi-cloud architecture, certain level of acceptance should be made for the proper usage of multi cloud environment that devoid their specific needs.

- ✓ **Automated Software Upgradation Issues:** As the software in multi-tenant cloud has been designed to be updated automatically, the concept of authorization is of question mark? As the multi-cloud runs on the same code concept, every individual cloud in a group will get updated without the knowledge of any single customers. There is also a possibility of removing several existing features of multi-cloud, which might be used by current applications of multi-cloud users, which prompts to the glitches in application that's run in cloud.

D. Right Side of Single Tenant Cloud

- ✓ **Ensures High Privacy:** Since it's a single cloud of user, there might be no possibility of eavesdropping or snooping on the information which ensures high privacy.
- ✓ Using a single tenant cloud makes sure that the business is having a unique solution as they are engaging their business in dedicated ERP.
- ✓ **Efficient Resource Management:** As the user uses single cloud and if the customers indulge in real time/intensive computing, the computations will make use of the cloud fully along with its resources
- ✓ **Efficient Resource Management:** As the user uses single cloud and if the customers indulge in real time/intensive computing, the computations will make use of the cloud fully along with its resources.

S.No	Existing Approaches	Techniques /Algorithm Used	Limitations	Possible Vulnerabilities
1	[3] Secure Multi-cloud data sharing Using Key aggregate Cryptosystem for scalable data sharing	Key aggregate Encryption	Constant decryption key size	Intrusion between classes
2	[4] Security and Privacy for Group data sharing in the Multi-cloud Node Environment	Data partitioning & Agent based Cryptography	Isolation of Physical Network	Scalable issues
3	[19] Data Security in Single and Multi-cloud Storage –an overview	Integrated approach	Data gets deleted when user unsubscribe	Contractors agreements
4	[5] Multi-cloud data security	Shamir Secret Sharing	Single point of attack	Isolated systems in a cloud
5	[6]A Secure Data sharing and communication with multiple cloud environments with Java API	Classes and object Hierarchy computation approach	Deciphering using same key	Visualized encrypted data

Retrieval Number:F13030476S519/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

6	[7] Enhanced Security for data sharing in Multi-cloud storage	File slicing with index based /SDSMC framework	Video based data	Leakage of KEY

Other Side of the Single Tenant Cloud

- ✓ **Expensive:** Owning the single cloud and its maintenance will be expensive in nature.
- ✓ Compared to Multi-tenant cloud, a single tenant cloud management will be crucial, as every updates and its cost will be abide by the single customer.
- ✓ As the cloud is not fully loaded, its resources will not be efficiently used up.

E. Data Sharing

It is a technique in cloud computing which is used to share the data of individual user of cloud in cloud easily. The cloud Service provider eases to outsource the user's data to reduce their cost. There arises problem of uncontrolled data, since the cloud is a third party provider one. The cloud user then feels the issues of security and privacy among using their data in cloud.If the user is using the single cloud, the problem of security and privacy will be of high enough, since it may not be of private cloud. What if the user is in multi-cloud? Data sharing in multi-tenant cloud is challenging one to solve, where several constraints to be considered[24][25].

Existing Data Protection Approaches in Single Cloud and Multi-Tenant Cloud

The following table exhibits the various techniques used and possible vulnerabilities along with limitations of single and multi-tenant cloud computing.

VI.CONCLUSION

This paper reveals the research direction of data sharing in the dynamic cloud i.e. a multi-tenant cloud along with various security and privacy issues in single cloud. Various techniques and algorithm for cloud security and privacy has been studied in this paper. Key concepts and the technologies discussed here comes out the need and the position of cloud computing and its security issues.

REFERENCES

1. https://www.forbes.com/sites/forbestechcouncil/2017/08/11/the-next-phase-of-the cloud-computing revolution-is here/#600c8d166a16.
2. https://blogs.sap.com/2015/07/12/multi-tenant-vs-single -tenant-architecture-saas
3. Suhas Bachhav, Chethan Choudhari, "Secure Multi-cloud data sharing Using Key aggregate Cryptosystem for scalable data sharing" International Journal of Computer Science and Information Technologies ,Vol 6 (5),2015,4479-4482.
4. Sandeep Srinivas Dwaram, Manish Yeruva ,"Security and Privacy for Group data sharing in the Multi-cloud Node Environment" International Journal of Science, Engineering and Technology Research (IJSERT), Volume 5 ,issue 3 March 2016.
5. Arun Singh,Darshan Jain "Multi-cloud data security" International Research Journal of Engineering and Technology(IRJET),Volume 3 issue 3 ,March 2016
6. Shiksha Joshi, Pallavi Jain "A Secure Data sharing and communication with multiple cloud environments with Java API" International Journal of Advanced Computer Research , Volume 2 ,Number 2 Issue 4 June 2012.
7. Dr.K.Subramanim and F.Leo John "Enhanced Security for data sharing in Multi-cloud storage(SDSMC)" International Journal of Advanced Computer Science and Applications(IJACSA),8(3),2017.http://dx.doi.org/10.14569/IJACSA.2017.080326
8. Ranjan Kumar Mondal and Debabrata Sarddar "Utilty Computing" International Journal of Grid Distribution computing ,Vol.8, No.4 ,2015,pp.115-122.
9. https://www03.ibm.com/autonomic/pdfs/AC Blueprint white Paper V7.pdf
10. searchservervirtualization.techtarget.com/definition/container-based-virtualization-operating-system-level-virtualization
11. https://apprenda.com/library/iaas-paas-saas-explained-compared/
12. Sultan Aldossary and William Allenn ,"Data security, Privacy, Availability and Integrity in cloud computing : Issues and current solutions" International journal of Advanced Computer Science and Applications ,Vol 7,No.4 2016.
13. K.D.Bowers,A.Juels and A.Opera "Hail: A High –Availability and integrity layer for cloud storage" in Proceedings of 16th ACM conference on Computers and Communications security.ACM 2009, pp.187-198
14. A.Bessani,M.Correia,B.Quaresma,F.Andre and P.sousa,"Depsky: dependable and secure storage in a cloud- of –clouds,"ACM Transactions on Storage(TOS), Vol 9 ,no.4 ,p12,2013.
15. Velev D., Zlateva P. (2011) Cloud Infrastructure Security. In: Camenisch J., Kisimov V., Dubovitskaya M. (eds) Open Research Problems in Network Security. Lecture Notes in Computer Science, vol 6555. Springer, Berlin, Heidelberg.
16. Lonea A.M., Tianfield H., Popescu D.E. (2013) Identity Management for Cloud Computing. In: Balas V., Fodor J., Várkonyi-Kóczy A. (eds) New Concepts and Applications in Soft Computing. Studies in Computational Intelligence, vol 417. Springer, Berlin, Heidelberg.
17. Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., 2009.
18. FeiLi,JingDu"Mass Data Storage and Management Solution Based on Cloud Computing" IERI Procedia Volume 2, 2012, Pages 742-747.
19. Dr.K.Subramanim and F.Leo John, "Data Security in Single and Multi Cloud Storage–An Overview" International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2016.
20. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings of the 29th Conference on Information Communications, INFOCOM'10, (Piscataway, NJ, USA), pp. 525–533, IEEE Press, 2010.
21. A. Cavoukian, The Security-Privacy Paradox: Issues, misconceptions, and Strategies.https://www.ipc.on.ca/images Resources/sec-priv.pdf, Retrieved November 2015.
22. A. Gholami, G. Svensson, E. Laure, M. Eickhoff, and G. Brasche, "Scabia: Scalable Brain Image Analysis in the Cloud," in CLOSER 2013 - Proceedings of the 3rd International Conference on Cloud Computing and Services Science, Aachen, Germany, 8-10 May, 2013, pp. 329–336, 2013.
23. S. Sharma, "Evolution of as-a-service era in cloud," CoRR, vol. abs/1507.00939, 2015.
24. S. Sharma, U. S. Tim, J. Wong, S. Gadia, "Proliferating Cloud Density through Big Data Ecosystem, Novel XCLOUDX Classification and Emergence of as-a-Service Era," 2015
25. S. Sharma, U. S. Tim, J. Wong, S. Gadia, S. Sharma, "A Brief Review on Leading Big Data Models," Data Science Journal, 13(0), 138-157. 2014.

Retrieval Number:F13030476S519/19©BEIESP

Published By:
BlueEyes Intelligence Engineering
& Sciences Publication

Retrieval Number:F13030476S519/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Retrieval Number:F13030476S519/19©BEIESP

Published By:
BlueEyes Intelligence Engineering
& Sciences Publication