A Study of Risk Management in Cloud Computing

Roshan Prabakar Raj

School of Computing, Informatics and Decision Systems Engineering
Arizona State University

Tempe, AZ

rprabaka@asu.edu

ABSTRACT

Risk Management is an integral part of any decision making process; to assess and contemplate whether a decision or a system is feasible or not can greatly reduce negative consequences of bad decisions by mitigating risks . It primarily involves three major processes: identification, assessment and prioritization of the risk involved in a process. The type of risks involving computation of data is security, integrity and availability. In particular to cloud computing, risk management can be categorically divided by its approach. We assess the various risks faced by a cloud computing system and the prioritization of risks depending on the approach and contrast their pros and cons.

1. INTRODUCTION

Distributed computing Services are presently utilized by a wide range of organizations, organizations and also singular end-clients today. It gives a chance to little entrepreneurs to saddle the figuring influence without spending extravagant measures of cash. The utilization of distributed computing assets being so high, the security, insurance and convenient accessibility of the clients' information is of most extreme significance. A size capable lump of distributed computing security includes the appraisal and administration of dangers included in the all aspects of cloud administrations. Hazard administration fundamentally means to wipe out the components that may later on end up being an impediment in accomplishing the fancied results. In the event that dangers are not surveyed and oversaw in an auspicious way then it could prompt desperate results. Without legitimate and intensive danger examination and administration, the event of an uncommon or unforeseen danger prompts disappointment of the whole operation like the administration being difficult to reach for drawn out stretches of time. We understand that hazard administration is an immense piece of guaranteeing that cloud administrations are productively conveyed to the clients, this inspires us to study Risk Management in Cloud Computing and pick up an inside and out information about the current practices in the business. Examining the different classifications of dangers and administration techniques allows us to investigate it in unequivocal subtle element, so we can separate points of interest and disservices of the current situation in the business. By examining preferences and drawbacks, we can propose where enhancements should be made and highlight the regions where gaps exist that offer ascent to open doors for getting into the framework and adventure significant data for pernicious purposes. We likewise think it is vital to look into creative ways that are still in exploratory stages and need calibrating before they can be utilized as part of the present reality.

2. OVERVIEW

Distributed computing is an administration based engineering which gives registering administrations (Software, Platform and Framework) as a utility. As a feature of our study, we focus on danger administration in distributed computing. The huge size of distributed computing opens it to various dangers and dangers from security point of view. To distinguish, maintain a strategic distance from and deal with these dangers, we perform a profound study into the different dangers and vulnerabilities of Natural Security, Information privacy, Security, Accessibility and limit impediment, and Business congruity in distributed computing. We depict contextual investigations falling under various classifications of distributed computing and how these case contemplates sway the fate of security and danger administration in distributed computing.

3. RESULTS OF STUDY

The Study was classified into five categories namely,

- Risk Management involved in Environmental Security of Cloud
- Risk management related to Data Privacy
- Risk Management for Business Continuity
- Risk Management related to Availability and Capacity Limitation
- Risk Management about Security in Cloud Computing

3.1 **Risk Management involved in Environmental Security of Cloud**

When we discuss natural dangers in distributed computing,we essentially discuss the virtual environment of cloud. There are different elements in cloud environment that can prompt a potential hazard. There can be dangers identified with secure sparing of pictures of virtual machines in a repository.There will likewise be danger included when we discuss the upkeep of the cloud environment.As a piece of this study, we have additionally alluded to a contextual investigation and have learnt how to alleviate dangers that may manifest when utilizing seller cloud environment. Likewise, we additionally consider the information security and protection assurance issues in the distributed computing environment. In addition, we additionally review security issues in various layers of distributed computing framework.

3.2 **Risk management related to Data Privacy**

Information Security is a basic segment of cloud danger administration. Safeguarding an individual's by and by identifiable data on the cloud is imperative as it is on untrusted areas far from the individual server farms. Such a domain opens it to a considerable measure of dangers from various gatherings. There are additionally distinctive procedures to deal with these dangers and they have been described.This study concentrates on a protection driven methodology of information in overseeing dangers in cloud frameworks as an outline standard, the plausibility of such a configuration, its points of interest utilizing a benchmark to assess execution lastly examine around a specific actualized model of Danger administration in distributed computing with a security administrator and security of information. The study covers in point of interest the exchange off between encryption methods, their space-time many-sided quality and the level of secrecy it offers. Notwithstanding this study shows the working of an Astute cloud track which performs Hazard Examination and a security information administration in distributed computing.

3.3 **Risk Management for Business Continuity**

Numerous organizations these days need their information to be extremely secure and accessible all the time and they all the while need to execute new innovations as well.This is an exceptionally difficult scenario.This issue can be overcome by actualizing cloud and incorporating the congruity administrations in it.Cloud processing mainly depends on equipment free virtualization technology,the organizations are permitted to rapidly go down information and the applications to the cloud.There are chiefly 2 fundamental administrations connected with the term Risk in cloud computing.The two administrations are business progression and fiasco recovery.Even in the most dire outcome imaginable, for example, Tsunami and other common calamity the association must be certain that there is no loss of information which is exceptionally critical.So, the associations execute the 2 administrations so as to secure the data.By the force of virtualization innovation we can without much of a stretch ensure that there is no misfortune.

3.4 **Risk Management related to Availability and Capacity Limitation**

Clients tend to nature of a cloud regarding how quick the administrations are and are the administrations accessible to them at whatever point required. For enterprises and little organizations, it is imperative to them the amount of limit would they be able to abuse at a given time. Hence it is essential to study dangers included in accessibility and limit impediment. Diverse administrations require distinctive limit necessities, so the dangers of a specific administration ought to be redone as indicated by the sort of prerequisite they have. A general methodology can't be intended to handle the limit impediment dangers of all distributed computing administrations. Case in point a cloud administration giving programming as an administration will require an alternate arrangement of limit parameters and stage as an administration will require an entire different set.As for accessibility, all cloud administrations should be accessible to the client at all times. On the off chance that at all there should be downtime it ought not be for broad timeframes. Additionally the downtime ought to be booked

deliberately so it happens when the administration is not utilized by a considerable measure of users. Also reinforcement frameworks ought to be conveyed quickly in times of crises in order to guarantee consumer loyalty.

3.5 **Risk Management about Security in Cloud Computing**

Security in Distributed computing is exceptionally inclined to chance subsequent to the base , stage and programming administrations are given by a 3 rd party supplier, which will be shared by different other customers,making it inclined to powerlessness hazard. We have talked about a few security dangers, investigated those dangers and oversaw them by acquainting and examining different systems with deal with those risks.Studied the primary security challenges which incorporate Verification and Personality Management,Access Control and Bookkeeping, Trust Administration and Arrangement Combination, Secure Administration, Protection and Information Insurance, Authoritative Security Administration. Broke down the Danger administration structure which is a standout amongst the most effective security evaluation apparatus to decrease dangers, vulnerabilities and security dangers. The system comprises procedures, for example, security dangers distinguishing proof, hazard examination, evaluation, relief and Dangers administration audit which are powerful for Danger investigation, recognition and administration in security in distributed computing.

4. INDIVIDUAL CONTRIBUTIONS

My research was primarily focused on risk mitigation in business continuity in cloud computing, wherein the papers I had studied were based on how business continuity plays a very crucial role in risk mitigation in cloud computing. In the worst case scenarios such as natural disaster business continuity plays a very crucial role in risk mitigation in cloud computing.The availability and security of data is a very major concern and business continuity ensures that all the risks are properly mitigated and data is secure. The implementation of Xenserver was studied which used the concepts of Virtualization technologies for ensuring business continuity in cloud computing. I learnt in detail about the topic Risk management in cloud computing and specifically business continuity in cloud computing. Finally after the study I got a very clear idea as how business continuity plays a very crucial role in mitigating risks in cloud computing

5. CONCLUSION

The danger administration highlight to handle distributer's danger is an Entrance control structure to manage VM Picture sharing. Every picture is possessed by a part. The part will concede authorization and access to different clients. There are two all around characterized authorizations: Checkin and Checkout. Checkout consent is for a client to recover and utilize the picture. On the off chance that the client rolls out any improvements to the picture and needs to store it, he will need to require the checkin authorization. Here, we have to realize that, if a picture is altered and put away as another picture, checkin authorization won't be required. The following framework talked about later will deal with it. Naturally, the entrance is set to just the proprietor and the administrator. For any operation, access is required. This will restrain unapproved access to pictures.

By performing the benchmark tests on normal DDL and DML summons, it was found that the execution punishments for read, compose and overhaul were almost in the same reach. The creation/compose exchanges had a more unfriendly impact on the execution. The space intricacy of the framework was observed to be infeasible with expanding size of information to the encryption. The
general focuses that were taken over from the benchmark trial was that the presentation of information security (encryption of information) had about no impact on the start-up time of the framework. The more prominent the info size of the framework, the more is the computational overhead of encoding the information, particularly while creation. Information relocation on the cloud must depend on encryption for protection. QoS parameters should be considered when working with Encryption in order to touch base at the right exchange off amongst execution and security.

6. REFERENCES

1. Sellami, Wael, Hatem Hadj Kacem, and Ahmed Hadj Kacem. "**Elastic multi-tenant business process based service pattern in cloud computing.** " Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. IEEE, 2014.

2. Sun, Hongjun, et al. "**Configuration and Optimization of Virtual Business in Cloud Computing Environment.**" Cloud and Green Computing (CGC), 2012 Second International Conference on. IEEE, 2012.

3. Staalinprasannah, N., and S. Suriya. "**Implementation of Xenserver to ensuring business continuity through power of virtualization for cloud computing**."Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.

4. Lins, F., et al. " **Ssc4cloud tooling: An integrated environment for the development of business processes with security requirements in the cloud.** " Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.

5. Klems, Markus, et al. "**Automating the delivery of IT Service Continuity Management through cloud service orchestration.**" Network Operations and Management Symposium (NOMS), 2010 IEEE. IEEE, 2010.

6. Kurt Hilderbrandt." **Take Business continuity in cloud**"http://www.cio.com/article/2871275/business-continuity/take-business-continuity-to-thecloud.html,2015