Risk Supervision Framework for a Federated Cloud

M. Satheesh, Research Scholar, Don Bosco Arts and Sci College, Karaikal.
Email: dbcsat14@gmail.com

Abstract

Cloud Federation is a new collaboration model organizations share the information and data across their private cloud infrastructures. But the adoption of cloud federations are hindered by the federated organizations primary concern is of the potential risks of unauthorized data leakage and misuse of data. For cloud federation to be feasible, federated organizations' privacy concerns should be remedied by providing mechanisms that can allow organizations control which users from other federated organizations can access the data. We propose This paper highlights the overview, benefits and security risks and challenges of cloud computing. The main problem discussed Risk supervision and Management is that several security risks and problems occur when using cloud computing in both sides. Users and Providers. These risks can be decreased when the level of trust grows between the users and providers. In the present scenario of the cloud development, the risks and problems affects both of cloud services and security. Thus the Risk Management Framework(RMF) is designed for dealing with few security issues and certain impacts on the business is proposed from the cloud provider's perspective. Cloud users are granted access to federated data when their identity attributes match the common policies, but without revealing their attributes to the organization which owns data. The RMF is suggested for cloud-computing providers regardless of their types and models, based on the NIST risk management guide and security risk management.

1. Introduction

Cloud-computing technology has rapidly developed. Widespread application is anticipated in social, business, and computing aspects. Cloud computing changes the Internet into a new computing and collaborative platform. It is a business model that achieves purchase on demand and pay-per-use in a network. Many competitors, organizations, and companies in industry have jumped into cloud computing and implemented it. Despite of all the advantages cloud Cloud computing has become popular in the IT industry. Cloud computing has numerous advantages of for providers, adopters, and users. Gupta, Seetharaman, and Raj reviewed some empirical studies on the usage and adoption of cloud computing by small and medium enterprises and found that cost reduction, avoiding natural disaster mishaps, sharing and collaboration, trust in cloud providers, reliability, security breaches, and service disruption are the most important parameters. They stated, "One of the biggest advantages of moving to cloud computing is the opportunity cost of freeing up some of the IT administrative time, which can now be applied to the business aspects of growing the core business of SMBs"[1]. Jadeja and Modi provided five benefits of cloud computing: easy management, cost reduction, uninterrupted services, disaster management, and green computing. In addition, Brohi and Bamiah revealed that cost reduction, easy scalability, and increased productivity are the main advantages of applying cloud computing [2]. Accordingly, cost reduction, ease of use and convenience, more productivity, reliability, sharing, and collaboration are the highlighted benefits of applying cloud computing. The two fold goals are to increase confidence between the user and the cloud provider and increase the security level in all cloud services.

2. Analysis of the Present Scenario

In the present scenario, as any new concept, cloud computing is facing several critical issues; the most prominent is the security issue. According to Tax and Ali [3], the “Gartner survey showed that more than 70% of respondents said they do not intend to use the cloud computing at recent, the main reason is afraid of the data security and privacy.” Also, they stated that a large number of Google users’ files were leaked in March. Aleem and Sprott, as cited in [7], “interviewed 200 Information and Communications Technologies professionals worldwide. Respondents’ most cited concern regarding the use of cloud computing was security, as reported by 93.4 percent of interviews.” Brohi and Bamiah stated, “According to a survey conducted by International Data Corporation (IDC), 53% of organizations in the Asia-Pacific region are already using some form of cloud computing services, and the remaining 47% of the organizations have plans to adopt private or public cloud services in the next 12 months” [16]. Additionally, they revealed that the survey results indicate that cloud computing is a not highly adopted technology; however, the growing contributions by researchers and IT industries will increase the use of cloud computing globally.

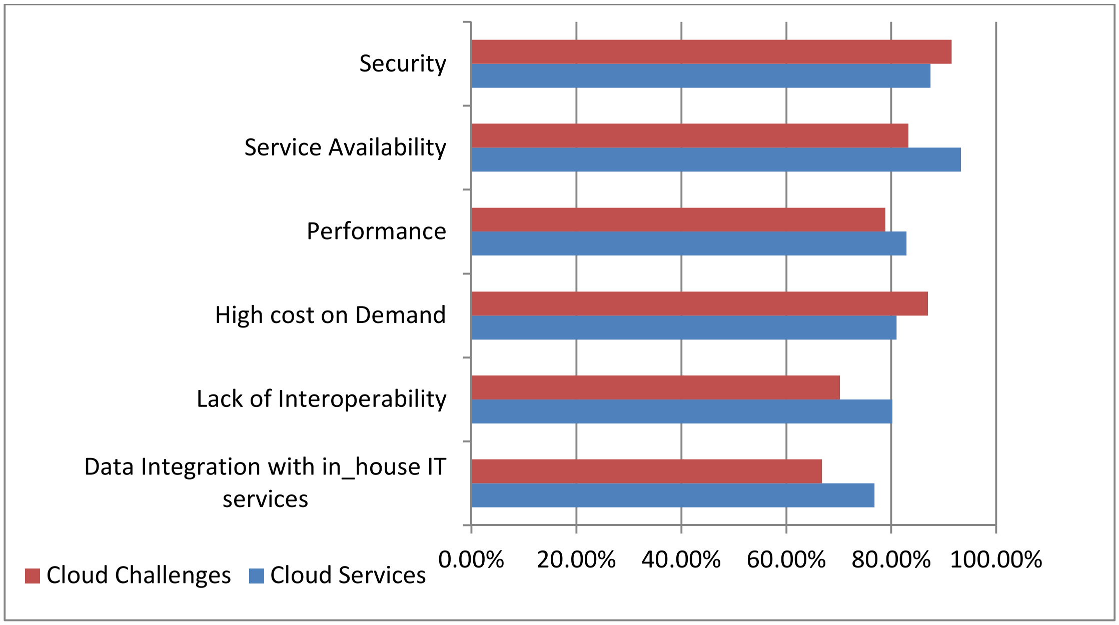
As the number of security incidents continues to increase, more people are worried using the cloud. Many studies and researchers have addressed cloud computing threats and other problems. Threats although many cloud-computing users tend to not worry about doing backups, keeping hackers out of their data or providing more virtual storage space, there are still various risks that users might not realize. The security is a significant problem. Cloud computing contains important and sensitive data, such as personal, government or business data, that attract hackers’ attention. Therefore, the cloud-computing system must be protected more carefully than any traditional network system.

The traditional security mechanisms cannot protect the cloud system entirely [4]. Some of the main security problems include data security, user data privacy protection, cloud computing platform stability, and cloud computing administration [4]. In 2008, “the U.S. information technology research and consulting firm Gartner issued a ‘cloud computing security risk assessment’ report, mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud, listing seven major security risks that the cloud computing technology exist”. Just to enumerate the collected data are presented as cloud services and challenges in Table 1. Risks or threats can be divided into two types: network and security. Though we will be discussing of both however, the focus will be on security threats.

S.No	Risks in Cloud - on_demand model	Percentage	
		security	services
1.	Data Integration with in_house IT services	76.80%	87.50
2.	Lack of Interoperability	80.20%	93.30
3.	High cost on Demand	81.00%	83.90
4.	Performance	82.90%	81.00
5.	Service Availability	83.30%	80.20
6.	Security	87.50%	76.80

Table-1: Risks and Challenges in cloud

The following graph depicts that as the cloud services on the increase the risks and challenges lie within minor differences with its available services. The factors are 1. Security, 2. Service availability, 3. Performance, 4. High cost on demand, 5. Lack of interoperability, 6. Data integration with in the house IT services. The analysis findings are made on study of the risks in clouds in the present scenario.



Graph1: Cloud challenges and Risks

3. Threats in Cloud

Although many cloud-computing users tend to not worry about doing backups, keeping hackers out of their data or providing more virtual storage space, there are still various risks that users might not realize. The security is a significant problem. Cloud computing contains important and sensitive data, such as personal, government or business data, that attract hackers' attention. Therefore, the cloud-computing system must be protected more carefully than the traditional system.

3.1 Seven Top Security Risks in Cloud Services

Risk	Description
Privileged user access	Sensitive data processed outside the enterprise brings with it an inherent level of risk
Regulatory compliance	cloud computing providers who refuse to external audits and security certifications
Data location	The customer probably don't know exactly where your data is Hosted
Data Segregation	Data in the cloud is typically in a shared environment alongside data from other customers

Recovery	A cloud provider should tell what will happen to the data and service in case of a disaster
Investigative support	Investigating inappropriate or illegal activity may be impossible in cloud computing
Long-term viability	Data should remain available even after such an event

3.2 Security Threats

As cloud-computing users, we lose control over physical security. So how can we ensure that data will not leak and privacy can be protected? In order to understand the suggested solutions available, types of attack that we might experience should be highlighted.

3.2.1 Browser Security

Once a user requests a service from the cloud server, the user's Web browser plays a significant role. Even if the Web browser uses SSL, sniffing packages on an intermediary host can get decrypted data [1]. Also, the attacker uses decrypted data (credentials) as a valid user on cloud system. Web Services Security is a method to eliminate the browser threat by using XML Encryption and XML Signature to guarantee confidentiality and integrity to SOAP messages [1], for example, Kerberos, standard usernames, passwords, and X.509.

3.2.2 Interfaces and Application Programming Interfaces APIs

Cloud users are provided with set of software interfaces or APIs to manage cloud services. Unsecure APIs, which allow software applications to interoperate with each other by passing login information between them, are among the top cloud threats [7]. According to Peerson and Yee, "From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy" [8]. The big concern with this threat is that third parties often build upon these interfaces to offer value-added services to their customers, which increases the security risks.

3.2.3 Cloud Malware Injection Attack.

This attack works against cloud services, applications, or virtual machines [7]. Attackers can create their own malicious service by using functionality changes or data modifications for specific purpose [2]. Then, they upload this service into the cloud system by tricking it. The cloud system automatically redirects valid user's requests to the malicious service implementation, and that code is executed. To prevent cloud malware injection attack, it is necessary to use the hash function, store a hash value on the original service instance's image file, and compare this value with the hash values of all new service instance images [1].

3.2.4 Flooding Attacks.

This attack exploits some cloud's features, which increases and initializes new services in order to maintain user's requirements and requests. The attacker requests a huge amount of particular service; this means that cloud computing would not be capable of supplying service to normal users' requests because the system works against the attacker's requests [2]. A denial of service (DoS) attack is one type of forceful flooding attack. According to Qaisar and Khawaja, installing firewall to detect and filter fake requests is a countermeasure for flooding attacks [2].

3.2.5 Data Protection

Data protection is very important and complicated for a cloud consumer because it is hard to ensure that the data are handled in a lawful way [2]. For this attack, the consumer should be aware of whether or not the data is handled in a rightful way. In addition, data compromise can occur due to unauthorized parties' accesses, loss of an encoding key, or deletion or alteration of records without a backup of the original content [8].

3.2.6 Incomplete Data Deletion.

The significant risk that a cloud consumer might experience is incomplete data deletion. The reason is that there are many replicas of these data in other servers, maybe as backup. Also, the majority of operating systems do not delete data accurately or completely. Jamil and Zaki, as cited in [2], revealed that "Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients." Additionally, Qaisar and Khawaja suggested using VPN and query for securing and completing removing of data from cloud servers that have replicate data.

3.2.7 Locks In.

The last security issue is locks in. It is related to data, application, and service portability. There is little offered in the way of tools, procedures, or standard data formats that could assure data, application, and service portability [2]. Therefore, the cloud customer cannot move from provider to another or shift the services back to an in-house IT environment.

3.3 Network Threats

The following are the major network issues related to cloud computing:

3.3.1 Denial of Service (DoS)

DoS attacks are not new; they can make cloud computing resources and services unavailable to the users [7]. Overflow frequent requests send to the server by attacker to stop the server functionality that provides the services. As a result, the server is unable to respond to the regular users. According to Qaisar and Khawaja [1], to avoid cloud computing DoS attack, it is important to reduce users/attackers' privileges based on their behaviors when they are connected to cloud server.

3.3.2 Network Sniffing

It is a way of analyzing network traffic for hacking unencrypted data that is transmitted through cloud network. To illustrate, if the user does not use encryption techniques during communication with the cloud server, hackers can capture data such as username and password. Therefore, an encryption technique is an effective method to eliminate network-sniffing threat [1]. Man in the Middle Attack. During data transmission between user and cloud server, there is a potential threat called “Man in the Middle Attack.” According to [7], data that are transmitted without encryption may be hack or stolen. [1] suggested encrypting and compressing the data during transmission by installing a secure socket layer (SSL) to prevent man in the middle attacks.

3.3.3 Port Scanning

Attackers use port scanning to discover exploitable communication channels/ports between the user and cloud server. The attacker’s goal is to find an active port and exploit vulnerable cloud services [1]. Thus, one main component of network security structure is the firewall. Both user and cloud server need to employ firewalls to detect and filter authorized traffic.

4. Risk Management Framework (RMF)

The RMF is suggested for cloud-computing providers regardless of their types and models, based on the NIST risk management guide and McGraw’s security risk management. From business perspective, cloud-computing providers were basically found to provide products and services for their own profits. Among various ways to deliver computing resources and services, cloud-computing providers’ underlying mission is that every user can use available applications and get services easily regardless of location and the device operating system [1]. Their basic business goal is to deliver high secure and reliable applications and services. Also, the providers aim to gain costumers trust and loyalty. Cloud-computing providers have encountered dangerous security risks and problems. These security risks would negatively affect confidentiality, privacy, reliability, and integrity of a provider’s services. Therefore, a specific RMF process dealing with security risks and problems is recommended.

The basic idea of RMF is simply identify, rank, track, and understand software security risk as it changes over time. This framework can be used widely and flexibly because it can fit with small and large enterprises. Also, the advantage of using RMF is that it “is not specific to security risks; it can be applied in non-software situations” [1]. However, the main goal of using RMF with cloud-computing providers is to consistently track and handle risks and threats. It is significant to define risk management and its purpose in general.

Stoneburner, Goguen, and Feringa defined it as “the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ missions.” The explicit goal of applying risk management in any organization is to minimize negative impacts on organizations and fulfill a need for sound basis in decision making [2]. Tanimoto et al. analyzed cloud computing security problems in detail based on the risk breakdown structure method and the risk matrix method. They provided risks that extracted from user’s viewpoints. Xie et al. suggested a risk management framework for cloud computing, which consisted of five components: user requirement self-assessment, cloud service providers desktop assessment, risk assessment, third-party agencies review, and continuous monitoring. Our framework is different from Xie et al. who involved users, providers, and third parties in their framework. We emphasize the business angle in this framework; the marriage of business and technical concerns is the central driver of our risk management plan. Also, increasing the adopters and users of cloud computing is one of this framework goals [3].

Our RMF consists of six stages, discussed in detail in the next section. A continuous risk management process is a necessity in cloud computing. Also, continuous monitoring process is highly required through ongoing risk identification, implementation and assessment. The risk management plan should be well planned and collaborative between and among different departments. So, sufficient time must be given for planning, collaboration, and communications.

Figure 2 shows that monitoring is needed all the time to ensure that what was expected is actually working. This needs to be performed at consistent time intervals set in the risk management documentation. Sometimes it is necessary to place a watch on areas, and at other times, it will be prudent to change a certain process. If the process has been changed, it is added to the risk management documentation. Some organizations prefer to outsource the monitoring, and others will keep the monitoring in-house. When monitoring cloud services, it might be logical to form a team between several different companies for better mobility in the documentation for the future reference and data filing.

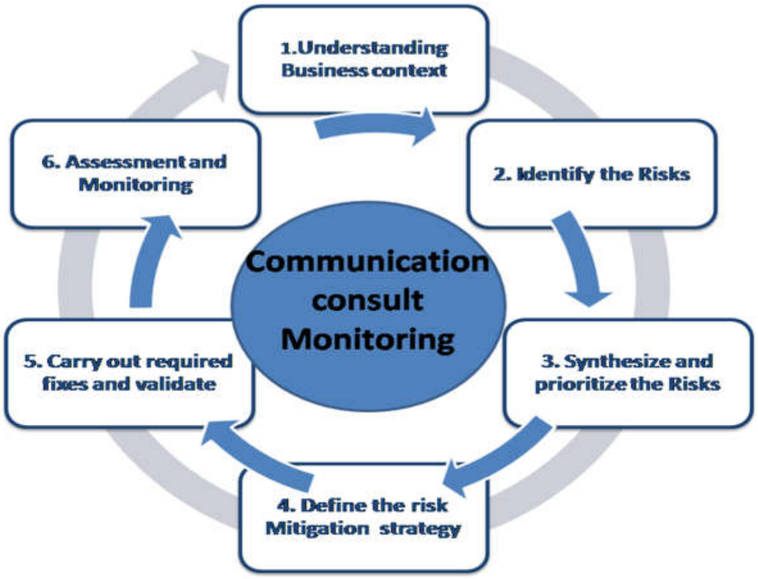

1.Understanding Business context
2. Identify the Risks
3. Synthesize and prioritize the Risks
4. Define the risk Mitigation strategy
5. Carry out required fixes and validate
6. Assessment and Monitoring
Communication consult Monitoring

Figure 2: RMF Six fundamental activity stages

6. Risk Management Framework Stages

The RMF consists of six fundamental activity stages:

1. Understand the business context
2. Identify the business technical risk
3. Synthesize and prioritize the risk,

4. Define the risk mitigation strategy
5. Carry out required solutions and validate that they are resolved, and
6. Overall assessment and monitoring of the system.

6.1 Understand the Business Context

This includes describing the business's goals, priorities, and circumstances to understand what software risks and which business goals are paramount. Different information, including quantitative and qualitative data, will be gathered. System analysts should develop several questions to interview and survey different people (e.g., manager, IT management, clients, developers, employees). Also, they are encouraged to develop research projects to examine the overall system and reduce it to a reasonably small set of components.

Table2 provides a guideline for ranking goals in a way that effectively meet standards required by federal regulations. This ranking places business goals under three broad heading of high (H), medium (M), and low (L), depending on the extent of its impact on the project, the employees, and the company at large. The goal is ranked high if it is crucial to the existence and continuity of the project. Failure of such goals has the potential to halt the entire project and directly affect the company. Medium-ranked goals are crucial to the existence of the project, and their failure may adversely affect many employees and also impact some higher ranked goals. Failure of a lower ranked goal can affect just a small portion of the company's revenue, and the impact may be felt by just a small portion of the company's employees Creating risk management plan's directions, committees, goals, requirements, timeline and scope is required in the beginning. The goal for doing this is to ensure that everyone in thecommittee is aware of his/her responsibility, role, and time. Also, it would make the efforts spend more effectively and directly.

Table 2.Guidelines for business goals rankings

Rank	Definition
High	These goals are critical to the existence of the project (and possibly the company). If not met, there is a real risk that the project will cease to exist and the company will be directly impacted
Medium	These goals are very important for the existence of the project (and possibly the company). A large number of employees may be affected if these goals are not met. A failure to achieve a medium-ranked business goal may result in a negative effect to high-rank goals
Low	These goals affect only a small portion of the company's revenue. A small number.

Table 3. Risk Likelihood value Description

Likelihood Value	Definition
High	The threat is highly motivated and sufficiently capable and controls to prevent the risk from occurring
Medium	The threat is motivated and capable, but controls are in place to impede its successful materialization
Low	The threat lacks motivation or capability or controls are in place to prevent, or at least significantly impede the risk from occurring

6.2 Identify the Business, Technical Risks, and Vulnerability

Business risks can impact business goals. For example, they can affect business reputation, revenue, and productivity. The identification of business risks helps to define and identify the most effective technical and managerial methods for measuring and mitigating these risks. In terms of technical risks, they are hard to find because they are often not actionable. They can be related to a system behaving in an unexpected way, violating its own design structures, or failing to perform as required. When identifying the business and technical risks, three fundamental sources of threats should be taken into account: natural (e.g., floods, earthquakes, tornadoes); human, including unintentional acts and deliberate actions such as network-based attacks; and environmental threats, such as long-term power failures, pollution, chemicals. Also, these sources can be dividing into adversarial incidents and non-adversarial incidents. Adversarial incidents are these initiated by the adversary such as hackers or cyber-criminal organizations, while non adversarial incidents occur due to environmental problems such as earthquakes, floods, system faults, or those initiated unintentionally by operators.

In this stage, technical, management, and operational vulnerability should also be investigated. Applying vulnerability sources, the performance of system security testing, and the development of a security checklists can help identify system weak points. After identifying risks and vulnerability, a ranking of risk indicators, impact of risks, and likelihood of identified risks must be created. Tables 3 shows risk indicators are signs and important tools within operational risk management that can monitor and measure to determine the risk status.

RANK	BUSINESS GOALS	BUSINESS IMPACT
High	These goals are critical to the existence of the project.	Risks will directly impact
Medium	These are important for the existence.	The risk will result in a negatively affect to the high rank goals
Low	High cost on Demand	Support system and finance will be affected directly

Table 3: Risk Indicators and Impacts

6.3 Overall Assessment and Monitoring

After carrying out the required solution, the teams of experts meet to continually evaluate and assess the outcome of the solution. Based on observations, the team decides whether the risk assessment meets the plan or not and what they should do next in each situation. If the assessment meets the plan, they can document the type of attack/threat and the effective solutions. They can then think of solution vulnerabilities and ways to fix them. Besides, alternative solutions can also be devised to increase readiness should the current solution fail for a similar attack. The experts can also evaluate the performance of the solution to see the effectiveness in meeting the goals of the business partners as well as securing the client confidence. If the solution failed, the experts can assess why it failed and develop fixes. They canevaluate the extent of damage and come up with effective ways of counteracting anyaftermath of attacks. They can also develop effective ways of restoring the confidence of their clients should the attack tamper with their data security or privacy information. This team of experts forms the backbone of cloud computing because their innovative thinking does not only provide robust mechanisms for combating known threats but also provides the platform for developing more effective and dynamic RMF. Since humans are potentially the most dangerous potential threat source, a team of humans performing continuous monitoring and creating combat procedures is indispensable to any reliable risk management framework.

7. Conclusion

In recent years, cloud computing has gained much popularity in the IT industry. Cloud computing is a computing resource with deployment and service models that enables users to get computing resources and applications from any location via an Internet connection. The powerful characteristic of cloud computing is that no special devices or software are required for the service. Cloud computing brings us both opportunities and challenges. Reduced coast, speed of deployment, scalability, less requirements for operating IT functions and other environmental benefits, such as less physical space, are among the advantages cloud computing provides. However, a large number of organizations and users in general do not use or adopt this new technology mainly because of security concerns and low trust. To prevent serious problems occurring with security aspect of cloud computing, we provided a risk management framework that can be applied for this purpose. The main goals are to raise trust between providers and users and to increase the number of users and adopters of cloud computing. To accomplish this, this paper has provided a comprehensive cloud computing risk management framework based on previous work.

This risk management framework consists of six stages:(1) understand the business context, (2) identify the business technical risk, (3) synthesize and prioritize the risk, (4) define the risk mitigation strategy, (5) carry out required solutions and validate that they are resolved. The first five steps are the well-known risk management stages, but this research has adopted a more robust approach to each of them. This paper highlights the details of these approaches used in the first five steps as well as the explanation of these steps.

To clarify these steps, a scenario explaining a step-by-step approach to applying this risk management framework to a hypothetical cloud computing provider has been outlined. The advantage of this risk management framework lies in its flexibility because it can fit with small and large enterprises.

References

[1] Qaisar, S., & Khawaja, K. (2012, January). Cloud Computing: Network/Security Threats and Countermeasures. Interdisciplinary Journal of Contemporary Research in Business, 3(9), 1323.

[2]. Cloud-computing Proceedings of The 2014 IAJC/ISAM Joint International Conference ISBN 978-1-60643-379.

[3] Han, Y. (2011, December) Cloud Computing: Case Studies and Total Costs of Ownership. Information Technology and Library, 30(4), 198-206.

[4] Tan, X., & Ai, B. (2011). The Issues of Cloud Computing Security in High-Speed Railway. International Conference on Electronic & Mechanical Engineering and Information Technology. Heilongjiang, China: Harbin.

[5] Lui, W. (2012). Research on Cloud Computing Security Problem and Strategy. 2nd International Conference on_Consumer Electronics, Communications and Networks, 1216-1219.

[6] Jadeja, Y., & Modi, K. (2012). Cloud Computing—Concepts, Architecture and Challenges. International Conference on Computing, Electronics and Electrical Technologies, 877-880.

[7] Claycomb, W., & Nicoll, A. (2013). Insider Threats to Cloud Computing: Directionsfor New Research Challenges. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52379

[8] Hutchings, A., Smith, R., & James, L. (2013). Cloud Computing for Small Business:Criminal and Security Threats and Prevention Measures. Trends & Issues in Crime andCriminal Justice, no. 456. Retrieved from http://www.aic.gov.au/publications/current%20series/tandi/441-460/tandi456.html

[9] Peerson, S., & Yee, G. (eds.). (2012). Privacy and Security for Cloud Computing.London: Springer.

[10] Cloud Security Alliance. (2010, March). Top Threats to Cloud Computing V1.0.Retrieved from https://cloudsecurityalliance.org/topthreats/csathreats.v.10.pdf

[11] Rittinghouse, J. W., & Ransome, J. F. (2010). Cloud Computing Implementation,Management, and Security. Boca Raton, FL: CRC Press.[11] McGraw, G. (2006). Software Security: Building Security In. Upper Saddle River,NJ:Pearson Education, Inc.

[12] Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., & Kanai, A. (2011). Risk Management on the Security Problem in Cloud Computing. First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering, 147-152.

[13] Xie, F., Peng, Y., Zhao, W., Chen, D., Wang, X., & Huo, X. (2012). A Risk Management Framework for Cloud Computing. IEEE 2nd International Conference on Cloud Computing and Intelligent Systems, 1, 476-480.

[14] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G.,Patterson, D., Rabkin, A., Stoica., I., & Zaharia, M (2010). A View of Cloud Computing. Communications of the ACM, 53(4),50-58.

Contact Address

M. Satheesh

Assistant Professor,

Department of Computer Science,

Don Bosco college of Arts and Science,

Karaikal – 609601. - 9442310791