ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

A Novel Risk management Method for Cloud Outage

N. Aafrin Parvin*, A.R. Meaheesha Poorani, N.Deepa
School of Information Technology and Engineering, VIT University, Vellore- 632014, India.
***Corresponding author: E-Mail: aafynazer1996@gmail.com**

ABSTRACT

Cloud computing is a trend nowadays. Almost all the applications are integrated with cloud computing with some advanced features like processing of data using the remote servers on the internet. As the technology is emerging so fast, there comes the security threat. To overcome this, it is necessary to have some security features and privacy concerns. In order to minimize impact of these threats, some risk management strategies need to be followed. Various cloud providers are facing these issues. Sometimes because of cloud outages, many cloud users as well as cloud providers are affected and the cloud providers are facing loss. In this paper, we presented the various risk and risk management strategies of cloud computing and a survey of cloud outages happened in cloud service organizations.

KEY WORDS: Cloud computing, Outage, risk, cloud provide, Service, Security, Threats.

1. INTRODUCTION

Cloud computing plays a crucial role in Information technology sector. As the benefits for cloud computing is growing enormously, it becomes the basic necessity for many peoples such as individuals, government agencies, and organizations for sharing and storing information. Since cloud services becoming a current trend almost 75% of the organizations are relocating to cloud services. Remaining people are not supporting cloud because it lacks security. Many organizations were working on these measures to prevent security threats because of these poor standards, many companies are migrating from one service provider to another for better service. Though it is easy to transfer data in the cloud, it may sometimes be accompanied with data security issues. The organization must be aware of the risk that might occur in the future and should take precautions. The main goal is to secure their customers from moving to other organizations. In software engineering, risk management is defined as a process for classifying, examining and responding to risk issues that affects the projects. Proper risk management not only reduces the probability of threats but also reduces the extent of effect. Similar to this, if the proper risk management is applied in cloud computing, then it minimize the threats and also increase the cloud users.

Literature survey: A survey is done on cloud outages that happened in top cloud providers. The top cloud providers are Amazon web services, Microsoft Azure, Google Cloud platform, IBM cloud, VMware, Rackspace, Verizon and Navisite. A cloud outage means that cloud services are unavailable for some period of time. The failure may occur due to loss of power or network connectivity issues or the cloud service is offline for some maintenance purpose. When cloud outage happens in large organizations, then the organization faces customer's dissatisfaction and severe loss of cost. It becomes more critical when the organization is not having a backup. When cloud outage happens, the organization should immediately react to the failure and should take appropriate risk management strategies to get back into normal state. Normally cloud providers like Microsoft, Amazon will be having a big cloud service and millions of users will be using regularly. In such case, the organization should be pre planned and should take risk mitigation steps to reduce the downtime. On September 2015, cloud provider Amazon Web Service subjected to outage. Because of this downtime, online service like Tinder, IMDb, Airbnb and Reddit went offline. The outage longed for five hours. It experienced error in read and write operations in the Amazon DynamoDB service. On September 2016, cloud provider Microsoft Azure hit an outage in India and Europe. In many regions, the database was down and many customer complaining about different problems they faced. The outage got widened and it took more time to resolve. On March 2016, Cloud Provider Google faced outage for 20 minutes, in which semi routine update to the network was done and it hit an error. Because of this error, the network went down. However google provided an apology and promise to credit the customer with 10% to 25% of the bill. On January 2017, cloud provider IBM's Blue Mix Softlayer portal went down. The supporting pages for softlayer like Facebook and twitter lead to dead or inaccessible pages. Since IBM has faced lots of outage, this softlayer outage was resolved after sometime. On June 2009, cloud service provider Rackspace went outage for 30 minutes. Though it was a massive outage, it was not a full outage. Since one of the nine servers was affected, it was resolved. On May 2011, cloud provider VMware suffered two outage, second outage happened while recovering the first. The first outage was because of power outage and second outage was because of VMware officials who were developing a mitigation plan to prevent the first outage. On January 2015, cloud provider Verizon had a planned outage for 48hours for maintenance activity. They informed the users ahead of time. Only 10% of the users were affected by the downtime, but Verizon claimed that there won't be interrupt in user service in the future. On August 2007, cloud provider Navisite face a major outage which lasted for 72hours. This happened because of Data Transfer. These were some of the top cloud providers who experienced outages over the years. Because of lack of risk management practices, some of the companies faced a widened outage. It is better to have an early risk detection plan instead of reacting to the risk after

the occurrence of outage. The statistics of cloud outage of different cloud providers is shown in Figure 1.

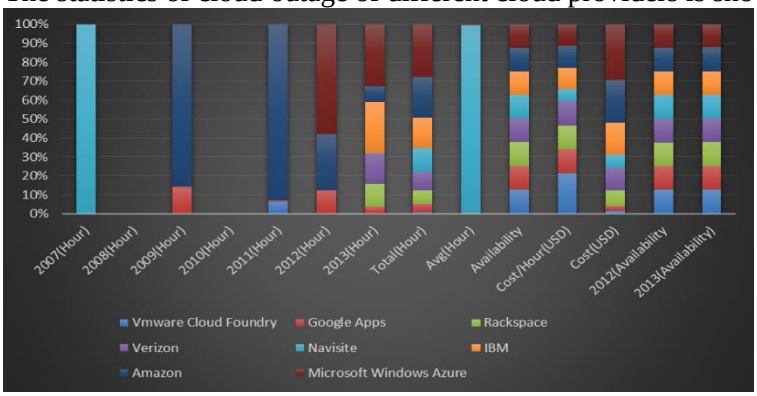

Figure.1. Statistics of Cloud outage from the year 2007-2013

Risk categories:

Loss of Knowledgeable Property: Some companies store some important data in the cloud. From the survey conducted by skyhigh, it is mentioned that 25% of files which are uploaded to cloud contains sensitive data. When the service is hacked, these sensitive data can be accessed by hackers. it is more risky when they claim ownership of the terms and conditions.

Lack of Regulatory Actions*:* Some companies have control over the information in the cloud. Even it is a government agencies, it constantly monitors the information. But these companies must have the knowledge about where the data, who is able to access it and how the data is protected.

Loss of control over Insider Threats*:* Since each and individual have their own private cloud, it is possible that they can store the confidential information about the company from company file to their private cloud. If the insider is a spy of the competitor, then there is more possibility that the confidential information is leaked to the competitor.

Malware Attacks: Cloud services can be used as path to data exfiltration which means copying or transferring an unauthorized data from the server. After analyzing, skyhigh exposed a technique named novel data exfiltration technique where hackers encode an important data into video files and upload them to YouTube. It also exfiltrates data through twitter accounts minimum 140 characters at a time.

Contract Breaking*:* Contract between the organizations and the business party does not contain information about how data is protected or who has the authority to use it. Unaware of these facts, the employee might upload the confidential document to the cloud service without approval. It is considered as leaking a confidential contract with the business party.

Loss of Customer's trust: Leakage of customer's information leads to reduce trust. For example when credit card information is leaked, cybercriminal may access it, which affects the customer and his trust on the organization and affects the company's income.

Increased Customer Awareness: When customer is aware about security threats, he will choose the organization which has high security. If he suspects that his information is not fully secured, then he will approach the company which has more security cloud services. D**ecreased Awareness among Employees:** When employees use their private cloud services, then the organization should restrict file transfer. And proper awareness about security threats should be given in order to reduce file breaching.

Peer to Peer sharing: If a work is given to an employee, he will ask help from his friend, so he will send the restricted data to a friend, which is also a form of file breaching, because it may also contain confidential information, which only restricted people have access to these information.

2. A PROPOSED RISK MANAGEMENT METHOD

The proposed risk management method (figure.2) below describes the steps taken when outage occurs in cloud service. The cloud server gives information to all the clients. It is important for the organization to have a backup server. When the cloud outage occurs, the backup server is contacted first to solve the problem. In case if the organization not having the backup server, then it is needed to check if the outage is solvable or not. If it is solvable, then apply solutions and update to cloud server and setup backup server. If the outage is not solvable, then look for the risk management database for the solutions and execute the plan and update to cloud server, in turn updated to back up server. Risk management database is filled with the test scenario along with the solutions. This is done early, in which organization need to create different scenarios based on outage or threats, and arrange a team to look after the process. Until the proper executable results arises, the steps needed to be repeated and stored in risk management database.

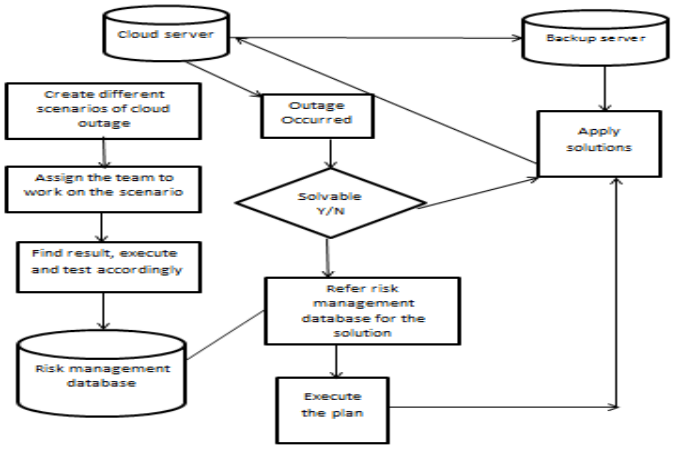

Figure.2. A Proposed Risk Management Method for Cloud Outage

Risk management solutions:

Implement Security Algorithm: Each and every organization need to have some security algorithm to provide trust to the customers. Amazon Web service implemented a formal information security program to protest confidentiality, integrity of customer's data.

Restrict unauthorized access of customer data: The organization need to know how to protect data. For that, the organization must restrict the usage of confidential information from normal employees.

Capture the usage of confidential information: When there is a need that many employees need confidential information for some purpose, then there should be a mechanism to capture who uses the data, when it is accessed, whether it is shared or not. This helps the organization to reduce insider threats.

Use Risk Management Frameworks: There are many risk frameworks available such as COBIT, IT Infrastructure Library, ISO27000x, etc. Integrating these frameworks in Cloud services provides some security features and solutions to other issues.

Choose Cloud Provider Carefully: It is necessary for the organization to have clear understanding of the potential, stability and capabilities of cloud provider.

Contact Cloud provider for Continuous service: When some interrupt happens in an organization, they can contact the cloud provider for the interrupt happened and uninterrupted service can be requested from cloud provider.

Keep Alternate Service: When the organization's cloud service depend on third party provider, it is possible that the third party services can shutdown at any time, so the organization needs to have an alternate service irrespective of whatever the interrupt occurs.

Produce Well Drafted Contract: Decide the relevant clauses of contract and negotiate accordingly. It provides some relief in an occurrence of service breakdown. The compensations for loss should be mentioned so that if the service interruption exceeded than the minutes specified, then compensation for the user must be written in contract.

Detecting Insider Threat Incidents: Violating company's cloud usage rules, creates an additional threat, because the range of severity ranges from illegal file sharing to stealing. When an insider makes multiple attempts to access a blocked file, then the insider is noted. The implementation of these features may reduce insider threat.

Have Internal Back up Options: When there is loss of Confidential file, having internal backup facility helps to recover the file. It is very harder to recover the corrupted encrypted data than unencrypted data.

3. CONCLUSION

In this paper, a formal introduction about cloud computing is described and survey on cloud outages happened in cloud providers is shown as statistics. Some of the risk that is possible due to data transfer is discussed. A risk management process for the cloud outage is described along with the diagram. And possible solutions to avoid risk are described. The risk management process describes the steps to be taken early or after the cloud outage has been occurred. In the future, this paper will be extended and the steps to implement these risk management process along with the real life scenario will be explained.

REFERENCES

Anthony Bisong, Syed Rahman M, An Overview of the Security Concerns in Enterprise Cloud Computing, International Journal of Network Security & Its Applications (IJNSA), 3 (1), 2011, 30-42.

Bernd Grobauer, Tobias Walloschek, Elamr Stocker, Understanding Cloud Computing Vulnerabilities, IEEE Security & Privacy, 9 (2), 2011, 50-57.

Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, A Taxonomy and Survey of Cloud Computing Systems, 2009 Fifth International Joint Conference on INC, IMS and IDC, 2009, 44-51.

Chiang Ku Fan, Tien-Chun Chen, The Risk Management Strategy of Applying Cloud Computing, (IJACSA) International Journal of Advanced Computer Science and Applications, 3 (9), 2012.

Cloud Provider Transparency: An Empirical Evaluation, IEEE Security & Privacy, 8 (6), 2010, 32 - 39

Farhan Bashir Shaikh, Sajjad Haider, Security threats in cloud computing, Internet Technology and Secured Transactions (ICITST), 2011 International Conference for Internet Technology and Secured Transactions, 2011, 214-219.

Hassan Takabi, James Joshi B.D, Gail-Joon Ahn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, 8 (6), 2010, 24-31.

Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, Maik Lindner, A Break in the clouds: Towards a cloud definition, ACM SIGCOMM Computer Communication Review archive, 39 (1), 2009, 50-55.

Nathalie Brender, Lliya Markov, Risk perception and risk management in cloud computing: Results from a case study of Swiss companies, International Journal of Information Management, 33 (5), 2013, 726–733

Wayne Jansen A, Cloud Hooks: Security and Privacy Issues in Cloud Computing, System Sciences (HICSS), 2011 44th Hawaii International Conference on System Sciences, 2011, 1-10.