RISK MANAGEMENT IN CLOUD BANKING

[1] Parvathi Hari Kumar, [2] SonalOjha
[1] B.COM AF, [2] B.COM AF
[1] Sri Krishna Arts and Science College/ Bharathiar University, India

Abstract: Cloud computing is the delivery of computing services, like servers, storage, databases and the same over the internet, which is termed as the 'cloud' to offer faster innovation, flexible resources and economies of scale. Despite the much progress in the cloud software, banks are very much hesitated to implement the cloud. When it comes to banking organizations the cloud has quite a failure rate, that makes other banks hesitate. Here in this paper, the Risk management of cloud banking, the cloud framework, it's classifications - The deployment models and the service models, the threats faced by banks and efficient ways to prevent them as well as the risk management framework that consists of five steps which starts from planning, assessment, prioritization and treatment, mitigation and avoidance and finally controlling are discussed here. A successful framework modelling for cloud computing risk management will greatly improve the probability of cloud computing success in banking organizations.

Index Terms **- Cloud Risk Management, Deployment models, Service models, Assessment, Prioritization, Planning, Mitigation.**

I. INTRODUCTION

Banking sector is now facing many groundbreaking changes. Technology has hastened to a greater level, granting control to the customer than the bank. Banks need to react to this new customer-driven environment with innovation in business operations and information technology. Cloud Technology offers a new model for delivering effective collaboration, improved speed to market and increased efficiency. But more often a cloud project has resulted in failure, for proper research has not been as to its adverse effects, and how to control, assess or treat them. It is no new knowledge that the internet is vulnerable to multiple threats. Hence cloud based information systems, which is basically and outsource system, are exposed to threats, that can disastrously affect financial operations, assets, individuals and other organizations. Sensitive information in the wrong hands, is an assimilability that compromises the security of information stored or that is being transmitted. Risk management activities can be grouped into three categories based upon the level at which they address risk related concerns - The administrative level (tier 1), The Mission and Business Process level (tier 2), and the Information system level (tier 3). The risk management framework of a bank must be a cyclical executed process based on a set of coordinated activities, set one after another for overseeing and controlling. A remarkable process should target the augmentation of strategic and tactical security that includes the three main risk management techniques, namely, -Execution of Risk assessment, implementation of risk mitigation strategy and the employment of risk control techniques. Cloud based information system require risks be managed throughout the system development life cycle.

II THE CLOUD FRAMEWORK -

To understand the risks involved in cloud computing, the knowledge as to the types is necessary. The choice of selecting the right model and service is essential for banks. Hence, it is to be understood that the cloud is basically divided into two broad categories. The deployment model, and the service model. The deployment model is in turn divided into four categories

1.The Public Cloud
2.The Private Cloud
3. The Community Cloud
4.The Hybrid Cloud.

2.1 The Public Cloud -

The public cloud is a type of cloud that is available to everyone, where the ownership of the cloud lies with the service provider. Each tenant's data in the public cloud, however, remains isolated from other tenants. The payments are made on the resource used and for how long it has been used, but certain public cloud services may also be for free. The entire environment of the public cloud is virtualized. It is easy to implement, but the security levels are only reasonable. This type of cloud cannot be utilized by banks, however, because security is a major concern. Few examples for Public cloud services are AWS, Oracle, Google etc.

2.2 The Private Cloud -

As the name suggests, it is solely owned by a particular institution, organization or enterprise. As a private cloud is only accessible by a single organization, that organization will have the ability to control and manage it in line with their needs to achieve their goals. A private cloud model can improve the allocation of resources within an organization, in the form of data or files efficiently. It doesn't matter if the cloud service is hosted internally or externally, it still offers better security, from third parties which is more suitable for banks. It helps to hosts applications and other applications used by their customers.

2.3 The Community Cloud -

A community cloud is similar to a public cloud, except that its access is limited to specific community of cloud consumers. The community cloud maybe jointly owned by the community members. The member cloud consumers of the community typically share the responsibility for defining and the evolving the community cloud. However, membership alone does not grant all parties access to the information resource within the cloud.

2.4 The Hybrid Cloud -

The Hybrid contains the best of private and public cloud services, that remain distinct from each, but at the same time are bound together to provide benefits of multiple deployment models. It crosses the barriers of isolation and provider boundaries so that it cannot be simply defined by putting it one category; public, private or community. Hybrid solutions ensure the scalability, safety, and performance. It can also manage the vulnerabilities found in mission critical data. In this form of cloud service, employees can access business critical applications and information to improve collaboration, and the rest of the information can be accessed by the customers. It serves to act as a more personalized approach, and is also suitable for banks.

III SECOND SECTION OF SERVICE RELATED CLASSIFICATIONS

1.Infrastructure as A Service

2.Platform as A Service

3. Software as A Service

3.1 Infrastructure as a Service-

It is a self-service code that aims to manage and monitor remote data center infrastructure for the following functions - Compute, Storage and Networking. The client shall decide on the operating system of his choice. They scale and spin virtual machines of their choice. The responsibility of providing initial provisioning of a system falls on the hands of the vendor. They supply these resources on-demand from their large pools of equipment installed in data centers. It provides all institutions with mostly everything related to computing resources including networks, servers, virtualizations, and storage and data center space. Cloud providers bill the IaaS (Infrastructure as a Service) services based on a utility computing basis - cost reflects the amount of resources allocated and consumed.

3.3 Platform as a Service -

This type of environment provides clients with a platform. A platform that supports everything required to complete the life cycle of building web-based applications or providing cloud applications without the difficulty and cost of managing hardware and software. The company is allowed to write application and pilot test them. It provides all operational and development environments for launch for applications. Also, PaaS consumers do not manage or control the underlying cloud infrastructure like servers, operating systems or storage, but only have control over deployed applications.

3.4 Software as a Service -

It is one of the commonly used cloud models. It is platform independent, and is mostly based on Pay Per Use of Application to users. It makes Cloud Computing cheap. All the resources are managed by the vendor. Also, additionally, the security of the services is all on the hands of the vendor as the customer has limited control. The applications hosted centrally, updates can be released without the need for consumers to install new software.

IV RISKS IN CLOUD BANKING -

Stringent levels of security are vital at banks more than ever before. The need to protect customer data, is their most vital task. Because, banks cannot survive without the trust of the customers. A few risks when it comes to cloud banking are as follows.

4.1 DATA BREACHES -

Cyber- criminals always find new ways to manipulate their way around the internet. Although cloud storage providers implement meticulous security measures, the same threats that impact traditional storage networks can also threaten the cloud network. Through a data breach, several sensitive customer information, intellectual property, can all be exposed. The loss that this would cause banks is unimaginable. While certain cloud services usually have several security protocols, banks must formulate a plan for protecting data in the cloud. The most efficient method is to use encryption and multi -factor authentication.

4.2 INSECURE API's -

Most cloud services and applications use Application Programming Interface, otherwise known as API's to communicate with other cloud services. As a result, the security of the API's themselves has a direct effect on the security of the cloud services. The chances of getting hacked increases if banks grant third parties' access to APIs. Banks may lose important client confidential data, and other financial plans. The best way to protect a bank from API hacks is to implement threat modeling applications and systems into the development life cycle. Also, they should make sure that the security codes are reviewed and updated from time to time.

4.3 MALICIOUS INSIDERS

If one exists inside the giant cloud organizations, the hazards are magnified. One tactic bank can use to protect themselves is to keep their encryption keys on the premises, not in the cloud. If the keys are not kept with the customer and are available only at data-usage time, the system can fall prey to a malicious insider attack. Systems that are solely independent on the cloud network are subject to greater risk.

4.4 WEAK AUTHENTICATION AND IDENTITY MANAGEMENT

A lack of proper authentication and identity management is responsible for data breaches. Often there is a struggle to allocate permissions appropriate to every user's job role. A faulty identity management can leave gaping holes. Two factor and Multi factor authentication systems, one-time passwords and phone-based authentication protect cloud services from hackers, who will find it hard to hack using stolen passwords. This is a measure that every bank should take to ensure complete security of its customer and its financial policies.

4.5 ABUSING CLOUD - INFRASTRUCTURE -

The cloud brings large scale, elastic services to both banks and hackers alike. Using limited hardware, may take hackers ages to crack encryption, but using an array of cloud services, he can serve malware and launch attacks like DOS (Denial of Service.) The responsibility for the users of cloud services rests with service providers, but it may be impossible for them to detect malicious users. The customers of the cloud service, in this case banks will need to assess service provider behavior.

4.6 DENIAL OF SERVICE-

Denial of service attacks are an old tactic, but remain a threat nevertheless. The attacks assault thousands of automatic requests for service. When a denial of service attacks occurs, hackers these days are conducting assault in such a way that it becomes hard to detect which parts of the incoming traffic are the hackers and which parts are legitimate users. When it attacks a customer's service in the cloud, it disables the service without shutting it down, which is like being caught in a rush hour traffic, where it is difficult to reach their destination. But the customer will still be billed for the resources.

4.7 DATA LOSS -

In the cloud Data Loss occurs when the owner of the encrypted key loses the key to unlock the encryption. Though some say that the chances of losing data in the cloud are minimal, hackers may gain access to cloud data centers and will wipe all data clean. That's why banks must distribute all its information and application across several zones and back data using off site storage if possible. When such security measures are not followed by a bank, customers lose the most important characteristic that a bank needs, which happens to be trust. Customers will move to other banks, or other safer investment options which will result in lower revenue for the banks.

4.8 RISK MANAGEMENT FRAMEWORK IN CLOUD BANKING

Risk is often regarded as the potential that an outcome, will differ from the expected outcome. Cloud providers develop cloud architectures and provide cloud services that include various functionalities and features, as well as incorporating security and privacy controls that meet the requirements of that particular institution. Therefore, this is a major responsibility in their hand, and the choice of right cloud provider becomes a necessary factor.

Organizations are more comfortable accepting rick, when they feel that they are in control of the process and the equipment involved. To preserve the security level of their information system and data in a cloud-based solution, banks need the ability to identify all cloud specific risk, adjusted security and privacy controls in advance, which is done in the following steps.

V CLOUD RISK PLANNING -

Risk is inherent with any project, and the same holds for the cloud. While considering to bring the cloud structure into the banking organization, the banks must break down the software structure, understand what suits the organizational structure, and the measures they can implement to protect this software should an unforeseen attack arise. To implement security, banks must know the risks that will attack this virtualized environment. This is called the identification of the risk factor. Only when this done and understood will the banks be able to move to further assessment and evaluation.

5.1 CLOUD RISK ASSESSMENT -

To put it in simple terms it is the analyzing of cloud environment to identify its potential short comings. It combines exposure and data to analyze the adverse occurrences, and plot necessary measures. The techniques for analyzation include, performance models, network analysis, statistical decision analysis and quality fact analysis. It involves systematic research of random scenarios, including the failure and success rates to further determine the risks. This information can be helpful to the managers and they can compare them, accordingly. Once the analyzation and evaluation are done, the selection of a perfect architecture, alone with security and privacy implementation should take place.

5.2 CLOUD RISK PRIORITIZATION AND TREATMENT -

After risk analysis, a number of risks appear to be of similar ranking or severity. When there are too many risks of equal importance, a method is needed to prioritize these risks. When it comes to the cloud the software risks must be categorized, and proper strategies to overcome these risks must be carried out. The degree of risk depends on two properties, the probability of the risk and the degree of impact on the software project if it works., when the treatment is in place. As for the treatment strategies, they are formulated, bringing together several strategies and ideas. Out of these ideas and strategies, one which will serve as an efficient barrier to these risks, in accordance with the cloud environment chosen by the bank is selected. Steps like information authorization in the cloud, and implementation of security software in the cloud to prevent threats like DOS are taken here.

5.3 CLOUD RISK MTIGATION AND AVOIDANCE -

The concept of mitigation is one were, should, any unforeseen risk arises, the security measures taken after the evaluation, prioritization, treatment, should be able to reduce the impact of the attack, saving the banks from a huge loss of data. As for the avoidance of risk, means, taking steps to ensure that the potential risk capacity is brought to zero, using different types of processes like XML encryption, proper authorization and by being careful about access being granted to the third party.

5.4 CLOUD RISK CONTROLLING -

Risks are better controlled, with proper acceptance of the attacks, and when the shortcomings that lead to the attack are analyzed. The risk controlling happens when only there is effectiveness in the strategies implemented. Different strategies for different levels of risk should be implemented. Aside from the framework of strategies, a contingency plan should a major risk hit, must be put in place. This helps to mitigate risk. However, Banks cannot always avoid risk. It can only be controlled through cloud development or updation projects.

VI CONCLUSION -

Financial enterprises are responsible for managing an immense volume of highly sensitive data. Information like high net-worth individual's financial statements or social security numbers, offer an extremely great opportunities for cyber-criminals. We've seen above in this paper the models of the cloud and its classifications, and also how choosing the right deployment model or service model is necessary for a bank. The necessary framework of risk management needed to mitigate and control the security issues by using artificial neural network algorithms and optimal techniques. Furthermore, successful framework modeling for cloud computing risk management will greatly improve the probability of cloud computing success in banks for protecting the customer's valuable information. The risks that come with cloud banking have also been discussed, and the efficient measures used to avoid them. However, it still remains that the data in the cloud may not always be safe. Though it is of the rarest situation, there will always be some loop hole that will be sighted by the cyber-criminals, especially if the security is weak. The only way to protect this information ultimately comes down to development, and that too continuous development.

REFERENCE

[1] A survey of issues in cloud computing D.Vasuyadav , Dr.V.Krishna Reddy.
[2] "Cloud Computing: Issues and Challenges", Tharam Dillon Chen Wu and Elizabeth Chang, IEEE 2010.
[3] A new conceptual framework modelling for cloud computing risk management in banking organizations Abdelrafe Elzamly, Burairah Hussin, Samy Abu Naser, Khalid Khanfar,Mohamed Doheir, and Ali Selamat , and Abdullah Rashed
[4] "Security Issues to Cloud Computing" Cyril Onwubiko, Springer
[5] https://www.ibm.com/blogs/cloud-computing-threats.