Research Approaches for Cloud Bank Risks Identification, Mitigation, and Coping

Mohammad Nashir Uddin, Prof. Li Tong, Prof. Li Hao
Yunnan University, Kunming, Yunnan, China

Abstract**—**Cloud computing is a distributed system that enabled on-demand access of dynamically configurable resources and managed with minimal effort or interaction. The cloud bank model inspired from real commercial bank model where cloud computing environment is classified into Cloud Resource Providers (CRP), the Cloud Bank (CB), and Cloud Resource Consumers (CRC) roles. CRP play the role as depositors where CRC play borrowers role and the cloud bank plays the role as a bank where transaction take place at commercial banks. CRP are distributed physically that creating uncertainties that can affect the reliability of the cloud bank. Other direct or indirect circumstances may cause risks for the cloud bank. So accessing the cloud bank risk identification method, mitigation, and coping strategy is an important part of the cloud bank model. Even though the cloud bank deal with intangible property unlike a real commercial bank but this paper will prove that it was worth to examine commercial banks' risk identification, mitigation, and coping methods to find possible solutions to make cloud bank environments reliable.

Keywords- *Distributed resources, hybrid cloud computing, risks identification, cloud bank reliability.*

*****

1. Introduction:

Cloud bank model is a new virtual infrastructure resource management model. Cloud bank is based on commercial bank operation and laws of the market, have the different roles in cloud computing deals respectively defined as cloud resource providers, consumers, and the cloud bank, which come from one or more different cloud (private cloud , public cloud or community cloud), under the premise that retain their own characteristics, framework by standardized or proprietary technology to bind together to form the overall, so that the best interests of all parties involved to get, a hybrid cloud architecture. The resource transaction management model is mainly divided into the following five layers: physical resource pool, service level agreement (SLA) pool, risk resistance, resource scheduling, pricing strategy [[1]]. There are many risks hidden in the process of resource transactions and the damages caused by these risks directly affect the quality of service (QoS) in cloud computing. Therefore, risk against is the most important part in cloud computing. [[2]]

2. Background study:

Developed from the commercial bank, the Cloud Bank Model [[3]] is a cloud resource management modeling based on economic principles. In this model, the resources are provided as service by the providers through the network and cloud bank provides services to the consumers. As mentioned above, there are risks hidden in the process of the resource transactions among the providers, cloud bank, and consumers, so how to assure the consumers get the services and the resource providers achieve their service promises is the most important issue in Cloud Bank Model. In [[4]] and [[5]] references, there are some research about risk against in cloud bank, but these two papers just give some strategies.

In the reference [[6]] examined emerging threats in cloud computing within a financial services organization. This includes consideration of insider threats, data leakage, insecure software, and new Cloud attack patterns. The nature and characteristics of the threats are explained and the paper explores the risk treatment options chosen by the sample organization. The authors' observations are synthesized in a general model that describes Cloud Risks and Controls for financial services institutions.

A cloud computing risk assessment framework has been proposed. Using the framework, analyze three different types attack including the damage value and the restored value of the cloud system, and then, get a payoff matrix. Based on the payoff matrix, the probabilities of attacker and defender have been computed. In the specific calculation process, assume that the system cost *CR D* and the penalty for an attacker when the defender repair the system are the linear function of the recovery value and the system damage value correspondingly [[7]].

In the reference [[8]] paper analyzed the resource management in cloud computing environment and delivered an economics principal-based cloud computing model. On basis of resource risk in cloud bank model and commercial bank risk management methods, this paper delivered a cloud resource management prediction method, which has solved a bottleneck problem in for the cloud bank model.

3 The Risks Identification and Classification:

To understand the cloud banking risk, it is necessary to understand different types of risk in a commercial bank. According to 'market realist' [[9]], there are eight types of bank risks: (Major risks: credit risk, market risk, operational risk),(other significant risks: liquidity risk, business risk, reputational risk), (unrelated risk: systemic risk, and moral hazard). It is worth to have a look at real commercial bank risks to identify possible risks in cloud bank environment:

3.1 Credit risk:

3.1.1 (Commercial bank) The default usually occurs because of inadequate income or business failure. Sometimes default may occur because of borrowers' unwillingness to pay back. Credit risk signifies a decline in the credit assets' value before default arises from the deterioration of an individual's credits quality. The loss of the credits asset's value also may cause of credit loss. A net charge-off is a difference between the amounts of a loan gone bad minus any recovery on the loan. An unpaid is a risk of doing the business.

3.1.2 (Cloud bank) In the cloud banking, a consumer can not cause credit risk because a consumer cannot get any physical resource. Credit risk arises from for non-performance by a resource provider [[8]]. Since the environment of cloud computing is dynamic, so a failure by the providers to provide resources during or according to contract in specific time duration that might affect the service provision which may cause a penalty to the resource providers for wasting consumers' time too.

3.2 Market risk:

3.2.1 (Commercial bank) Market risk is the most prominent for banks present in investment banking. The major components of market risk include interest rate risk, equity risk, foreign exchange risk, commodity risk.

3.2.1.1 Interest rate risk: It is the potential loss due to movement of interest rates. This risk arises because a bank's assets usually have a significantly longer maturity than its liabilities. Management of interest risk is also called Asset-Liability Management (ALM).

3.2.1.2 Equity risk: It is the potential loss due to an adverse change in the stock price. Banks usually accept equity as collateral for loans and purchases stakes in other companies as investment from their free or investible cash. Any negative change in stock price either leads to loss or reduction of investment value.

3.2.1.3 Foreign exchange risk: Exchange rate fluctuation may cause a potential loss due to change in the value of the bank's assets or liabilities. A sudden diminish the value of the currency may cause a loss of the bank since banks always transact in foreign exchange for their customer or for the banks' own account.

3.2.1.4 Commodity risk: The changes of commodity prices cause potential loss and the commodities include agriculture, industrial commodities, and energy commodities. Since commodities' value fluctuates due to demand and supply, a bank can be in commodity risk if holding them as part of an investment.

3.2.2 (Cloud bank) Market risk will vary on cloud banks' investment sectors and strategies. But foreign exchange risk will take place once there will be an issue to receive and pay up in different currencies.

3.3 Operational risk:

3.3.1 (Commercial bank) Operational risk takes place day to day operation activities. This risk arises almost all the department such as credit, investment, treasury, and IT. This risk may cause by incompetency or wrong posting of personnel and misuse of power, failure of the IT system, and process related error (error in information processing, data transmission, data retrieval, inaccuracy of result or output).

3.3.2 (Cloud bank) The cloud bank's operational risk happen when the internal operational management and operational mechanism fails.

3.4 Liquidity Risk:

3.4.1 (Commercial bank) For a commercial bank, liquidity risk is not to be able to have enough cash to carry out day to day operations. Liquidity refers to a bank have ability to meet payment obligations and has enough cash to give loans.

.4.2 (Cloud bank) Liquidity risk arises when the cloud bank unable to provide services because of lack of resources. Liquidity risk can cause for the following reasons: when the contract expires with the resource providers, the resource providers bridge the contract and withdraw resources when resources are rented, resource pool doesn't have enough resources to replace removed or withdrawn resources. The quality of service decreases if the cloud bank cannot supply according to demand.

3.5 Reutational risk:

3.5.1 (Commercial bank) Reputational risk arises when the risk of damage to a bank's image and public standing due to doubtable actions taken by the bank. Reputational risk can cause by negative publicity against the bank too. Reputational risk leads to the public's loss of confidence in a bank that lead to a financial digester.

3.5.2 (Cloud bank) The reputational risk in a cloud bank has very similar impact as a commercial bank. Once there is an imbalance of supply and demand in a cloud bank then the quality of service decrease which leads to customers' dissatisfaction. And customers' dissatisfaction leads to reputational risk. Reputational risk also may cause the failure of IT system which may bring dissatisfactory issues towards resource providers and resource consumers.

3.6 Business risk:

3.6.1 (Commercial bank) Usually, the business risk arises from a bank's long-term business strategy because bank always needs to keep up with challenges that are changing dynamically. Business risk also arises if the bank chooses the wrong strategy which might lead to its failure.

3.6.2 (Cloud bank) Cloud bank will face business risk which is very similar to a commercial bank. Cloud bank will have to deal with challenges too like making wrong products for the consumers may lead to business risk.

3.7 Systemic risk:

3.7.1 (Commercial bank) According to 'Market Realist' systemic risk is quite unrelated that can arise from surrounding environment changes, crisis, natural disaster etc. Once changes effect targeted bank customers, bank's regular transactions get affected too which is called systemic risk.

3.7.2 (Cloud bank) Systemic risk also can arise in cloud banking since resource providers and resource consumers are venerable to get affected by environment changes, crisis, natural disaster etc.

3.8 Moral hazard:

3.8.1 (Commercial bank) Economist describes that moral hazard arise when one person to make a big decision with high risk and someone else to pay the price. Moral hazard refers to the situation where a person, a group or an organization to have a tendency to take the high risk if even it's economically unsound. Usually, boards of directors are there to watch over the decision makers and directors step in the situation when necessary.

3.8.2 (Cloud bank) Moral hazard is applicable to cloud bank since there will be always someone to make important decisions.

Market Realist also mentioned about other minor risks like legal risk, country risk where legal risk can an issue for a bank when financial risk arising from legal suits filed against the bank or by a bank for applying a law wrong way. On the other hand, cloud bank also can count loss for creating and applying privacy and policies wrongly.

4 The Risks Mitigation and Coping:

4.1 (Commercial bank) In many instances, the institution will eliminate or mitigate the financial risk associated with a transaction by proper business practices. In others, it will shift the risk to other parties through a combination of pricing and product design. There are three types of risks that all financial institutions can be segmented from the management perspective:

1. Risks can be eliminated or avoided by simple business practices.

2. Risks can be transferred to other participants.

3. Risks must be actively managed at the firm level.

Common risk-avoidance practices here include at least three types of actions.

1. The standardization of process,
2. contracts, and
3. Procedures to prevent inefficient or incorrect financial decisions ,

Some risks can be eliminated or reduced through the technique of transfer risks. Interest rate products such as swaps or other derivatives can transfer interest rate risk. Borrowing terms can be altered to effect a change in their duration. the bank can buy or sell financial claims to diversify or concentrate the risks that result from servicing its client base. There are still some risks should be absorbed at the bank level. These risks should be monitored and managed efficiently by the institution [[10]].

4.2 (Cloud bank) The cloud bank has its own features which are different from the commercial bank but uncertainties are similar to the cloud bank model. There are two major features to be focused on cloud bank which is related to credit risk:

1. Unchanged ownership of the resources
2. The consumer's unclear resource requirements

The Cloud Bank model is an open public cloud computing model. The resources and ownership are physically distributed on the Internet [[11]].

Real cloud computing applications are very complex and commercial. Even the experts in this area cannot give a clear and precise resource requirement about an application, so it is possible that a consumer wants to change the resource requirements when the contract expires. The change of the resource requirements might cause risk, such as when a consumer wants to renew the contract, but the resources should be given back to the providers. In order not to aggrieve the consumer's benefits, the Cloud Bank could only renew the contract. Then, because of the unchanged ownership of the resources, the Cloud Bank should search for other resources to provide to the consumer. If the search result failed, the credit of the Cloud Bank would be affected.

There is one significant feature about the damage of risk in Cloud Bank that should be emphasized: fast and irreparable damage without any cushioning. As mentioned above, cloud computing applications are commercial, so keeping the applications running continuously is very important. If a risk arises and an application stops running, the damage will be caused immediately and irreparably. There are no equivalents in Cloud Banking to mortgages in commercial banks, which provide some cushioning when risks arise. Therefore, early risks identification, prediction based on risks classification is the best practice for early risks mitigation.

5 Summary and Future Work:

Cloud computing environment is distributed and dynamic. But there are lots uncertainties that can lead to various risks in the resource transactions. So, risks identification is very important to prevent cloud bank from risks. This paper took commercial bank's risks classifications as a model to identify cloud bank's risks even though a major risk like credit risk can not take place in cloud bank as a commercial bank as this paper described in the body section. This paper also explained why it was worthy to examine commercial bank's risks classifications risk identification, mitigation, and coping methods.

However, there are still some risks yet to be solved, such as liquidity risk that helps the quality of cloud bank service decreases if the cloud bank cannot supply according to demand. Liquidity risk to be emphasized in future research to make cloud bank more reliable to the service consumers and resource providers.

References**:**

[1] Hao Li, Shuwei Jia, Fan Yang, Renxiang Wang. Cloud Bank Model Based on AHP Resource Scheduling Strategy Research (journal)

[2] Mojun Su, Hao Li, Shenglin Yang, Joan Lu. A Service Level Agreement for the Resource Transaction Risk based on Cloud Bank Model (journal)

[3] Huixi Li, Hao Li. A Research of Resource Provider-Oriented Pricing Mechanism Based on Game Theory in Cloud Bank Model, IEEE, (journal)

[4] Hao Li, Mojun Su. A Research of the Prediction of the Liquidity Risk in Cloud Computing. (journal)

[5] Hao Li, Miao Xin. Multiple Linear Regression-based Cloud Resource Risk Prediction, IEEE, International Workshop on Information and Electronics Engineering (IWIEE2012), 2012. (journal)

[6] Paul Rohmeyer, Tal Ben-Zvi. Managing Cloud Computing Risks in Financial Services Institutions
2015 Proceedings of PICMET '15: Management of the Technology Age Stevens Institute of Technology, Howe School of Technology Management, Hoboken, New Jersey, USA

[7] Yuxia Sun, Zhi Li, Wu Chaoxia. Cloud Computing Risk Assessment Method Based on Game Theory

[8] Hao Li , Miao Xin. An Approach for Cloud Resource Risk Prediction International Workshop on Information and Electronics Engineering (IWIEE) 2012

[9] Saul Perez. Overview: What you need to know about banking risks Market Realist | Sep 1, 2014 11:37 am EDT

[10] Douglas W. Diamond and Raghuram G. Rajan, Liquidity Risk, Liquidity Creation and Financial Fragility: A Theory of Banking, National Bureau of Economic Research Working Paper No.7430, Cambridge MA 02138, December 1999.

[11] Rajkumar Buyya. Economic-based distributed resource management and scheduling for Grid computing, Thesis.2002, Monash University.