Cloud Security Risk Assessment using FAIR

[1]Ishan Rastogi, [2]Adesh Chandra, [3]Anurag Singh
[1,2,3]Dept. of Cyber Law and Information Security, IIIT Allahabad, India

Abstract
Cloud computing is a very powerful concept but with it comes various security scares which are enough to keep most of the perspective users at bay.This paper tries to calculate the additional risk which an organization might have to face when shifting to cloud computing, by performing cloud security risk assessment using the FAIR model.

Keywords
Cloud Computing, Security, FAIR, Risk Assessment, Risk, Impact

I. Introduction

Cloud computing is the next step in the evolution of computing. It aims at delivering computing resources as a service over a network by using virtualization and distributed computing techniques, thus providing computation power to the users at low costs by employing a pay as you go model for bill payment, i.e., a user pays only for the resources she has used.

As stated above cloud computing is based on distributed computing in which the data is decentralized and any computation performed is done by many different computer systems simultaneously and not by a single computer, thus enhancing the efficiency by reducing the computation time. Because of having distributed computing as its base, cloud computing is scalable, i.e., at any given time any user can utilize more resources than she initially asked for without worrying about losing business because of increased needs and can later simply pay for the additional resources used.

Three major services which are delivered using cloud computing are:Software-as-a-Service (SaaS), Platform-as-a-Service (Paas) and Infrastructure-as-a-Service (IaaS).

Cloud based on the type of providers can also be divided into public cloud, private cloud and hybrid cloud.

Delivery of services means that user data is stored in the cloud and is not in the control of the user which raises security concerns. The flexibility, distributed nature and the economy of scale though are useful; these features have also made cloud computing riskier. The huge amount of data and resources available in the cloud has made it a gold mine for hackers, who try to get their hands on any piece of important data, or on the resources themselves. Therefore, there is a need to perform cloud computing security risk assessment. In this paper we try to calculate the additional risk which gets introduced when an organization decides to use cloud computing, by performing cloud security risk assessment by using a risk assessment framework known as Factor Analysis of Information Risk (FAIR).

The remaining paper is organized as follows.We first provide a list of the most important risks related to cloud computing. We then provide a brief explanation of the FAIR model.We then use the FAIR model to assess the risk. The conclusion and references are then provided.

II. Top Cloud Computing Security Risks

The security risks which are associated with cloud computing have forced many people to stay clear from it. The major cloud computing security risks accounted in this paper are:

A. Loss of Governance

since all the data is with the cloud provider and SLAs may not cover all the points, a client may feel lack of control over her data.

B. Lock-in

The lack of current availability of portability may cause difficulties to users who wish to migrate to different cloud provider, or bring the entire data back to in-house environment, or outsource the services to a third-party.

C. Isolation Failure

Multi-tenancy and resource sharing may cause security concerns to the user if the isolation mechanisms are not appropriate.

D. Compliance Risks

An organization may lose some of its security certifications if it decides to migrate to cloud.

E. Interface Compromise

Since the management interfaces provided by a public cloud provider are accessible over the internet, they also pose serious security risks.

F. Data Protection

The cloud computing setup makes it difficult for any client to monitor the handling of her data by the cloud provider and to ensure that the data is being handled in an ethical and lawful manner.

G. Data Deletion

Since the data in a cloud computing environment is decentralized, any request made to delete a particular resource may not result in complete deletion of data. Proper deletion may also not be possible, either because the stored backup of data is not available, or because the disk which is to be destroyed contains data from other users as well.

H. Malicious Insider

The damage which can be caused by a malicious insider occupying a high-risk role viz. system administrator can have much more impact on an organization.

It is sometimes advised thatthe cloud client should transfer the information risks to the cloud service provider [1].

III. Factor Analysis of Information Risk

FAIR provides a logical and reasoned framework to understand, analyse and measure risks associated to information security. It utilizes both quantitative and qualitative techniques for risk calculation. FAIR provides taxonomy of all those factors which constitute information risk which helps to have a basic understanding of information risk. It provides a method for the measurement of the factors which drive information risk. It provides a computational engine that mathematically simulates the relationship between all the measured factors. It also provides a simulation model that allows for the application of the taxonomy, the measurement model, and the computational engine to analyse the risk.

FAIR provides various benefits in the process of risk assessment. It helps in better understanding of the problem space. It helps in promoting thorough and consistent analysis. It provides a metrics and data analysis framework. Using a proper risk assessment framework (such as FAIR)helps in increasing credibility of the organization with the stake-holders. Also, the risk calculated using FAIR helps in promoting well-informed decision making.

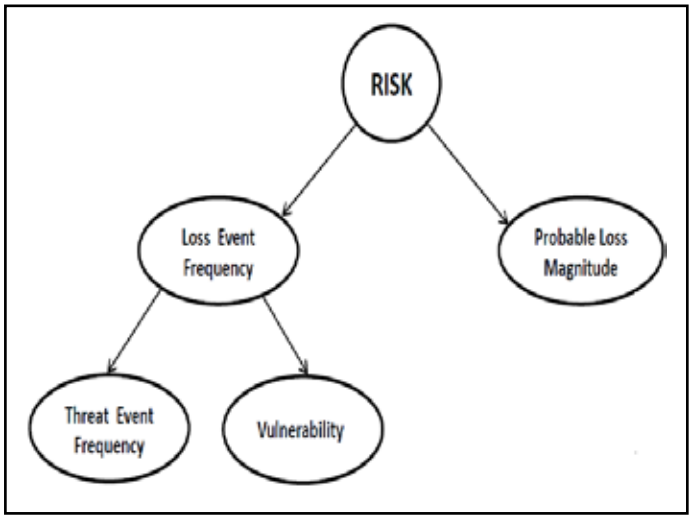

Fig. 1: FAIR Risk Decomposition

Fig. 1 shows how FAIR model decomposes risk into its constituent factors. FAIR model provides the following definitions for risk and itsdriving factors:

A. Risk

FAIR model defines risk as a combined effect of probable frequency with the probable magnitude of the losses which the might occur if the risk leads to some damage.

B. Loss Event Frequency (LEF)

LEF gives the probable frequency of a threat agent inflicting harm upon an asset during a particular time period.

C. Threat Event Frequency (TEF)

TEF gives the probable frequency of a threat agent acting against an asset during a given time period. FAIR has provided the following table to precisely measure TEF.

Table 1: Rating for TEF

Rating	Description
VH	>100 events per year
H	10-100 events per year
M	1-10 events per year
L	.1-1 events per year
VL	<.1 events per year

TEF can itself be decomposed into two factors namely contact and action.

D. Contact

It gives the probable frequency of a threat agent coming in contact with an asset during a given time period. Contact can be of three types: random, regular and intentional.

E. Action

It gives the probability of a threat agent acting against an asset in case contact occurs.

F. Vulnerability

It gives the probability of an asset being unable in resisting in the actions of a threat agent. Vulnerability can be decomposed into two factors namely threat capability and control strength.

G. Threat Capability (TCap)

It gives the probable capability of a threat agent, i.e., the level of force with which a threat agent can act against an asset.
FAIR uses the following scale to measure the threat capability.

Table 2: Rating for TCap

Rating	Description
VH	Top 2% of all the threat population
H	Top 16% of all the threat population
M	Average
L	Bottom 16% of all the threat population
VL	Bottom 2% of all the threat population

H. Control Strength (CS)

It gives the strength of the controls applied against the baseline value of force. FAIR calculates CS indirectly using TCap as reference.

Table 3: Rating for Control strength

Rating	Description
VH	Fails only against top 2% of all the threat population
H	Fails only against top 16% of all the threat population
M	Protects against average threats
L	Protects only against bottom 16% of all the threat population
VL	Protects only against bottom 2% of all the threat population

I. Probable Loss Magnitude (PLM)

PLM describes the factors that drive magnitude of loss in case of occurrence of an event. Calculating the probable loss magnitude is difficult because of many reasons including:

- Calculating the exact value of assets at risk is not easy.
- Assets usually can have multiple liability characteristics.
- Loss can be of multiple forms.
- A single security event may result in many different forms of losses.
- Various complex relationships may exist between various forms of losses.
- Loss magnitude is determined by many different factors.

Difficulty in calculating loss magnitude is increased even more by the fact that in information risk environment enough good data about loss magnitude is not available.

J. FAIR has Identified Six Forms of Loss Namely

Productivity, response, replacement, reputation, competitive advantage and, fines and judgements. FAIR uses the following scale to roughly measure loss magnitude.

Table 4: Measure due to Magnitude of Probable Loss

Magnitude	Probable Loss
SV	>$10,000,000
H	$1,000,000- $9,999,999
Sg	$100,000- $999,999
M	$10,000- $99,999
L	$1,000- $9,999
VL	<$1,000

This scale, however, is flexible.
Organizations of different sizesmay have differentcapacity of bearing losses [2].

IV. Risk Measurement

A. Risk 1: Lock-In

Currently there is a lack of mechanisms which could provide data and service portability making it difficult for a customer to migrate to different cloud provider, or bring the entire data back to in-house environment. This dependency may lead to severe business failure in case the cloud provider goes out of business without sufficient warning. Different cloud types have different natures and extent of lock-in.

1. SaaS Lock-in

Customer data is stored in a database at the SaaS provider. SaaS providers generally provide customers with features to read the data, but do not provide features to export the data and the customers need to develop their own modules to extract the data and write it to a file which is ready for import at another provider. Most common form of lock-in in the SaaS environment is the application lock-in. Customers will have to develop new programs to interact with the provider's APIs and also SaaS customers who have a large user-base will face high switching costs as the end-user experience gets impacted.

2. PaaS Lock-in

PaaS Lock-in can occur at both the API layer,as well as, the component layer. Code developed by the customer for a particular provider will not necessarily work at a different provider because of difference in API offered and the data access model.PaaS lock-in generally happens at the runtime layer. Similar to SaaS, PaaS also suffers from data lock-in, but here it is the responsibility of the customer to develop compatible export routines.

3. IaaS Lock-in

Migration between different IaaS providers will remain a non-trivial issue until some open standard is adopted. Just like SaaS and Paas, IaaS too suffers from data lock-in. As more and more data gets pushed to the cloud, data lock-in is bound to increase until cloud providers do not provide some mechanisms for portability. With the above understanding we can estimate this risk as:

Table 5: Risk Due to Lock in

Lock-in	
TEF	Moderate
TCap	High
CS	Low
Vulnerabilities	Lack of standard mechanisms, Incomplete and non-transparent terms of use, Misjudgement in selection of the provider
Vulnerability	Very High
LEF	Moderate
Drivers of Loss Magnitude	Company Reputation, Sensitive Personal Data, Personal Data, Critical Personal Data, Real-time Service Delivery, Service Delivery
PLM	SaaS: Significant PaaS: High IaaS: Severe
Risk	SaaS: High PaaS: High IaaS: Critical

B. Risk 2: Loss of Governance

In a cloud infrastructure, since all the data is with the cloud provider and SLAs may not cover all the points, a client may feel lack of control over her data. The cloud provider could also outsource the services to a third-party which might not offer similar guarantees regarding the user data. Thus loss of governance could have a catastrophic impact on the business goals and strategies of an organization.

Table 6: Risk Due to Loss of Governance

Loss of Governance	
TEF	Very High
TCap	High
CS	Low
Vulnerabilities	Lack of clarity of roles and responsibilities, non-clear ownership of assets, no vulnerability assessment process, no certification schemes, audit not available to customers, conflicting promises in SLAs, lack of jurisdiction, hidden dependency created by cross-cloud applications
Vulnerability	Very High
LEF	Very High
Drivers of Loss Magnitude	Reputation of company, trust of customers, loyalty and experience of employees, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery.

PLM	SaaS: Low PaaS: Significant IaaS: Severe
Risk	SaaS: Medium Paas: Critical IaaS: Critical

C. Risk 3: Compliance Challenges

Many organizations spend considerable amount of money for achieving certain certifications. Those certifications can be put to risk by migrating to cloud if the cloud provider does not have evidence of itself being compliant to the requirements, or if the cloud provider does not allow the auditing by the certifying authority. In some cases the compliance cannot be achieved because of the cloud infrastructure and thus cannot be used to perform services where certification is mandatory.

Table 7: Risk due to Compliance Challenges

Compliance Challenges	
TEF	High
TCap	High
CS	Low
Vulnerabilities	Certification and audit not made available to the customers, lack of standard solutions, certification schemes not available for cloud infrastructures, lack of jurisdictions, incomplete and non-transparent terms of use
Vulnerability	Very High
LEF	High
Drivers of Loss Magnitude	Certification, reputation, competitive advantage
PLM	IaaS: Significant
Risk	IaaS: High

D. Risk 4: Business Reputation Loss Because ofCo-Tenant Activities

Table 8: Risk due to Business Reputation Loss Because of Co-Tenant Activities

Co-Tenant Activities	
TEF	Low
TCap	Moderate
CS	Moderate
Vulnerabilities	Failure of resource isolation, vulnerabilities of the hypervisor, failure of reputational isolation
Vulnerability	Moderate
LEF	Low
Drivers of Loss Magnitude	Reputation of company, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery
PLM	Moderate
Risk	Moderate

E. Risk 5: Failure or Termination of Cloud Services

Table 9: Risk due to Failure or Termination of Cloud Services

Failure or Termination of cloud services	
TEF	Very Low
TCap	Very High
CS	Low
Vulnerabilities	Misjudgement in the selection of cloud provider, lack of or improper supplier redundancy, incomplete and non-transparent terms of use
Vulnerability	Very High
LEF	Very Low
Drivers of Loss Magnitude	Reputation of the company, trust in the company, loyalty and experience of the employees, service delivery, real-time service delivery
PLM	Severe
Risk	High

F. Risk 6: Acquisition of the Cloud Provider

Table 10: Risk due to Acquisition of the Cloud Provider

Cloud Provider Acquisition	
TEF	Very Low
TCap	Low
CS	Moderate
Vulnerabilities	Incomplete and non-transparent terms of use
Vulnerability	Low
LEF	Very Low
Drivers of Loss Magnitude	Reputation of the company, trust in the company, loyalty and experience of the employees, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery, HR data, intellectual property
PLM	Moderate
Risk	Low

G. Risk 7: Supply Chain Failure

Table 11: Risk due to Supply Chain Failure

Supply Chain Failure	
TEF	Very Low
TCap	Moderate
CS	Moderate
Vulnerabilities	Hidden dependency created by cross-cloud applications, misjudgement in the selection of provider, incomplete and non-transparent terms of use, lack of or improper supplier redundancy
Vulnerability	Moderate
LEF	Very Low

Drivers of Loss Magnitude	Reputation of the company, trust in the company, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery
PLM	Significant
Risk	Medium

H. Risk 8: Exhaustion of Resources

Being an on-demand service, there is a risk involved in allocating all the available resources of a cloud service. Resources are allocated based on some statistical projections and the inaccurate modelling of resource utilization may result in.

1. Service Unavailability

The services are either not available or their performance is degraded.

2. Compromise of Access Control System

This puts both the confidentiality and integrity of data at risk. Economic losses and loss of Reputation: this might occur as a result of not being able to meet the demands of the users, violation of some clauses of SLA etc.

Table 12: Risk due to Exhaustion of Resources

Exhaustion of Resources	
TEF	Inability to provide additional resources: Moderate Inability to provide agreed upon capacity level: Low
TCap	Moderate
CS	Low
Vulnerabilities	Inaccurate modelling of resource utilization and allocation, inadequate resource provisioning and deprovisioning, inadequate investments in infrastructure, no policy defining the maximum resources which can be allocated, lack of or improper supplier redundancy
Vulnerability	High
LEF	Inability to provide additional resources: Moderate Inability to provide agreed upon capacity level: Low
Drivers of Loss Magnitude	Reputation of the company, trust in the company, service delivery, access control
PLM	Inability to provide additional resources: Moderate Inability to provide agreed upon capacity level: Significant
Risk	Inability to provide additional resources: Medium Inability to provide agreed upon capacity level: Medium

I. Risk 9: Isolation Failure

Multi-tenancy and resource sharing may cause security concerns to the user if the isolation mechanisms are not appropriate.

Table 13: Risk due to Isolation Failure

Isolation Failure	
TEF	Moderate
TCap	High
CS	Low
Vulnerabilities	Vulnerabilities of the hypervisor, lack of or improper isolation, failure of reputational isolation
Vulnerability	Very High
LEF	Moderate
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery
PLM	Significant
Risk	High

J. Risk 10: Malicious Insider at the Cloud Provider

The activities of a malicious insider might have a potential impact on the confidentiality of the data, intellectual property, services, and alsoon their integrity availability. The necessity of high-risk roles in cloud infrastructure increases the probability of such kind of malicious activities. Roles such as cloud provider's system administrator, auditor, manager etc. are all examples of such high-risk roles.

Table 14: Risk due to Malicious Insider at the Cloud Provider

Malicious Insider	
TEF	Moderate
TCap	High
CS	Low
Vulnerabilities	Improper segregation of duties, non-implementation of need-to-know principle, AAA vulnerabilities, improper implementation of roles, vulnerabilities of the system, inadequate and improper measures for physical security, vulnerabilities of the application.
Vulnerability	Very High
LEF	Moderate
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, loyalty and experience of the employees, intellectual property, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery, HR data
PLM	Significant
Risk	High

K. Risk 11: Compromise of Management Interface

Since the management interfaces provided by a public cloud provider are accessible over the internet, they also pose serious security risks.

Table 15: Risk due to Compromise of Management Interface

Management Interface Compromise	
TEF	Moderate
TCap	Moderate
CS	Moderate
Vulnerabilities	Improper configuration, AAA vulnerabilities, vulnerabilities of the system, vulnerabilities of the application, remote access to the management interface
Vulnerability	Moderate
LEF	Moderate
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery, management interface of the cloud service
PLM	Moderate
Risk	Medium

L. Risk 12: Interception of the Data in Transit

Table 16: Risk due to Interception of the Data in Transit

Interception of data in transit	
TEF	Moderate
TCap	Moderate
CS	Moderate
Vulnerabilities	Vulnerabilities in the encryption, AAA vulnerabilities, incomplete and non-transparent terms of use, improper encryption of archives
Vulnerability	Moderate
LEF	Moderate
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, personal data, sensitive personal data, intellectual property, service delivery, real-time service delivery, HR data, critical personal data, archive or back-up data
PLM	Moderate
Risk	Medium

M. Risk 13: Data Leakage on Upload or Download

Table 17: Risk due to Data Leakage

Data Leakage	
TEF	Moderate
TCap	Moderate
CS	Moderate
Vulnerabilities	Vulnerabilities in the encryption, AAA vulnerabilities, incomplete and non-transparent terms of use, improper encryption of archives
Vulnerability	Moderate
LEF	Moderate
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, personal data, sensitive personal data, intellectual property, service delivery, real-time service delivery, HR data, critical personal data, archive or back-up data
PLM	Moderate
Risk	Medium

N. Risk 14: Insecure Data Deletion

Since the data in a cloud computing environment is decentralized, any request made to delete a particular resource may not result in complete deletion of data. Proper deletion may also not be possible, either because the stored backup of data is not available, or because the disk which is to be destroyed contains data from other users as well.

Table 18: Risk due to Insecure Data Deletion

Insecure Data Deletion	
TEF	Moderate
TCap	Moderate
CS	Low
Vulnerabilities	Improper media sanitization
Vulnerability	High
LEF	Moderate
Drivers of Loss Magnitude	Credentials, personal data, critical personal data, sensitive personal data
PLM	Moderate
Risk	Medium

O. Risk 15: Distributed Denial of Service

Table 19: Risk due to Distributed Denial of Service

DDoS	
TEF	Customer: Moderate Provider: Low
TCap	High
CS	Low
Vulnerabilities	Improper configuration, vulnerabilities of the system, improperly configured or inadequate traffic filtering resources
Vulnerability	Very High
LEF	Customer: Moderate Provider: Low
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, service delivery, real-time service delivery, network, management interface of cloud services
PLM	Customer: Significant Provider: High
Risk	Customer: High Provider: High

P. Risk 16: Economic Denial of Service

Table 20: Risk due to Economic Denial of Service

EDOS	
TEF	Low
TCap	Moderate
CS	Moderate
Vulnerabilities	AAA vulnerabilities, vulnerabilities in user provisioning and deprovisioning, no policy defining the maximum resources which can be allocated, remote access to the service management interface
Vulnerability	Moderate
LEF	Low
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, service delivery, real-time service delivery
PLM	Moderate
Risk	Medium

Q. Risk 17: Loss of the Encryption Keys

Table 21: Risk due to Loss of the Encryption Keys

Loss of encryption keys	
TEF	Low
TCap	Moderate
CS	Moderate
Vulnerabilities	Poor management of keys, poor key generation techniques
Vulnerability	Moderate
LEF	Low
Drivers of Loss Magnitude	Credential, personal data, sensitive personal data, critical personal data, intellectual property, HR data
PLM	Significant
Risk	Medium

R. Risk 18: Undertaking Malicious Probes

Table 22: Risk due to Malicious Probes or Scans

Malicious Probes or Scans	
TEF	Moderate
TCap	Low
CS	Moderate
Vulnerabilities	Possibility of internal probing
Vulnerability	Low
LEF	Low
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, service delivery, real-time service delivery
PLM	Moderate
Risk	Medium

S. Risk 19: Compromised Service Engine

Table 23: Risk due to Compromised Service Engine

Compromise Service Engine	
TEF	Low
TCap	Moderate
CS	Moderate
Vulnerabilities	Vulnerabilities of the hypervisor, improper isolation of resources
Vulnerability	Moderate
LEF	Low
Drivers of Loss Magnitude	HR data, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery
PLM	Moderate
Risk	Medium

T. Risk 20: Conflicts between the hardening procedures being applied by the customer and the cloud environment

Table 24: Risk Due to Conflicts

Conflicts	
TEF	Low
TCap	Low
CS	Low
Vulnerabilities	Incomplete and non-transparent terms of use, improper distribution of roles and responsibilities, conflicting clauses in SLA
Vulnerability	Moderate
LEF	Low
Drivers of Loss Magnitude	Personal data, sensitive personal data, critical personal data, intellectual property
PLM	Moderate
Risk	Medium

U. Risk 21: Subpoena and E-Discovery

Table 25: Risk due to Subpoena and E-discovery

Subpoena and E-discovery	
TEF	High
TCap	High
CS	Low
Vulnerabilities	Improper resource isolation, lack of proper information regarding jurisdictions, storing of data under multiple jurisdictions
Vulnerability	Very High
LEF	High

Drivers of Loss Magnitude	Reputation of the company, trust of the customer, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery
PLM	High
Risk	High

V. Risk 22: Change of Jurisdiction

Table 26: Risk due to Change of Jurisdiction

Change of Jurisdiction	
TEF	Very High
TCap	High
CS	Low
Vulnerabilities	Lack of proper information regarding jurisdictions, storing of data under multiple jurisdictions
Vulnerability	Very High
LEF	Very High
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, personal data, sensitive personal, critical personal data, service delivery, real-time service delivery
PLM	Significant
Risk	Critical

W. Risk 23: Data Protection Risks

Table 27: Risk due to Data Protection Risks

Data Protection Risks	
TEF	High
TCap	High
CS	Low
Vulnerabilities	Lack of proper information regarding jurisdictions, storing of data under multiple jurisdictions
Vulnerability	Very High
LEF	High
Drivers of Loss Magnitude	Reputation of the company, trust of the customer, personal data, sensitive personal data, critical personal data, service delivery, real-time service delivery
PLM	Significant
Risk	High

X. Risk 24: Risks in Licensing

Table 28: Risk due to Licensing

Licensing Risk	
TEF	Moderate
TCap	Low
CS	Moderate
Vulnerabilities	Incomplete and non-transparent terms of use
Vulnerability	Low
LEF	Low
Drivers of Loss Magnitude	Reputation of the company, certifications, real-time service delivery
PLM	Moderate
Risk	Medium

V. Conclusion

In this paper, we have tried to calculate all the additional risks which an organization may face when opting for a cloud solution. From the above calculations it is quite evident that cloud services though very useful come with significant risks and therefore the decision to move to cloud should be a well-thought and strategized one.The risk values calculated by us in this paper are in no way uniform, and might not be directly applicable for every organization.

References

[1] ENISA Report on Cloud Computing Security Risk Assessment, [Online] Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (accessed on December 10th, 2012.)

[2] Jack A. Jones,"An Introduction to Factor Analysis of Information Risk (FAIR)", CISSP, CISM, CISA

IshanRastogi, He completed his B.Tech in Computer Science and Engineering from Jaypee Institute of Information Technology, Noida in 2011. He is currently pursuing M.S in Cyber Law and Information Security from Indian Institute of Information Technology, Allahabad.

He is an EC Council – Certified Ethical Hacker v6, a CISCO Certified Network Associate and Microsoft Certified Professional. He secured 10th Rank in ACM ICPC – Kanpur Gwalior Regionals 2009.His area of interest is Cloud Computing, Cryptography and Cyber Forensics.

Adesh Chandra, He completed his B.Tech in Information Technology from Dr. K. N. Modi Institute of Engineering and Technology, Ghaziabad in 2011. He is currently pursuing M.S in Cyber Law and Information Security from Indian Institute of Information Technology, Allahabad. His Area of interest are Risk management, ITIL and Computer networks.

Anurag Singh, He completed his B.Techin Information Technology from Dr. Ram ManoharLohiaAvadh University Faizabad in 2011. He is currently pursuing M.S in Cyber Law and Information Security from Indian Institute of Information Technology, Allahabad. His Area of interest are Risk management, ISO, PCI-DSS & Knowledgebase.