RiskManagement in CloudAdoption: Issues, Strategies and Mitigation

Nisha
Mater of Computer Applications
Ansal University
Gurgaon, India

Vijaya Lakshmi Singh
School of Engineering and Technology
Ansal University
Gurgaon, India

***ABSTRACT*--- This paper presents risk management while cloud adoption. It explains risk from cloud provider's perspective as well as from cloud customer perspective. Before adopting any cloud it tells about the issues which need to be clarified.While using the cloud service it also tells about risk identification and after this it explains the risk assessment process and develop assessment criteria.In this review paper there are strategies to address risks in cloud environment. Risk mitigation is also involved to mitigate the all type of risk in cloud computing while using the cloud service.**

Keywords--- Cloud Computing management, Cloud Risks, Strategies, Assessment process strategies and Risk mitigation.

I. INTRODUCTION

Cloud computing providing the best computing paradigm from the last few years [1].Organizations doing their all work by replacing traditional computer system and provide with cloud computing services.Increasing popularity of cloud computing will become the bright future of IT(Information Technology)[2].Cloud computing as "a model for enabling suitable, on-demand network access to a shared pool of configuration computing resources that can be rapidly provisioned and free with minimum management effort or service provider interaction" defines by NIST (National Institute of Standards and Technology)[3].The development of the paradox which is generally known as cloud computing produceaessential change in the way information technology (IT) services are maintained, scaled, developed, design, updated, deployed and paid for. Computing as we know today reflects a contradiction — on one hand, computers continue to become exponentially very strong [4] and cost of computing fall quickly according to the per unit cost, so much so that computing power per se is nowadays considered to be largely a commodity [5].

Today cloud computing paradigm increasing day by day and therefore risks also appeared in that cloud computing paradigm. With some new risk we also get some specific issues and this is only because of law and regulation. Some of the operational risks occurred by using the outside provider. First of all cloud community find out the specific risks and then re-evaluate them. In cloud computing risk should be considered at infrastructure layers and service. According to the Cloud architecture level of risk vary significantly. Cloud users can transfer some of the risk to outside cloud provider.

Five essential Characteristics of Cloud computing are resource pooling, fast elasticity, regular service, on demand self-service, and broad network access [6].

Objectives of this review paper are:-

1. Find out the loss by using the scientific and objective methods for providing the good cloud computing services.
2. Loss exposure measuring and analyzing from cloud computing
3. Facilitate the information to the administrator so that risk management decisions can be made in cloud computing.
4. Based on the objective and risk focused assessments provide support to the management's authorization
5. Make good risk management strategies so that have control over the attributable to cloud computing

The remainder of this paper reflects the issues/risks of adopting cloud computing, strategies to prevent those risks, risk management including mitigation of risks, control standards of cloud computing given by various institutions and finally, conclusions and implications are provided.

II. ISSUES/RISKS FROM CLOUD PROVIDERS PERSPECTIVE

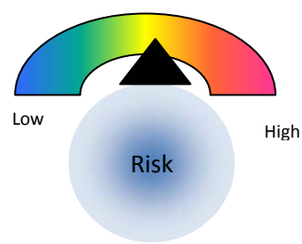

Figure 1 Medium Risk

RQ1: Risks from Cloud Providers Perspective

A. Data Security, Privacy & Control Risks

In cloud computing both data security and privacy risks can be reduced with the help of data encryption and cloud service provider responsible for handlingtheserisks. [6]. There should be data backup and encryption schema for the data availability and integrity [7]. Cloud service providers are also responsible for data security measures.There are some of the strong encryption techniques which help in data security [8].Cloud Providersmainlyresponsible for the both privacy and security of data in cloud computing [9]. When data is being processed and transferred and then stored in that case only cloud service providers

responsible for security of the data [10]. Cloud Service Provider can only specify the all thesecurity settings distantly.If the security risks not apply properly then it isserious security risks for Cloud Service Provider if the security settings are not fully implemented [11].

- *Identity and Access Management (IAM)*

In IAM by adjusting the serious security problems we can increase operational productivity and governing compliance. To keep away from unofficial access, the CSP should provide strict access control tool. In cloud computing managerial access is done by the internet and this strengthens the risk of unofficialaccess to data. So, it is very important to control and observe the managerial access to preserve protocols [12,7]. Information or Data in the cloud computing is distributed worldwide which show the concern of control and security [13]. Before allow access, only 38% of cloud giver was assured about safety to verify users whereas, 51% of cloud giver examine IAM as the cloud giver's duty. Therefore, attain compliance need could be difficult [14].

- *Multi-tenancy*

It is important elements of cloud computing because it helps in improve the use of basic hardware resources and permit for proper resource facilities. One of the detracting challenges for the public cloudis efficient Literature Review 289Multi-tenancy safeguard and privacy [15]. It is the duty of CSP to provide aunique border line for each user's data at both physical and implementation levels [16]. The private and financial data of customer's are stored by the CSP. So, CSP is accountable for customer's information[17].

In the same database data from many occupants is possible to be stored, the risk is very high between these occupants [10].Data from other clients is placed in a shared environment whichresult into a high risk for Cloud Service Provider. There is a requirement for some tools by which CSP assure data privacy between clients and they will be responsible for the privacy[18].

- *Data Availability and Backup*

The data are provide differently in the cloud because it is not easy for CSP to assure sufficient availability and support of data in the cloud computing.In the expansion it is not only difficult to backup and recover the information in case of failure [19].There are many different places in the cloud environment that will damage the data or informationcontaining the cloud computing facilities [20].

B. Organizational Risks

Organizational risks are classifiedas the causality that may influence the structure of the business organization as an object. These risks contain the loss of goodwill of firmand any change in the firm that can cause the provider's failure and ending of the addition [21].

- *Organizational Change Management*

The biggest organizational risk Resistance to change good from organizational politics, changes to people work. To modify this, use insight from organizational changemanagement and involve main stakeholders in the approval procedure [22].

- *Resource Planning*

The risk to resource planning is the loss of control over resources, which lead to unclear roles and duties. To reduce this, it is important to make clear roles and responsibilities before cloud adoption. [22]

- *Organizational Security Management*

The current security management models have significantly changed when organization choose cloud. There is a need to review the current security models and expand security standards to ensure the arrangement and adoption of secure clouds [9].

C. Technical Risks

Technical risks are defined as the failures relatedto the innovation and services provided by the CSP, including resource sharing privacy problems, unkind attacks on the CSP risks related to movable and assent [23]. Technical 290 R. Latif et al.risks are related to hardware involving worst conservation of hardware, unmoved system, decrease in the availability and hardware failure [6].

- *Portability in the Cloud*

Interoperability between clouds is due to incompatibilities between CSP platforms. The solution is to use cloud middleware for the ease of cloud interoperability [12].

- *Application Development*

Risk of service interruption at providers side results in extensive outages and unavailability of services or loss of data. The solution suggested by the authors is to use multiple cloud providers and monitor applications from outside the cloud [12].

- *Lack of Interoperability Standards*

Cloud computing lacks interoperability standards. There is no standard of communication and data export format between and within CSP, which makes it difficult to establish appropriate security frameworks [17]. For CSP, adoption of universal standards is also recommended to ensure interoperability among CSP [7].

D. Compliance and Audit

Risks related to lack of authority information, changes in authority, unauthorized conditionin the contract and in progress legal conflict.The rules and regulation defined in the contract and audit SLAs regularly should be followed by the customer and CSP [24]. Standard CSP is subjected to outside audits and security confirmation. If a CSP does not stick to these security audits, then it leads to an obviousdecrease in customer trust [25]. CSP should

have security policies with recoverymethods in case of disasters and the ability to restore data completely in a pre-established amount of time [18].

E. Physical Security

- *Data Location and Data Center*

To provide a safe physical location for customers' data CSP should giveassurance to secure operation of the cloud data center [26]. CSP manages the infrastructure including servers, networks, storagedevices. CSP should apply and operate suitableinfrastructure controls containing staff training, physical location security, network firewalls. To reduce these risks are of most importance because if the physical access control is weak, attackers can steal entire servers, even if they are protected by firewalls and encryption [26]. The cloud provider is not only responsible to store and process data in specific jurisdictions but should also responsible to obeythe privacy regulations of those jurisdictions [27].

3.2 RQ2: Risks from Cloud Customer Perspective

A. Data Security, Privacy & Control Risks

- *User Access*

For the management of all software security controls the customer is fully responsible. These include application access control, IAM, software patching, viruses Cloud Computing Risk Assessment: A Systematic Literature Review 291protection [26]. One of the risks is how a customer face the privileged status of CSP and security issues such as fault elimination, data damage and data migration [28].

- *Data Privacy and Security*

It is an essential security concern for the end- users to know about the privacy and protection of their data from CSP in order to ensure that data privacy is not compromised. But eventually the customers are responsible for the security and integrity of their own data even it resides on providers' premises [14]. The loss of encryption key or privileged access code will bring serious problem to cloud service users [29]. Accordingly, lack of cryptographic management information will heavily lead sensitive damages of data loss and unexpected leakage of user data to the outside world. Customer data and commercial secrets should not be leaked while residing on CSP premises [26]. According to CSA group [30], the burden of avoiding data loss does notfall completely on the provider's shoulder. If a customer encrypts data before placing it to the cloud, and lost the encryption key, the data will be lost as well.

- *Data Segregation*

To find out the techniques used by the provider to segregate the data is the responsibility of cloud customer and must ensure that the encryption schemes are deployed and are effective enough to provide security [31]. Encryption cannot be assumed as the single solution for data segregation problem. In some cases, customers may not want to encrypt data because encryption accident can destroy the data [25].

- *Data Availability*

When the client data is uploaded into the cloud, clients no longer possess any data on the cloud. Customers'personal data and information on the Cloud in not available either lost or heck, it is difficult to retrieve the original data [32].

- *Secure Data Deletion*

Suitable, error free and timely data removal may be impossible and undesirable. One of the reasons is the extra copies of data locate at different locations and the other is that the disk to be destroyed also contain data from other clients [18]. When it is no longer required, data is supposed to be lost completely. The data deleted may still exist and can be restored due to the physical characteristics of storage medium. This may cause a risk of sensitive data acknowledgment to the customer [13].

B. Technical Risks

- *Infrastructure Capabilities*

It is difficult to show CSP that their cloud performance is not in accordance with their agreed SLA because of the server's workload and variable nature of the network. This cause disputes and litigation. The solution is to evaluate the cloud performance under appropriate investigation before adopting. Another solution is to use third party monitoring tools for the verification of system performance [12].

- *Application Development*

The purpose is to allow developers to develop their applications over the provided platform. Therefore, the customers are mainly responsible for protecting their 292 R. Latif et al developed applications and the platform. At the same time, the providers are responsible for isolating the customers' applications and development environments [9].

- *Portability*

According to K. Popovic and Z. Hocenski [33], the risk of compatibility arises if the customer wants to move from one provider to the other because the storage services offered by one CSP may be incompatible with another provider's service.

C. Compliance and Audit

- *Disaster Recovery*

Cloud Customer should know what will happen to their data if a disaster occurs.Therefore, it is the customers' primary security responsibility to ask whether the providerwill be able to completely recover your data and how long it will take. [31]

- *Legal Challenges*

CSP is more influenced to legal and regulatory involvement and commit to keep and process customers' data in specialauthoritythat provides security and privacy of data as promised in their SLA's. Even then, for the privacy of their data kept at the CSP site the organizations are mainly

responsible [34]. The computer processing power or storage one buys via a Cloud service may be based in another country or may be divided between multiple countries. Itraises legal issues by exporting customer's data[35,36].

D. Physical Security

- *Data Location*

As the data is stored redundantly in multiple physical locations by the CSP and that location information is not revealed to the customer. On the customer side, it is difficult to determine whether appropriate security measures are in place to secure customers' data [12]. The customer cannot avoid the downtime of a cloud computing environment, which is the time in which the CSP machines are not working properly. This situation brings immense discourage to the confidence of customers [37].

III. ISSUES TO CLARIFY BEFORE ADOPTING CLOUD COMPUTING

Seven security concerns that an organization cloud computing user should address with cloud computing givers (Edwards, 2009) before adopting has identified by world's main information technology research and advisory company.

*A. User Access:*For hiring and oversight of privileged administrators and the controls over their access to information or data ask providers for special information. Organizations should demand and accomplish their own hiring criteria for personnel that will help them tooperate their cloud computing environments.

*B. Regulatory Compliance:*You should confirm from your provider about submission toexternal audits and securitycertifications.

C. Data location: Organization must be require that cloud provider should reserve and process information or data in specialauthority and they should also agree for privacy rules [38].

*D. Data Segregation:*Look for what is done to select your data and ask about any of the proof that encryption plans are deployed and are adequate.

E. Disaster Recovery Verification: Ask your provider if disaster strikes then they will be able to provide your backup or not and how much time it will take to recover.

*F. Disaster Recovery:*To support specialtypes of information, such as the research involved in the discovery phase of a trial, and verify that the provider has successfully supported such activities in the past we should ask the provider for this. Without evidence, don't assume that it can do so.

*G. Long-term Viability:*Ask providers about howcan you take tour data back from them if they were to fail or be acquired, and check out your data would be in the proper format which will help you in importing into your replacement application.

IV. RISK MANAGEMENT

If any uncertainty or risk occurred then Risk management allow management to properly deal with those risks, which improve the ability to build the quality or value. In this Management – Integrated Framework provide mitigation ways of risk and identification of risk will facilitate the identification of risks and mitigation strategies with the growing cloud computing standard which show thebeneficial opportunities as well as uncertainty[39].

There are many different types of businesses in which circumstances show opportunities for useful and threats to success, i.e. positive and negative condition of risks, respectively.

In this way comparison to traditional risk prevention strategies, accepting some of the risks leads to obtain unique benefits. The Risk Management is the process in whichenterprises treat, in a organized way, risks related with their activities [40]. Thepurpose of each activity is to get benefits and maintainable values and it is anessential part of any enterprise's strategic management.

In cloud computing there is lot ofrisk taking place that should be acknowledged by the cloud providers and they should also be accomplished. For finding the risk in the cloud computing we need to implement the management process like ways of risk mitigation and risk strategies so that risk will take place again

There are two types of safety management principles first is risk based in which it maintain the remaining risk should be analyzed probabilistic and the quality of risk. The second safety principle is consequence based safety in which it state that least possible events at an installation should not have result outside the borders or boundaries and accordingly it give more information about risk mitigation. This indicates that very doubtful events might, but not necessarily will, be tolerated.

Risk management helps in while making decisions and it helps in achieving the organization goals by implementing it on individual performance or activity and functional area. It support with decisions such as the agreement of science-based proof and other factors it also support costs with benefits and expectations in limited public resources where they invest; and the governance to support due diligence, responsible risk-taking, addition and accountability.

Risk Management steps include:

- The security posture monitor continuously
- Assign and track corrective actions, as required, to decrease residual risk to an acceptable level

Figure 2 Risk Management Cycle

Risk management is acontinuous, forward program for building and managing an adequate information or data system position. The risk management program checks it through every day activities and follow-on security risk analyses when an adequate posture is attained. In many cases when follow-on risk analysis must be done, the rules, regulations, or policies that govern the information program will stipulate.

V. RISK IDENTIFICATION

The risk identification phase should result in the definition of relevant IT risks as well as the categorization of existing threats (i. e., risk sources). In order to determine these business-related threats, decision makers are required to identify possible vulnerabilities in their specific IT systems. Only after acquiring knowledge of the weak points, it becomes possible to determine which threats can accomplishment them and, thus, are relevant for risk management [41].For find out the risk enterprise can apply various methodsthat can be classify into collection method. Collection methods like checklists have the risk-specific data collection in common. Therefore, they are mainlysufficient for the identification of already known IT security risks. Creativitymethods such as, brainstorming or the Delphi method, are based on creative processes, which are characterized by divergent thinking. Thus, they can be used to anticipate future previously unknown risks. Analytical searchmethods use the existing IT infrastructure and its characteristics as a starting point for searching vulnerabilities and threats [41] (Prokein, 2008, pp. 19f.). Examples for these methods are threat or attack trees (Amoroso, 1994, pp. 15–29), or penetration tests (Eckert, 2006, pp. 76–86). Reports from security-related organizations addressed IT security risks related to Cloud Computing. These reports can be used during the risk identification phase as checklists in order to discover more threats and risks in the individual scenario. For example, the Cloud Security Alliance provides guidelines and practical recommendations for managers that aim to protect security, stability, and privacy when using Cloud Computing[30]. Additionally, the Cloud Security Alliance issued a whitepaper including in-depth descriptions of the top seven threats to Cloud Computing [30]. Likewise, the European Network and Information Security Agency (ENISA) also published recommendations regarding information security risks for potential and existing usersof Cloud Computing (European Network and Information Security Agency, 2009).The report describes major risks, and presents an information assurance framework including technical measures for risk mitigation and provides guidelines regarding the assessment of security risks and benefits involved in the use of Cloud Computing.

VI. RISK ASSESSMENT

Value defined as a function of risk and reaction. Each and every decision either improves or conserves the value. It is given that risk is intrinsic to the inquiry of value, strategic-minded organizations do not attempt to exclude risk or they do not even try to mitigate it, a perspective that serves as disapproving change from the traditional view of risk as something to avoid. Relatively, these organizations explore to maintain risk acknowledgment over all elements of their organizations so that, in the given period of time, they get only right type of risk and risk should be no more nor less so that they can achieve their strategic goal easily.

Risk assessment is necessary because it helps the organization to handle the risk and also tells about how useful these risk to the organization to achieve their goal. To accomplish this, organization need to practically because it is very easy to understand. This assessment process should be continuing in a proper and organized manner. It should be perfectly sized to the organization's size, intricacy, and earthly reach. While enterprise-wide risk management (ERM) is a relatively new regulation, application techniques have been expanding over the last decade. The main motive of this review paper is to facilitate leadership with the risk assessment techniques and that will help in decision making. [43]

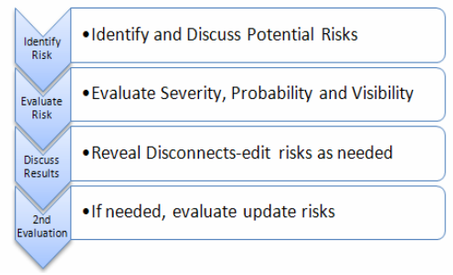

Figure 3 Risk Assessment: Process Mapping

A. *The Risk Assessment Process*

Risk assessment chases event identification and introduces risk return. Its main goal is to determine the risk length in both the case individually and collectively so that risk management can focus on the most threats and opportunities of the risk and to temporal the originwork maintained within the defined boundaries without controlled for running desirable opportunities. Measuring and prioritizing risks so that risk levels are managed within defined tolerance thresholds without for risk return. Risk assessment is mainly about the all about calculating and arranging risks so that risk can be being overcontrolled or forgoing desirable opportunities. Actions alsogenerate risk assessment containing the fundamentalestablishment,regular refresh, commencement of the project,recoveryand a big restructuring. Some of the risks are changing and desirepersistenton-going checking and computation, like some of the markets production risks. Other risks are more static and need rechecking on a periodic basis with on-goingchecking produce an alert to reassess sooner should circumstances change.

B. *Identify risks*

The risk identification process lead risk checking and produces a detailed list of risks which maintain by the risk classification (financial, operational, strategic, compliance) and sub-category (market, credit, liquidity, etc.) for organization units, corporate functions, and capital projects. At this stage, a wide net is cast to understand the universe of risks making up the enterprise's risk profile. Whatever the risk catch may be useful to administration at the function and business unit level, the list requires prioritization

to focus senior management and board attention on key risks. This prioritization is accomplishedby performing the risk assessment.

C. Develop assessment criteria

The first activity within the risk assessment process is to develop a common set of assessment criteria to be deployed across business units, corporate functions, and large capital projects. Risks and opportunities are typically assessed in terms of impact and likelihood. Many enterprises recognize the utility of evaluating risk along additional dimensions such as vulnerability and speed of onset.

- *Assess risks:*Assessing risks consists of assigning values to each risk and opportunity using the defined criteria. This may be accomplished in two stages where an initial screening of the risks is performed using qualitative techniques followed by a more quantitative analysis of the most important risks.

- *Assess risk interaction:*Risks do not exist in isolation. Enterprises have come to recognize the importance of managing risk interactions. Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions, to cause great damage or create significant opportunity. Therefore, enterprises are gravitating toward an integrated or holistic view of risks using techniques such as risk interaction matrices, bow-tie diagrams, and aggregated probability distributions.

- *Prioritize risks:*Risk prioritization is the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds. Risk is viewed not just in terms of financial impact and probability, but also subjective criteria such as health and safety impact, reputational impact, vulnerability, and speed of onset.

- *Respond to risks:*The results of the risk assessment process then serve as the primary input to risk responses whereby response options are examined (accept, reduce, share, or avoid), cost-benefit analyses performed, a

- response strategy formulated, and risk response plans developed.

Discussions of event identification and risk response are beyond the scope of this paper. For detailed treatment, refer to the COSO *Enterprise Risk Management – Integrated Framework* (2004).

VII. STRATEGIES TO ADDRESS RISKS

Cloud computing strategies [42] comprises six phases of adoption lifecycle starting from the initial phase until the governance of continuous operations.

A. Initial Planning

In this phase, a high-level analysis exploring the business objectives and how adoption a cloud can fit with the business strategy is executed. There are several key outputs from this phase, i.e. the business model in which the current capabilities and values are explored to find the necessary improvements, a high level plan of projects including the project owners, and the expected business outcomes to be realized in a due time.

B. Enterprise capabilities and cloud vision

The focus of this phase is to provide an understanding of the overarching abilities needed to support the cloud implementation. Several key work artifacts from this phase are the vision statement of cloud adoption; adoption pattern; a business case which provides information about plausible costs and benefits, value propositions and return on investment for cloud and a governance model.

C. Target architecture and cloud enablers

In this phase, the requirements influencing the cloud adoption decisions are explored in greater details. There are three areas relevant for the updates in the existing architecture in relation to cloud adoption: 1) the business architecture, 2) the information system, and 3) technology and infrastructure architecture.

D. Gap analysis and transition planning

state and a cloud adoption roadmap which provides a list of actions for realizing the cloud adoption strategy. Gap analysis is must and it helps in the comparison of organization's actual performance with its capability and hence to know the insufficiency of current situation. A conversion plan is the planning for a change and for this, a sufficient understanding on the change management needs is important to achieving the benefits. The key reachable for this phase are a change management plan which introduce how to organize the people and the organization from its current state to the future

E. Implementation of Planning

In this last phase of cloud adoption strategy a settlement with the cloud provider is made and contract is signed to star the mostimportant works in this phase. The key movement of this phase is SLA arrangement and the formulation of the union requirements.

F. Governance

This is a continuous activity which underlines the whole processes of cloud adoption. The governance is expected to provide a strategic direction which defines how the cloud adoption will be performed, managed and controlled.

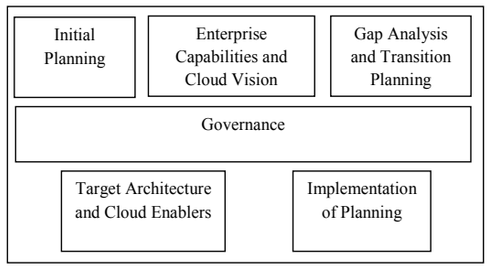

Figure 4: Cloud Adoption Strategies

VIII. RISK MITIGATION IN THE CLOUD

Mitigating Risk in Cloud Computing, categorizes cloud risk mitigation by several functional areas:

- Security and privacy — Security is the most important worry for the cloud distribution or deployment. In cloud computing cloud security demands that the integrity of data stored and it should be processed within the cloud, and then data should also be transferred from and to the cloud be protected. Security mainly linked to the privacy concern, with the target of privacy falling objectively on information or data that consist of linked to privatelydetectabledata.

- Availability and reliability — The organization should confirm that cloud service and all data or information should be accessible only by the authorized user all the time while using the cloud service. Bottom line affect by the lack of availability or reliability that means loss of availability for many enterprise or organizations, like opportunities of lost businessor lost fertility. Disaster recovery and business continuity planning play a major role in availability and reliability considerations in the cloud.Users of cloud computing believe that cloud means reliable but cloud failures can be occurred anytime or from.Each and every organization always focus on the availability and reliability for delivering the good service and they should also have full planning of disaster recovery which should be implementand therefore they can secure their data or information. These plans help the organization by keeping the redundant copy of their data or resources at remote site or different places so that they can recover these redundant copies at the time of any disaster.

- Scalability — It is not necessary that everyapplication which is designed in the cloud computing will work properly.Cloud providesscalability which is of high level but single application may not. For example, an application may execute hugeinformation or data transfers for all transactions which result in performance bottleneck and acquire high service charges. To achieve the scalability it may require rewriting and redesigning part of in house application within the cloud so that scalability concerns can be reduced or eliminate from the cloud. Cloud scalability another condition is being prepared for actualfacilities of resources according to the requirement, as well as rapid deprovisioning when resources are no longer needed. Within the cloudeliminate scalability risks can increase performance and reduce costs for cloud implementations.

- Compatibility and standardization — Organizations used to held important, remarkable concerns regarding vendor lock-in with cloud deployments. Example, an organization writes an application to communicate with a particular cloud provider's unique APIs. In future, that organization should move its application to a separate cloud, those portions of the application would have to be rewritten so as to use a separate cloud provider's unique API. Luckily, customer's complaints have driven many cloud providers to drop their use of unique APIs. But still, IT shops are cautioned to avoid clouds. Instead, clouds with better standardized approach to interoperability must be sought.

- Commercial viability — Risks faced in achieving a return on investment in cloud resources must be addressed by an enterprise. It is believed by a large amount of users that cloud service invariably gives cost savings for organizations, but actually, standard technologies are cheaper than cloud solutions under few circumstances like every other IT resource, Cloud resources must be managed. It is not necessary that all the applications are designed with cloud infrastructures in mind, therefore behaviour of those applications may take up important cloud resources and therefore correspondingly costly.

IX. CONCLUSION

Cheaper processors, faster networks, and the rise of mobile devices are driving innovation faster than ever before. Cloud computing is a manifestation and core enabler of this transformation. Just as the Internet has led to the creation of new business models unfathomable 20 years ago, cloud computing will disrupt and reshape entire industries in unforeseen ways. Though Cloud Computing is revolution in IT technology which can change the IT usage which always looks for cost reductions, there are issues and challenges in cloud adoption which if addressed properly can lead to a safe, pleasant and economically viable cloud adoption.

Prospective users of cloud need to understand and evaluate the risks associated with different cloud service and delivery models, paying particular attention to business requirements, data protection laws and compliance regimes. In every area, customers need to work closely with providers to put the right security in place. Some responsibilities are shared while other rest with either party but it is vital to know who is responsible for what, and ensure that the right governance processes, and mechanisms for sharing information, are in place.

There is evidence that security considerations are still inhibiting many organizations' adoption of cloud, but we believe that with the right approach to security they can pursue cloud strategies safely and reap the benefits.

REFERENCE

[1] R. Charanya, M. Aramudhan, K. Mohan, S. Nithya, "Levels of Security Issues in Cloud Computing,"

[2] Buyya R. and Parashar M. User requirements for cloud computing architecture, Proc. 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, Melbourne, Australia, 17-20 May 2010, pp. 625-630.

[3] Rebollo, O., Mellado, D.: Systematic Review of Information Security Governance Frameworks

[4] Lasica JD. Identity in the Age of cloud computing: The Next-generation Internet's Impact on Business, Governance and Social Interaction, The Aspen Institute, 2009.

[5] Hackett S. Managed Services: An Industry Built on Trust, IDC, 2008.

[6] Djemame, K., Armstrong, D.: Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. In: Int. Conference on Cloud Computing, GRIDs, and Virtualization(2011)

[7] Harauz, J., Kauifman, M., Potter, B.: Data Security in the world of cloud computing. IEEE Security & Privacy 7(4), 61–64 (2009)

[8] Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1–11 (2011)

[9] Takabi, H., Joshi, J.B.D.: Security and Privacy Challenges in Cloud Computing Environments. Published. IEEE Security and Privacy 8(6), 24–31 (2010)

[10] Hashizume, K., Rosado, D.G., Medina, E.F., Fernandez, E.: An analysis of security issues for cloud computing. Journal of Internet Services and Applications 4(5) (2013)

[11] Reddy, V.K., Thirumala, R.B., Reddy, L.S.S., Kiran, S.: Research Issues in Cloud Computing. Global Journal of Computer Science and Technology 11(11) (July 2011)

[12] Khajeh- Hosseini, A., Sommerville, I., Bogaerts, J., Teregowda, P.: Decision Support Tools for Cloud Migration in the Enterprise. In: IEEE CLOUD 2011 (November 2011)

[13] Rahul, S.S., Rai, J.K.: Security & Privacy Issues In Cloud Computing. International Journal of Engineering Research & Technology (IJERT) 2(3) (March 2013)

[14] Argall, K.: Compliance in a Cloud Computing Environment. HIPAA and PCI DSS (2010)

[15] Ren, K., Wang, C., Wang, Q.: Security Challenges for the Public Cloud. Journal of Internet Computing IEEE 16(1) (2012)

[16] Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1–11 (2011)

[17] Pearson, S., Benameur, A.: Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2nd Int Conference on Cloud Computing Technology and Science (2010)

[18] Ayala, L.C., Vega, M., Vargas, L.M.: Emerging Threats, Risk and Attacks in Distributed Systems: Cloud Computing. In: Elleithy, K., Sobh, T. (eds.) Innovations and Advances inComputer, Information, Systems Sciences, and Engineering. LNEE, vol. 152, pp. 37–52. Springer, Heidelberg (2013)

[19] Pearson, S., Benameur, A.: Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2nd Int Conference on Cloud Computing Technology and Science (2010)

[20] Chen, D., Zhao, H.: Data Security and Privacy Protection Issues in Cloud Computing. In: Int. Conference on Computer Science and Electronics Engineering, pp. 647–651 (2012)

[21] Dahbur, K., Mohammad, B.: A Survey of Risks, Threats and Vulnerabilities in Cloud Computing. In: Int Conference on Intelligent Semantic Web-Services and Applications(2011)

[22] Khajeh- Hosseini, A., Sommerville, I., Bogaerts, J., Teregowda, P.: Decision Support Tools for Cloud Migration in the Enterprise. In: IEEE CLOUD 2011 (November 2011)

[23] Rana, S., Joshi, P.K.: Risk Analysis in Web Applications by Using Cloud Computing. International Journal of Multidisciplinary Research 2 (January 2012)

[24] Chou, Y., Oetting, J.: Risk Assessment for Cloud-Based IT Systems. International Journal of Grid and High Performance Computing, 1–13 (April - June 2011)

[25] Kumar, V., Swetha, M.S.: Cloud Computing: Towards Case Study of Data Security Mechanisms. International Journal of Advanced Technology & Engineering Research 2(4)V (2012)

[26] Julisch, K., Hall, M.: Security and Control in the Cloud. Information Security Journal: A Global Perspective, 299–309 (2010)

[27] Kumar, A.: World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER) 1(2) (June 2012)

[28] Che, J., Duan, Y., Zhang, T.: Study on the Security Models and strategies of cloud Computing. In: Proc: Int Conference on Power Electronics and Engineering Application (2011)

[29] Lee, K.: Security Threats in Cloud Computing Environments. International Journal of Security and Applications 6(4) (October 2012)

[30] Cloud Security Alliance CSA: The Notorious Nine Cloud Computing Threats 2013 (2013)

[31] Bisong, A., Rahman, S.M.: An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & its Applications 3(1) (January 2011)

[32] Ahmad, T., Amanul, H.M., Al-Nafjan, M., Ansari, A.: Development of Cloud Computing and Security Issues. Information and Knowledge Management 3(1) (2013), http://www.iiste.org

[33] Popović, K., Hocenski, Ž.: Cloud computing security issues and challenges. MIPRO (2010)

[34] Jansen, W., Grance, T.: Guidelines on Security and Privacy in Cloud Computing. NIST (2011)

[35] Prasad, M., Naik, R., Bapuji, V.: Cloud Computing: Research Issues and Implications. International Journal of Cloud Computing and Services Science 2(2), 134–140 (2013)

[36] Sharma, M., Bansal, H., Sharma, A.K.: Cloud Computing: Different Approach & Security Challenge. International Journal of Soft Computing and Engineering 2(1) (March 2012)

[37] Peiyu, L., Dong, L.: Risk Assessment Model for Information System in Cloud Computing Environment. Advanced in Control Engineering and Information Science. V. 15 (2011)

[38] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[39] [Online] Cloud Computing, http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf.

[40] "ISO 31000:2009," Risk management - Principles and guidelines, 2009, http://www.iso.org/iso/cataloguedetail?csnumber=43170.

[41] Isom, P., & Holley, K. (2012). Is your company ready for cloud? Choosing the best cloud adoption strategy for your business. Boston: Pearson Education, Inc.

[42] [Online] Mitigating Risk in Cloud, http://webobjects.cdw.com/webobjects/media/pdf/Solutions/Cloud-Computing/151383-Mitigating-Risk-in-the-Cloud.pdf

[43] R. M. Steinberg, Miles Everson, Frank J. Martens, Lucy E. Nottingham, "Enterprise Risk Management-Integrated Framework", COSO, September 2004.

AUTHORS PROFILE

Nisha is the student of Master of Computer Applications in Ansal University, Gurgaon, Haryana, India.

Vijaya Lakshmi Singh is the Assistant Professor in School of Engineering and Technology, Ansal University, Gurgaon, Haryana, India. She has 6 years of teaching experience. Her areas of interest includes ad hoc network and cloud computing.