CLOUD SECURITY BENEFITS AND RISK MANAGEMENT IN CLOUD BANKING

[1] Harjeet Singh,[2] Shwetank,[3] Thirupathi.M
[1] III B.COM,[2] III B.COM,[3] Assistant Professor
[1] Department of Commerce,
[1] Acharya Institute of Graduate Studies, Bangalore

Abstract : Cloud computing is playing a major role, providing alternative ways to access to core banking technology. Cloud computing also provides outsourcing of resources bringing economic benefits. In this report we have analysed and provided the benefits of cloud computing which is helpful to know its uses. We have furthermore described about how cloud computing helps in risk management..

IndexTerms- Cloud computing, benefits.

I. INTRODUCTION

Cloud banking is the upgraded technology upon which data can be stored instantly without any shortcomings. Core banking is a connected network of many banks having a single connected server through which transactions can be done without much obstacles. Banking technology was mostly manual until the mid-20th century, It was after the mid 20th century when the computers were brought in to automate and speed up processes. The first computer in banking was introduced in 1955.
The history of cloud computing starts way back in 1960s, when anintergalactic computer network was first suggested, and in recent years the technology has served to shake-up both the IT enterprise and supplier landscape. Over the course of the past decade, cloud computing has evolved from being something service providers told companies they should be adopting to becoming the technological lifeblood that runs through most modern enterprises.

1.1 OBJECTIVES

- To analyse the benefits of cloud banking security.
- To analyse the risk level in cloud banking.

1.2 STATEMENT OF THE PROBLEM

Why cloud security?
Cloud computing not merely provides security but also gives assurance to the user relating to their data. Most of the public are afraid of using cloud storage because of the risk factor involved, cloud security benefits help in understanding about how cloud security works and the level of security they provide.
Why risk management in cloud banking?
The common word that pops up when we hear about the cloud banking is the risk factor involved. The various risk included in cloud banking demotivates the users. Risk management becomes an essential factor which needs to be taken care of.

1.3 SCOPE OF CLOUD COMPUTING ON BANKING

Cloud computing creates an opportunity for bankers to connect with their users directly. Digital services maintain the customer relations anywhere and anytime through cloud computing. With the help of the internet, many services like storing, managing and accessing the information have become easier for both the bankers and the consumers. Cloud computing is an easy technique to deploy and integrate with all the services of the bank system which decreases the time and effort of the user.
The evolution of cloud computing enabled the banks to focus more on the customer- centric model and digitalizing the trading & wealth. Cloud computing creates a multi-channel relationship with the customer at every aspect of the service. It helps in storing, backup and recovering huge data of the company.

1.4 APPLICATIONS OF CLOUD TECHNOLOGY IN BANKING

Cloud computing increases the efficiency in the industry. Using the cloud technology is an added advantage in banking and finance sector. Digitalizing the services allows the banks and financial institution to build up an infrastructure to provide the best and appropriate services to the customer. Usually data centres go through many attacks from the hackers which corrupt and leadto loss of crucial information in the banks. Such attacks can be eliminated by authenticating the data centres which are very easy through cloud computing. Every data stored is safe with hybrid cloud computing technology.
Amazon web services and Microsoft's Azure are cloud providers who provide hybrid cloud computing servers to the companies. Hybrid cloud computing is a combination of private and public servers, in hybrid computing the most crucial data is safe and secured which are encrypted and not visible to public eye, it also includes websites which contains information which are accessible by the public. Getting the hybrid cloud computing servers provides end to end protection to the information stored in the cloud.

1.5 CLOUD SECURITY

Cloud security provides multiple levels of controls within the network infrastructure in orderto provide continuity and protection for cloud-based assets like websites and web applications. Whether in a public or private cloud, businesses need to balance DDoS protection, high availability, data security and regulatory compliance in their cloud security provider.

II BENEFITS OF CLOUD SECURITY

1. Cloud DDoS Protection

DDoS means Distributed denial of services which are now on the rise. DDoS attacks particularly occur on retail and gaming websites.In 2014 CD Networks saw a 29% increase in DDoS attack. DDoS attack utilizes vulnerable systems which are also known as zombie computers, If a DDoS attack is successful it results in shut down of the website and none of the users are able to access it which results in huge loss. "Cloud securities four step protection process starts with identifying incoming DDoS attacks, alerting website managers of the DDoS attacks and effectively absorbing DDoS traffic and dispersing it across global points of presence and provides post attack analysis.

2. High Availability

The cloud security solution offers constant support for company's assets. They provide 24x7 help in live monitoring over the company's websites and servers. Cloud security solution have a built-in protocol that ensures that your company's website and application are always on and running. It also enhances the delivery of websites content as well as application functionality on a global scale.

3. Data security

In 2014 several major data breaches at various high profile companies led the year to be nicknamed as "The Year of the Data Breach". Now in this ever increasing era of data breaches surrounding us, has resulted in, investment in access control, intrusion prevention, identify management and virus and malware protection are on the rise.

Cloud security solution which have security protocols which help protect sensitive information and transactions which are very important to users. Cloudcomputing solutions help prevent a third party to access or eavesdrop or tamper with the data which is being transmitted or the information which is highly sensitive whose misuse would cost huge losses.

4. Regulatory compliance

Some of the top financial institution and E-commerce have more industrial and government regulations than other. The top cloud security solution helps these institutions in regulating industries by maintaining and managing enhances infrastructure that supports regulatory compliance and protects customer/user's personal data.

5. Flexibility

A cloud computing solution provides us with security that is required whether you're turning up or down the capacity. The cloud computing solution will provide us flexibility which will help in avoiding server crashes during high traffic period by scaling up your cloud solution and when the high traffic is over you can scale back down to reduce cost.

6. Data loss prevention

A companies valid and critical information, if lost can cause huge losses and is a thing to be afraid off. Cloud security solution provides protected encryption to the company's data backup system and protects them against any malware as well as cyber-attacks.

7. Do more with less

With cloud computing, companies across the globe can reduces the size of their own data centres or eliminates their data centre footprints all together. The reduction in the number of servers ultimately results in reduction of software cost as well as number of staffs with fewer data centre across the world will have collectively less impact on the environment.

8. Improved collaboration

Cloud applications will give raise to much more improved collaboration by allowing different group of people to meet virtually and share their information easily as their information is well protected by cloud security solution. You can also meet each other in real time and share information via shared storage. This capability of cloud solution will reduce time and improve product application and customer service.

Cloud security solution is emerging concept which is very helpful in protection and encryption of data and transaction of various companies and concerns cloud security solution reduces high traffic which in turn helps in preventing DDoS attacks. It also helps in reduction of data centres across the globe which results in reduction of software cost as well as number of man power. The data which is storedin the cloud storage are encrypted and can not be easily accessed by the third party, thus cloud security solution is very helpful.

III EVALUATE THE CLOUD VENDOR

3.1 Risk Management

- Before engaging in partnership with any cloud vendor an organisation should request proper documentation for their own safety.
- They should investigate about the reputation as well as background of the cloud provider and learn about for how long the cloud vendor has been in the market.
- In addition, several important steps that an organization should consider addressing regulatory compliance, privacy and business continuity are detailed.

3.2 Privacy

- Data that is stored in the cloud is in a shared environment alongside with data from other customers.
- Data encryption becomes a crucial issue while protecting the confidentiality and privacy of the data both in transit and in storage.
- Also, the client should know the user access and monitoring controls, especially for privileged account.

3.3 Business Continuity Plan

- In case any disaster occurs, the organisation must have the knowledge in about what steps the cloud provider will take to protect their data and continue services.
- The organisation must also know in case of any disaster will the cloud vendor can provide complete restoration of the data and how long will it take.

3.4 A framework for evaluating cloud computing risk

- Effectiveness of controls
- Auditing and oversight
- Technical security architecture
- Data encryption
- Operations security
- Standardized procedures
- Business stability
- Intellectual property
- Contractual language

IV HOW TO MINIMIZE THE RISK IN CLOUD BANKING

- **Who access your sensitive data:**The physical logical and personnel controls that were put in place when the data was in-house company's data centre will be no longer valid when the organisation information is moved to the cloud. The cloud provider will maintain its own hiring practices rotational shifts of the individual worker, so it becomes very important to understand the hiring practices of the cloud vendor you choose. Some cloud vendors provide detailed information regarding how sensitive their data moves and who gets to see what.
- **Regulatory compliance:**The company's data after being stored on the providers cloud does not mean they are off the hook. The organisation will still be accountable to their customers for any security and integrity issues that might affect their data, they are responsible to weight the risks of their information and ensure that the cloud provider has the necessary standards and procedures in place to encounter those risks.
- **Geographical spread of your data:**The organisation or the companies should know that their data may not be residing in the same city, state for that matter the same country where the organisation resides. Even though the service provider may be contractually obliged to you for ensuring the privacy of your data, they may be even more obliged to the loss of the state or the country in which the data resides.
- **Data loss and recovery:**The data which is stored on the cloud is almost always encrypted that is to ensure the safety of the data. But, this safety comes with a price- the corrupted encrypted data is always harder to recover then the data which is not unencrypted. It is very important for the organisation to know about how the provider plans to recover their data in case of any disaster scenario and most importantly how long will it take to recover that data. The cloud provider selected by the organisation must be able to demonstrate the data recovery in disaster scenario.
- **What happens when your provider gets acquired:**The organisation before transferring or moving the data in the cloud should think about what is going to be their exit strategy and what technical issues will they be facing to get their data moved some place else. The provider that the organisation will choose should be able to clearly acknowledge an address this possible scenario in the contract.
- **Availability of data:**The cloud provider relies on a combination of network, equipment, application and storage components to provide the cloud services. If any of the above components malfunction or goes down the organisation will not be able to access the information, therefore it is important for them to understand how much work can be done by them without a certain kind of information, before the organisation decides to put the information on the cloud.

V CONCLUSION

- Applying cloud computing solutions without the proper care, due diligence and controls is bound to cause unforeseen problems.
- Used appropriately with the necessary precautions and controls inplace, cloud computing could yield a multitude of benefits, some unheard of until now and yet to be discovered,
- By being aware of the risk and other issues related to cloud computing, executives are more likely to achieve their organization's objectives as they manage the risks in this dynamic and evolving environment that likely will become the most popular computing model of the future.

REFERENCE

1. Haghighat, M, Zonouz, S, Abdel-Mottalev, M(2015), "CloudID": TrustWorthy cloud-based and Cross-EnterpriseBiometric identification.
2. Swamp computing a.k.a. cloud computing. "Web Security Journal" 2009-12-28. Retrieved 2010-01-25.
3. Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concern". Retrieved 2012-02-12.
4. "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011.Retrieved 2011-05-04.
5. "Cloud Security Front and Center". Forrester Research. 2009-11-18. Retrieved 2010-01-25.
6. "What is a CASB (Cloud Access Security Broker)?". Cipher Cloud. Retrieved 2018-08-30.
7. "Identity Management in the Cloud". Information Week. 2013-10-25. Retrieved 2013-06-05.
8. Thangasamy, Veeraiyah (2017). "Journal of Applied Technology and Innovation".
9. "Assessing Cloud Computing Agreements and Controls". WTN News. Retrieved 2010-08-22.
10. "Cloud Certification From Compliance Mandate to Competitive Differentiator".Cloudcor. Retrieved 2011-09-2