STUDY OF SECURITY RISK MODEL IN CLOUD COMPUTING

Praveen Kumar Shrivastava[1], Dr. S.M.Ghosh[2]
[1]Research Scholar, [2]Professor
[1]Department of Computer Application, Dr. C.V.Raman University, Bilaspur Chhatishgarh India
[2]Department of Computer Science & Engineering, Rungta College of Engineering & Technology, Bhilai, Chhatisgarh, India

Abstract: Cloud computing is a hopeful technology to impede development of large, on-demand, flexible computing infrastructures. But without using security into inventive technology that supports cloud computing organizations are setting themselves up for a fall. The trend of adopting this technology by the businesses automatically introduced new risk on top of currently existing risk. Locating everything in a single box like cloud will only make it easier for hacker. The qualitative aspect of this research separates facts from unfounded worries, and creates a Modal that can help perceived risks of cloud computing with actual risks. Also include the several security and challenging issues, rising application and the future trends of cloud computing.

Keywords: Cloud Computing, cloud Security, cloud security risk model.

I. INTRODUCTION

Cloud computing is currently one of the most valued IT innovations. Many IT companies planning to the cloud computing prototype. Though cloud computing itself is still not yet in your prime enough, it is already apparent that its most critical flaw in security. Many corporations are allowing for moving mission-critical workloads to cloud computing. In the nearest future we can expect to see a bunch of new security exploitation events around cloud computing providers and users, which will shape the cloud computing security research guides for future. Hence, we have seen a rapid evolution of a cloud computing security discipline, with ongoing efforts to cope with the individual requirements and capabilities regarding privacy and security issues that this new paradigm raises. Clouds have created new security surfaces for attacks. Clouds built for the insatiable need to collect an ever-increasing amount of data and generating many new challenges in the area of regulatory compliance. We create a model that can help categorize and value cloud-computing risks is a significant contribution to the IT community and computing science body of knowledge. In this development, we closely look cloud computing security on a technical level, focusing primarily on attacks and hacking attempts related to cloud computing providers and systems. However cloud computing offers Huge opportunities to IT industry, development of cloud computing technology is currently at its infancy, with many issues still to be addressed We pointed out specific security threats and vulnerabilities of services and service-oriented architectures require new security criteria,. In this research paper, we try to find outs security issues that will arise from the cloud computing prototype, and we give preliminary some solution to assist in the evaluation and implementation of clouds and some improvement strategies to reduce IT risks.

II. SECURITY CONCERN

Security threats must be overcome in order to benefit fully from this new computing model. Some security concerns are pointed and discussed here:

- Businesses fells great IT challenges, and are being asked to do more with less. This has encouraged more cloud adoption to control low cost IT for Non-critical and non-confidential data.
- Storage services provided by one cloud dealer may be incompatible with another dealer's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud).
- Ensuring the integrity of the data means that it changes only in response to authorized transactions.
- Some government regulations have strict limits on what data about its citizens can be stored and for how long.
- Customers may be able to take legal action cloud service providers if their privacy rights are violated, and in any case the cloud service providers may face damage to their reputation.
- With the cloud model physical security is lost because of sharing computing resources among companies. No knowledge or control of where the resources stored and where the resources.

Vulnerabilities- VM isolation can be easily compromised and in some situation the attacker can gain full access to the host. Control of the host allows full access to confidential data available to other VMs within the physical server. One third of the vulnerabilities are located on the hypervisor software itself, but almost half of the vulnerabilities are attributed to third-party software. This underscores the need to validate and demand well-defined security test acceptance criteria.

Some risk factor is related to the issues associated with sharing the same physical IT resources like CPU, firewalls, memory, storage and other hardware components. Sometimes also associated with the sharing of software resources like backup or database. The majority of the attacks exploit common vulnerabilities associated with misconfigurations and poorly managed devices. Clouds are highly automated and complex systems have large number of computer, storage and network bandwidth has provided surface for error.

III. DELPHI RESEARCH PROCESS

The Delphi method is a popular research methodology for doctoral dissertations. The methodology is suitable for research efforts that are trying to increase the understanding of a problem and to gain experiences of early adopters of new technologies. We selected here Delphi methodology because we were interested in finding qualitative measures and tried to understand cloud computing risks by leveraging the knowledge of cloud experts and other cloud early adopters. Delphi method has been useful with research problems where there is imperfect and scarce information available.

IV. SOLUTION FOR CLOUD SECURITY RISK MODEL

Cloud Security Framework is divided into three main concepts, driven by (1) additional attack rise; (2) value attention; and, (3) huge data. The first concept, additional attack rise, is the aggregated additional software required to manage the cloud. The main factors driving the additional attack rise are: cloud administration, virtualization, virtual networks and storage, Multitenancy, endpoints, authorization and authentication.

A.CLOUD ADMINISTRATION:

The cloud administration risk factor consists of those vectors that add more software to the cloud in support of the cloud management process, APIs, and automation process. The level of maturity of cloud management software is relative low and this inevitably tends to cause vulnerabilities. Some solution strategy for cloud administration risks are –

- Use Cloud Provider recommended Configurations- To diminish the risk associated with cloud administration software it is best to follow the guidance provided by the cloud provider regarding how to use cloud resources and services. To follow the cloud provider's instructions is one of the Cloud Security recommendations in their Security Guidance for Critical Areas of Focus in Cloud Computing v2.1. Every cloud structure is different so the same procedure cannot be applied to all clouds. If possible, the managed service provided by the cloud provider should be used. Since cloud providers maintain their managed services interfaces for many customers, these interfaces be liable to be associated with standard measures.
- Backup all data - For backups and disaster recovery, a different cloud provider should be used, or, at a minimum, backups and disaster recovery sites should not be collocated with the production site.
- Automation and cloud administration- the new attack surface created by the automation and cloud administration software is a factor that is out of the control of the user. The best policy is to remain as isolated as possible from the intricacies of the cloud provider's APIs, allowing easy movement of a solution to other clouds when necessary.

B.VIRTUAL SERVICES:

Virtualization is the act of simulating IT resources on a physical host. The virtualization risk factor is divided into three types of virtualizations: virtual servers, networks, and storage. All of these refer to the ability to virtualized resources and share them across multiple tasks. Some solution strategy for virtual services risk:

- Clean regularly – Avoid extensive of VMs by removing frequently inactive VMs. This can be done by users to delete their VMs or enforcing time limitations on inactive VMs. to avoid security exposures old accounts that haven't been used in a while should be removed to avoid hackers using those accounts for malicious exploit.
- Rascal VMs – Avoid using VM images created by others. If possible, create your own company VM images, distribute those to your employees, and keep the images in a secure storage. Disable Dangerous Hyper visor commands – Mitigate the risk of hyper visors by disabling or limiting the use of commands or tools most frequently used by hackers to break into a virtualized environment. For example, the tools VMchat, VMCat, VMftp use the COM Channel in VMWare to gain access across VMs.
- Avoid Sharing Host – VMs need a secure location, a multitenant environment should be avoided, and a private cloud should be used instead.
- Secure Sensitive Data – Put additional security around your most sensitive data and confidential information. Establish a secure zone for long term storage that is encrypted and not accessible by administrators without prior authorization.
- Perform Security Audits- Make sure development processes complete regular security audits to avoid the most common attacks.
- Protect your virtual network – Several layers of switches and firewalls should be created around the network to have multiple barriers against intruders. Use network protection software for virtual networks.

C. MULTITENANCY & STANDARDIZATION FACTORS:

Multitenancy is the capability of sharing a software service and hardware resource across multiple users running independent workloads. A multitenant environment is usually characterized by a instance that is shared between many users, and it is the responsibility of the service to maintain isolation across the many tenants. Standardization procedure simplifies our support and encourages reuse. The combination of standardization and multitenancy also creates a double risk because the security of the system will only be as strong as the weakest link. In this case the weakest link tends to be high-risk images shared by high-risk tenants. Some solution strategy for Multitenancy risk.

- Penetration test –These kinds of tests can help establish a more realistic assessment of the risks associated with the cloud service.
- Avoid Shared Resources - For businesses with high confidentiality and integrity requirements for their data, it is best to avoid multitenancy environments.
- Data Encryption – Encrypting your data is a mitigation strategy shared with virtualization and other risks factors.
- Change Management Process – Since clouds change very fast—especially multitenant SaaS applications. it is very important for cloud providers and tenants to establish a well-documented change management process.
- Test early, well and often – It is well understood in the industry that the more you test your software the better quality you will have.

D. AUTHORIZATION & AUTHENTICATION FACTORS:

Authentication is the process followed by cloud provider to verify the identity of users. Authentications factors are usually based on something the user knows (e.g., password, PIN, user ID), something the user has (e.g. cell phone, smart card), and something the user is (e.g. fingerprint, hand geometry, iris, voice). Authentication works very closely with Authorization and is the process used to define what data and resources the user can have access to and what operations the user can perform on resources. Some solution for Authorization and Authentication-

- Multi -factor Authentication – Avoid single factor authentication services because these can easily be spoofed. It is very important to ensure services support multi-factor authentication.
- Distributed Authentication – To neglect the risk of getting locked into a single cloud proprietary authentication service and duplicating identities, it is best to use a distributed authentication.
- Use Challenge-Response tests – To lower the likelihood a challenge-response program like CAPTCHA should be used, which requires human intervention to analyze and produce a viable response. it will ensure that it is a human and not a machine.
- Remove Inactive or Suspicious users – Test the validity of users through data analytics, and evaluate the outliers. If a user has unusual behavior, investigate the source and this user.

E. ENDPOINTS FACTOR:

This is a very important security factor for clouds because the main interfaces to clouds are browsers, and the security of the endpoints provides the first line of defense for cloud solutions. This means the endpoints are monitored for viruses, and software is updated regularly to limit exposure to vulnerabilities.

- Use Trusted Endpoints - Establish a process to authenticate endpoints. This includes PCs, workstations, and mobile devices like phones and other smart devices.
- Device convergence – Due to the overwhelming differences between many mobile devices it is best to select a set of devices supported by your business or application. Review this list annually, or based on the lifecycle of devices in your Enterprise.
- Endpoint-Managed service – Since devices are going to be lost and stolen it is important to have an endpoint-managed service that can disable the device and delete any important information in the device as soon as the device is made available again in the Internet.

F. VALUE CONCENTRATION:

Cloud computing relies on economies of scale to provision compute services at significantly lower cost. It is also this large volume of servers that provides the elasticity characteristic of cloud computing, which makes clouds attractive to applications with unpredictable loads.

- Use System Administrators Monitoring Tools – Investigate the way a cloud provider monitors system administrators' updates to the system. Make certain that changes to the systems can be tracked to the system administrator who made the changes.
- Use a Private Clouds – If data is confidential, highly sensitive, and must remain secure at all costs, a private cloud connected to a private network.
- Use Multiple Clouds – To mitigate the risk of a possible attack or failure of a data center, never trust a single cloud location for production and disaster recovery. To slow down the risk associated with large data centers use two different clouds as for production and another for disaster recovery.
- Inspect your data center – Before moving data to a cloud mega data center, discuss with the cloud provider the possibility of inspecting the site to ensure proper procedures are implemented in the data center.

G. DATA FACTOR:

Risk associated with storing data in the clouds is that your cloud providers will have the ability to learn about you by hosting your workloads; You don't want your cloud provider to have access to your data. At the same time you don't want others to access the information you gave to your cloud provider during registration, as it may includes credit card information and other contact information you don't want publicly available. There are significant risks associated with managing huge data systems, large distributed databases and shared storage devices. Solution for huge Data:

- Private Storage for Highly Confidential Data-If you have highly confidential data, it is best to store your data in a private cloud where you don't share the storage device with other users.
- Encrypt your data – If a private cloud is not an affordable alternative and you still need to use a

cloud to store confidential information, make sure to encrypt all your data with strong encryption and manage your own encryption keys.

- Analyze your data – One of the great advantages of moving data to the clouds is to gain the ability to analyze data against different data sources.
- Define the Information required for Audits – Ensure your data is auditable and that you can get access to your data in case you need to support an audit request.
- Use the right data service for the job – Document your database requirements and evaluate the data services available from your cloud provider.

V. CONCLUSION AND FUTURE WORK

Cloud computing is the future of IT industries It helps the industries to get efficient use of their IT Hardware and Software resources at very low cost. This paper discuss about cloud computing security issues and Challenges. This paper also analyze cloud computing vulnerabilities and security threats that cloud computing faces and presented security objective that need to be achieved. Sensitive applications of a Cloud computing require high degree of security. From data obtained here, the Cloud Security Risk Framework, And the Cloud Compliance Framework, we have sufficient evidence to conclude that clouds have substantially higher risks than traditional IT in the areas of security and compliance. The future of cloud computing is really interesting, giving the way of cheap communications. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Large scale cloud computing is another challenging issue in the near future which can be already foreseen. Research found several areas that could benefit from additional research. For example, there is a wealth of additional research that should be done on how to improve cyber forensics tools and methodology in cloud environments. The dynamic aspects of clouds have created many challenges for cyber forensics practitioners, and there are not too many mitigation strategies to contain this risk vector. Since the pace of technology is very fast in the area of cloud computing, it would be interesting to do an evaluation of cloud risks in several years to show how risk vectors, identified by this research, have changed with new technologies.

REFERENCES

[1] S. Ramgovind, M. M. Eloff and E. Smith, “TheManagement of Security in Cloud Computing”, IEEE, 2010.

[2] M. S. Mimoso, “Cloud Security Alliance releases top cloud computing security threats” http://searchcloudsecurity.techtarget.com/news/1395924/Cloud-Security- Alliance-releases-top-cloud-computing-security-threats, 2010, Accessed November

[3] C. McMonigal and P. S. Levy, “Cloud Storage Usage Models and Reference Architectures”, Intel Developer Forum, San Francisco, CA, 2011.

[4] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, et al., “Cloud computing — The business perspective ”, Decision Support Systems, vol. 51, no. 1, pp. 176-189,April 2011.