A Study of Risk Management in Cloud Computing

CSE 543: Information Assurance and Security

Group Project Report – Group 8

School of Computing, Informatics, Decision Systems Engineering (CIDSE)

Arizona State University

Tempe, Arizona

Authors:

Abhishek Rayasam Venkata
Graduate Student, CIDSE

Chintan Khatri
Graduate Student, CIDSE

Rohith Honnenahalli Yogesh
Graduate Student, CIDSE

Ami Vashi
Graduate Student, CIDSE

Jason Dsouza
Graduate Student, CIDSE

Roshan Prabakar Raj
Graduate Student, CIDSE

Anand Ganesh
Graduate Student, CIDSE

Jundong Li
Graduate Student, CIDSE

Sudhashree Gholkar
Graduate Student, CIDSE

Anoop Sahoo
Graduate Student, CIDSE

ARIZONA STATE UNIVERSITY

Summary: Risk Management is an integral part of any decision making process; to assess and contemplate whether a decision or a system is feasible or not can greatly reduce negative consequences of bad decisions by mitigating risks. It primarily involves three major processes: identification, assessment and prioritization of the risk involved in a process. In cloud computing, risk management can be categorically divided by its approach. We assess the various risks faced by a cloud computing system and the prioritization of risks depending on the approach and contrast their pros and cons.

TABLE OF CONTENT

1. Abstract

The study deals with the different risks associated with cloud computing. All these risks are described in detail and ways to mitigate them are also discussed. The pros and cons, strengths and weaknesses of each strategy is highlighted. The risks are broadly divided into five categories namely environmental risks, data privacy, security, availability and capacity limitation and business continuity. These risks encompass all the major threats and vulnerabilities of a cloud environment. By looking into these risks, it is possible to avoid any kind of malicious attacks or disasters that may occur.

2. Introduction

2.1. Motivation and Background

Motivation:

Cloud Computing Services are now used by all kinds of businesses, companies as well as individual end-users today. It gives an opportunity to small business owners to harness the computing power without having to spend exorbitant amounts of money. The usage of cloud computing resources being so high, the security, protection and timely availability of the users' data is of utmost importance. A sizeable chunk of cloud computing security involves the assessment and management of risks involved in the all facets of cloud services. Risk management basically aims to eliminate the factors that may in the future prove to be a hindrance in achieving the desired results. If risks are not assessed and managed in a timely manner then it could lead to dire consequences. Without proper and thorough risk analysis and management, the occurrence of a rare or unanticipated risk leads to failure of the entire operation like the service being inaccessible for long periods of time. We realize that risk management is a huge part of ensuring that cloud services are efficiently delivered to the users, this motivates us to study Risk Management in Cloud Computing and gain an in depth knowledge about the existing practices in the industry. Researching the various categories of risks and management strategies gives us a chance to analyze it in explicit detail, so that we can extract advantages and disadvantages of the existing scenario in the industry. By studying advantages and disadvantages, we are able to suggest where improvements need to be made and highlight the areas where holes exist that give rise to opportunities for getting into the system and exploit valuable information for malicious purposes. We also think it is important to research innovative ways that are still in experimental phases and need fine tuning before they can be used in the real world.

Background:

Cloud computing is a service based architecture which provides computing services (Software, Platform and Infrastructure) as a utility. As part of our study, we concentrate on risk management in cloud

computing. The massive scale of cloud computing exposes it to numerous threats and risks from security perspective. To detect, avoid and manage these risks, we perform a deep study into the various risks and vulnerabilities of Environmental Security, Data privacy, Security, Availability and capacity limitation, and Business continuity in cloud computing. We describe case studies falling under different categories of cloud computing and how these case studies impact the future of security and risk management in cloud computing.

2.2. Goals and scope of study

Goals:

- To gain theoretical and implementation knowledge of risk management in cloud computing.
- Analyze specific traits and scenarios that govern the implementation details such as Environmental Security, Data Privacy and Security in Cloud computing, Business continuity, Capacity limitation and availability.
- Summarize the gathered traits to guide in the process of risk management.
- Provide recommendation if any for the any future possibilities

Scope:

The scope of our report involves study of the different risks involved in the cloud infrastructure and ways to mitigate them.

Risks in our study are classified into the following 5 categories.

- Risk Management involved in Environmental Security of Cloud
- Risk management related to Data Privacy
- Risk Management for Business Continuity
- Risk Management related to Availability and Capacity Limitation
- Risk Management about Security in Cloud Computing

We also include existing vulnerabilities and threats in the cloud environment. We focus on techniques of handling the risks that are in practice in today's scenario of cloud services. The strategies that are in place to deal with risks and also the deficiencies that exist are studied in depth according to the categories mentioned above. Attacks that have been successful and attacks that have been successfully deflected are also studied in detail. Any future scope for improvements in documented and pros and cons of existing strategies are mentioned.

3. Overview

We have discussed the risk analysis, detection and management in cloud computing in following domains.

3.1. Environmental risk mitigation in Cloud Computing

When we talk about environmental risks in cloud computing, we primarily talk about the virtual environment of cloud. There are various factors in cloud environment that can lead to a potential risk. There can be risks related to secure saving of images of virtual machines in a repository. There will also be risk involved when we talk about the maintenance of the cloud environment. As a part of this study, we have also referred to a case study and have learnt how to mitigate risks that may crop up when using vendor cloud environment. In addition, we also study the data security and privacy protection issues in the cloud computing environment. Moreover, we also survey security issues in different layers of cloud computing system.

Abhishek:

As part of our study, we have looked into securely managing virtual machines. Securely managing virtual machines (VM) and their images that encapsulate applications in the cloud. The images should have high integrity because initial state of the VM in the cloud is created and determined by a pre-existing image. We have also looked into a case study of an environmental risk. Through the case study, we have understood about what the risks are involved in the environment in cloud services. We have also looked into a few steps to mitigate the risks.

Jundong:

We investigate several challenges that are present in the cloud computing environment from the risk management perspective. In addition, we study the data security and privacy protection issues in the cloud computing environment. We find that the security and protection issues exist in all stages of the data cycle. At last, we survey some security issues in service delivery models. Specifically, we focus on security issues of risk management in SaaS, PaaS and IaaS.

3.2. Data privacy in Cloud Computing

Data Privacy is a critical component of cloud risk management. Preserving an individual's personally identifiable information on the cloud is very important as it is on untrusted domains away from the personal data centers. Such an environment exposes it to a lot of risks from different parties. There are also different strategies to manage these risks and they have been described.

Rohith:

The study highlights the key risks to data privacy and techniques to mitigate or avoid them. Few of the risks described are external attacks to private data, data misuse by cloud service provider, data transmission across different secure and insecure domains, accountability of user data privacy by cloud service providers, resolving users that are allowed to access content and interacting with third parties using the user data. Then, there are the different techniques available to manage these risks. ORAM technology, Deduplication technology, making use of third party auditing, guidelines when choosing a cloud service, data encryption strategies, utilization of standardized privacy protection solutions, deciding upon clear contracts for accountability with the cloud service provider itself, using a privacy manager to assist privacy management, and the importance of privacy impact assessments while opting for a cloud solution.

Anand:

This study focuses on a privacy centric approach of data in managing risks in cloud systems as a design principle, the feasibility of such a design, its advantages using a benchmark to evaluate performance and finally discuss about a particular implemented model of Risk management in cloud computing with a privacy manager and security of data. The study covers in detail the trade-off between encryption techniques, their space-time complexity and the level of confidentiality it offers. In addition to this study illustrates the working of an Intelligent cloud track which performs Risk Analysis and a privacy data management in cloud computing.

3.3. Security in Cloud Computing

Security in Cloud computing is very prone to risk since the infrastructure , platform and software services are provided by a 3rd party provider, which will be shared by various other customers, making it prone to vulnerability risk. We have discussed several security risks, analyzed those risks and managed them by introducing and discussing various frameworks to manage those risks.

Jason:

I contributed by analyzing Risk in Mobile cloud computing, discussing how there are no standard guidelines surrounding security from threat in Mobile phone which can lead to breach of data transmitted through mobile network. We also discussed approaches to mitigate these risks like antivirus for phones etc. Further, we discussed risk management approaches to security in cloud computing like IAM aka identity and access management, SLA aka service level agreement and TCCP aka trusted cloud computing platform.

Sudhashree:

Studied the main security challenges which include Authentication and Identity Management, Access Control and Accounting, Trust Management and Policy Integration, Secure-Service Management, Privacy and Data Protection, Organizational Security Management. Analysed the Risk management framework which is one of the most efficient security assessment tool to reduce threats, vulnerabilities and security risks. The framework consists processes such as security risks identification, risk analysis, assessment, mitigation and Risks management review which are effective for Risk analysis, detection and management in security in cloud computing.

3.4. Availability and Capacity Limitation in Cloud Computing

Users tend to quality of a cloud in terms of how fast the services are and are the services available to them whenever required. For corporations and small businesses, it is important to them how much capacity can they exploit at a given time. Therefore it is important to study risks involved in availability and capacity limitation. Different services require different capacity requirements, so the risks of any particular service should be customized according to the kind of requirement they have. A general approach cannot be designed to handle the capacity limitation risks of all cloud computing services. For instance a cloud service providing software as a service will require a different set of capacity parameters and platform as a service will require a whole other set.

As for availability, all cloud services need to be available to the user at all times. If at all there needs to be downtime it should not be for extensive periods of time. Also the downtime should be scheduled strategically so that it takes place when the service is not used by a lot of users. Also backup systems should be deployed immediately in times of emergencies so as to ensure customer satisfaction.

Ami Vashi:

Studied practices on capacity limitation and issues faced by major cloud service providers due to availability and capacity hazards. Major papers cover issues that were faced in the past due to various factors influencing the availability of the services. Mainly due to technical emergencies and natural disasters, how they were mitigated and how they can be prevented in the future.

Chintan:

Studied by understanding about the security concerns in cloud computing. Researched papers and articles that focus on availability of cloud computing and capacity limitation. Reviewed, studied and summarized the techniques to improve availability of cloud computing services. The content mainly pertains to Load Balancing and HAIL Protocol. Load balancing is a critical component of cloud computing (described how it helps to improve availability) and HAIL protocol (how it helps in ensuring data integrity and availability).

3.5 Business Continuity in Cloud services

Many companies nowadays want their data to be very secure and available all the time and they simultaneously want to implement new technologies as well. This is a very difficult scenario. This problem can be overcome by implementing cloud and including the continuity services in it. Cloud computing mainly relies on hardware-independent virtualization technology, the companies are allowed to quickly back up data and the applications to the cloud. There are mainly 2 main services associated with the term Risk in cloud computing. The two services are business continuity and disaster recovery.

Anoop:

Even in the worst case scenario such as Tsunami and other natural disaster the organization must be very sure that there is no loss of data which is very critical. So, the organizations implement the 2 services in order to secure the data. By the power of virtualization technology we can easily make sure that there is no loss.

Roshan:

We have started by understanding how the automation and configuration of virtual business is done. Researched through a no. of papers and understood how the virtual business is implemented and also how the delivery of services is done .Studied about the virtualization technology in business continuity and understood in detail with the help of Xenserver. Studied in detail about the cloud service orchestration.

4. Detailed results of all individual members

What are risks?

Risk is a chance of occurrence of something that is undesirable and harmful. Occurrence of risk in any system is always a possibility. To assume that our system is “perfect” and that there is no possible way of a risk damaging the system is not a good practice, in fact it is irresponsible. Risk finds its way in almost all the possible industries, be it Finance, Construction, Medicine, Business or Technology.

What is Risk Management?

Risk management involves identification, assessment and prioritization of risks (defined by ISO 31000). After a detailed compilation of risks is completed, the next step is to find ways to monitor the situation for occurrence of risks, and try to minimize or control the possibility of risks.

This entire process is as important as the actual creation of a particular product or system. It plays a huge role in increasing the longevity of the product and improves sustainability.

Security in Cloud Computing

Security in cloud computing - Cloud computing provides solutions to a lot of IT problems and it is one of the foremost needs of today. But it is relatively weak when it comes to security. Mainly because the focus has always been on implementing new and improved services, that security has taken a back seat. This paper however emphasizes how it’s important to have security in cloud computing and how risks should be analyzed and mitigated so that we can have better control over the cloud services.

Immediate and efficient protocols need to be set so that if and when a risk occurs, it can be handled appropriately.

How to tackle Risk Management?

The foundation that cloud computing is built upon is virtual technology. All the operations and services of the cloud take place by exploiting virtual technologies. The general user does not fully understand what is virtualization and virtual technology. This makes them constantly doubt the security of their data on the cloud.

We divide Risk Management in Cloud Computing Services into broad areas of concerns. These areas are discussed in detail in the following sections of the report.

4.1. Environmental risks in Cloud computing.

4.1.1 Risk Management in Cloud Computing Environment

Managing Security of virtual machine images in a cloud environment [5]

Securely managing virtual machines (VM) and their images that encapsulate applications in the cloud. The images should have high integrity because initial state of the VM in the cloud is created and determined by a pre-existing image. A few images are also provided by third parties. Users using the third party images must also take into consideration the safe sharing of these images. We should also look into the image publishers, who publish the image, and image retrievers, who retrieve and use the image of the VM.

To address the risks that the publishers and retrievers face, the paper proposes image management system that controls the access to the VM images, tracks image history and provides the administrators and users with an efficient image scanners and filters system that detect and fix security violations.

Two risks that the paper discusses about are the need for high integrity in the VMs as they determine the initial state of the running VMs. Secondly, the images are often shared among different, often unrelated users. These two risks pose high privacy and security issues. A few companies support concepts like security group. A security group is related to the IP addresses that are either denied or allowed access to target VMs as defined by the firewall rules.

As we talk about the security risks in image repository, there are three key members that we must talk about who play crucial role in in the sharing activity. As mentioned in the paper [1], “The publisher, or owner, of an image is the one who contributes the original image to the repository. The publisher is mostly concerned about confidentiality (e.g., inadvertent leaking of sensitive information and unauthorized accesses to the image). The retriever, or consumer, of an image is the one who retrieves the image from the repository and runs it on the computer servers. She is mostly concerned about safety (e.g., a malicious image that is capable of corrupting or stealing the retriever's own private data). Common to both the retriever and the administrator is the risk of non-compliance (e.g., running unlicensed software or software with expired licenses). The administrator is concerned with the security and compliance of the cloud system as a whole and the integrity of individual images. The administrator assumes the liability of potential damages caused by malware contained in any image stored in the repository.”

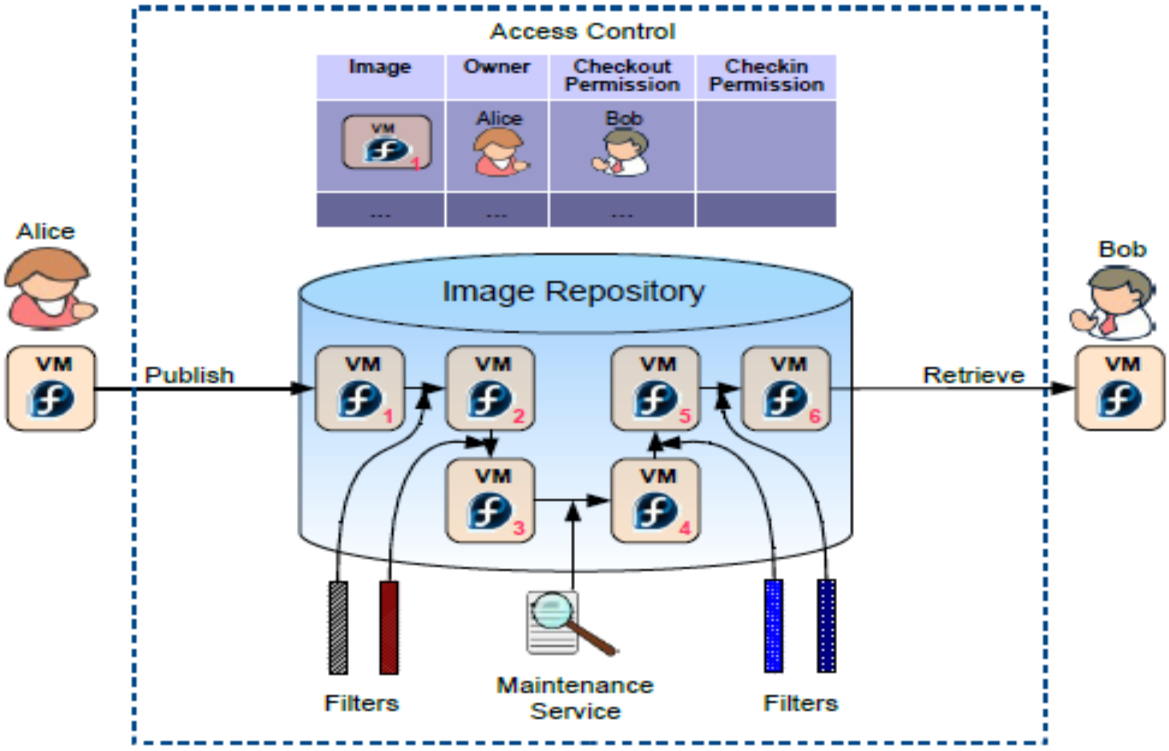

Figure 4.1.1: Mirage Image Management System [5]

When we talk about the publisher's risk, the risk of inadvertently releasing sensitive information is the most possible one. The images contain pre-installed and completely configured applications. The configuration part requires information like password protected account details. When publishing an image, the publisher may unwillingly publish such sensitive information in to the network. Such information should not be made public. A good example of sensitive data leak is that of browsing history. Along with protecting the sensitive information, the publisher may also want to keep the image access to a few users. This can be achieved by access control of the images.

When we talk about the Retriever's risk, it is about the risks involved in running malicious or vulnerable images in the repository. Running a malicious image is as good as placing an attacker's system into the network, thereby giving bypassing the intrusion detection system or any firewalls. It also involves lowering the security level in the entire network in which the image is running. When this happens, the effort taken by an attacker to customize a Trojan horse is also decreased. Usually, a Trojan horse program should be customized for every system. When a Trojan is introduced in an image, the image encapsulates the software dependencies of the Trojan horse. Another risk that the retriever runs into is running illegal software or unlicensed software in the image.

When we talk about the administrator's risk, the admin has the risk of hosting and distribution of images containing illegal or malicious information. When there is distribution of images, we should make sure that such information /content should not be distributed. Such images are referred to as dormant images. As time goes by, the risks in such images will become more and more visible. Such risks are referred to as latent security risk. This type of risk is often overlooked by admins due to high maintenance costs. Such risks grow with the number of images.

4.1.2 A survey on security issues in service delivery models of cloud computing [6]

Cloud computing provides a way to add the computing capacities dynamically without any further invest in new machines, new infrastructure, or new software. Even though it has been a hot concept, but enterprise are still reluctant to put their services in the cloud. The reason is that the concerns are continuously growing are raised about a safe environment about cloud computing. Security is one of the biggest issues in risk management which reduce the growth of cloud computing and complications. When new technologies are employed in practice, one should be aware of the architecture of the cloud services. The detailed architecture of cloud computing service is as follows.

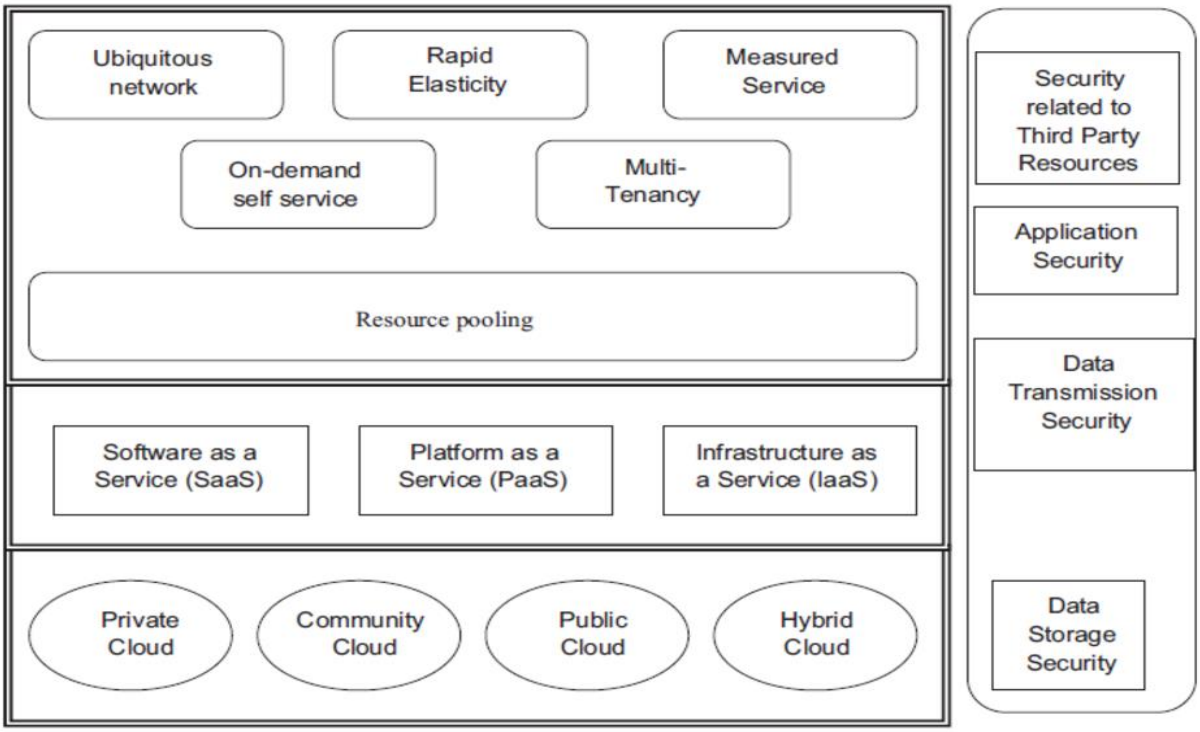

Figure 4.1.2 Complexity of security in cloud environment [6]

The paper discusses security issues in risk management from three aspects: security issues in SaaS, security issues in PaaS and security issues in IaaS.

Security issues of SaaS in risk management: For security issues in SaaS, the following key points should be carefully addressed which are considered as an important part of SaaS application development and deployment process: Data security, network security, data locality, data integrity, data segregation, data access, authentication and authorization.

Security issues of PaaS in risk management: In PaaS, provider of the cloud computing gives control to the users to build applications on top of the platform. However, the security below the application level such as host and network intrusion prevention is still under the control of the provider and the provider needs to ensure that data is not accessible between different applications. Therefore, it is more extensive than SaaS, but requires more customer-ready features.

Security issues of IaaS in risk management: For the security issues in IaaS, the developer has better control as there is no security hole in the virtualization manager. Another important factor is the reliability of data which is stored in the hardware. With the increasing trend of virtualization, obtaining the highest control over the data has received increasingly attention. The responsibilities of the provider and the consumer differ widely. Taking Amazon's EC2 for example, the service provider can only take care of the security controls while the consumer is responsible for the securities that relates to the OS, data and applications.

4.1.3 Case study: Amazon data center outage on April-21-2011 [10] [11] [12]

Amazon's famous Amazon Web Services (AWS) crashed on April 21st, 2011 taking down several of the websites. Many websites like the reddit, Quora etc. websites were down. The outage lasted for 2 days and is considered one of the major outages to have ever occurred. The company has stated that the outage was primarily due to lack of storage space. However, customers were not satisfied as the data was supposed to be distributed and isolated in different available zones. This distribution made sure that the outage in one zone did not affect the other zones. However, this did not happen.

In theory, the websites could distribute the services in different AWS regions. However, it is very slow and unreliable. The reason being that it requires sending data through the Internet. It is considered

impractical. The approach followed by Amazon is that it divides every physical data center into different availability zones. The zones are meant to be separate and redundant, but located in close proximity so that they do not need to transfer data over public Internet if we want to have them as a backup.

However, in Amazon's case, physical failure in one of the availability zone brought down the others. This meant even companies that have planned for redundant systems were at loss.

4.2 Data privacy

4.2.1 Data Privacy

Data privacy is one of the most important factors in deciding the success of a cloud service in being accepted by its users and winning their trust. . Especially in the case of *IAAS* (Infrastructure as a Service) *where* the third party offers the clients, the ability to store data remotely on virtual machines requires sufficient certified level of confidentiality and privacy the ability to outsource computing is a great tool and stepping stone to faster, more efficient distributed computing. *Sun* and *Zhang* [21] define *privacy* as the ability of an individual or a group to seclude themselves or information about themselves selectively. In cloud computing, achieving privacy would mean that a client is assured data privacy from an adversary (even with physical access to the system) as the data is stored remotely. Therefore, data privacy in cloud computing is said to possess the following issues; How to enable users to have control over their data without theft, unauthorized resale or any other nefarious use; To avoid data loss or leakage by using redundant storage and maintaining privacy in those systems as well; Adhering to storage of legal information and how to keep a check on them; Controlling and ensuring that the outsourced work is also in accordance to the required level of privacy. These issues can be characterized as the various goals/risk management objectives that are set on a cloud service system.

"Privacy is the ability of a an individual or group to seclude themselves or information about themselves and thereby reveal them selectively.", as quoted in paper [15]. Privacy in the cloud comes into play when users in the cloud visit the data and adversaries can infer the users' behavior by observing the usage of the individual's resources. ORAM technology (Oblivious RAM) technology may be used to thwart such occurrences. This technology works by visiting several copies of the data thus hiding the intent of the user.

Service abuse occurs when the attackers use the cloud service to acquire extra data or harm that of the other users. Deduplication technology is used by means of storing multiple instances of the same data only once as it proves to be a great cost cutting tool for the company. This makes it more vulnerable to

attacks because now attackers can access the data through the code of the stored files. Such attackers may lead to the increase in the cost of the service. They may consume resources maliciously which leads to the increase in the cost of that particular cloud service.

Since the cloud is involved with a large number of resources and users, they must be able to thwart denial of service attacks. Trusted computation models such as TCP and TSS may be used along with the cloud services. Since the cloud requires the users transfer their data on to the cloud merely based on trust, it becomes a key point for greater adoption.

Whenever third parties are involved in the cloud computing environment of a client it increases the threat to the system simply because of the heterogeneity that may result from it. Trusted third party independent approach may be used for identity management and identity data may be used on hosts that are not trusted. Different levels of security may be enforced to prevent loss of privacy. [15]

Traditional cryptographic techniques for data encryption cannot be used since the users do not store their data physically on their personal data centers. The large I/O costs that come with verifying the integrity of data by means of downloading it makes it unfeasible for use. Verifying the correctness of the data is also her because of the limited computational power on the user end. The solution to this problem is to enable public auditing wherein the users may consult a third party auditor(TPA) that possesses the skills and know how to handle the situation at hand that the user does not.

Auditing may be done by using a public key based homomorphic authenticator which the TPA can use for auditing without the actual data being present with him. The actual contents of the data can be hidden from the TPA by means of using random masking along with the authenticator. By the user of this technique the resources of the user are also spared as all the computational overhead is handled by the TPA.

There are also a few design goals to be kept in mind while enforcing this. The integrity of the data must be determined by the TPA without actually receiving an entire copy of it, no cloud servers must pass the audit and not maintain the correctness of the user data, the personal data of the users must not be extracted by the TPA during the audit, efficient processing by means of using batch processing should be used and the auditing process must be carried out with minimum computational or network overhead. [16]

At a very broad level, privacy is right that entails a person to have his life and activities undisclosed according to his wishes. In a computational and consumer context it refers to the personal information of

the customers, their online activities and usage and metrics of the sort. For organizations it comes down to the standards and protocols according to which they manage the personal information of their clients. Privacy in the cloud greatly depends on the context in the sense that there are situations when strict privacy norms need to be enforced (such as PII of clients and business processes) and other times when they may be relatively lax (public information). There are a few major reasons as to why privacy in the cloud has risks associated with it.

The user loses control of the data when migrating to the cloud. This is because all his data would be stored on the service provider's servers, all applications would be run off shore from his control. Thus there exists a threat of data misuse, the clients must always be able to access their personal information at request and delete them when required. Such tasks must be guaranteed by the service provider.

There is a risk that the personal data of the consumer may be used by the service provide in an unauthorized manner since they possess control over it. Such customer data may be used for selling customer specific advertisements or sold to other parties interested in such data. The question of data integrity and accessibility also arises if ever the service provider goes bankrupt or acquired by another parent company.

The data in a cloud is often proliferated to ensure its availability to the customers. As a result of this, it may be so that data is stored in centers that would not comply with the wishes of the user, it may be transferred to another geographic location violating even legal requirements of handling data within a certain jurisdiction. The fact that the user data may be transferred across country borders greatly undermines privacy of the data as it would be very difficult to pinpoint and pick out which particular server the data is currently in.

It is also not clear as to which body enforces legal requirements on the data, if standards to handle the data are set or if those standards would be able to securely handle the data. Subcontractors may be involved in handling the data who should be trustworthy.

Those are the issues of data privacy in cloud computing. The below describes a few techniques to address these concerns.

The customer of the cloud service would serve itself well by following a few guidelines while choosing the cloud service provider. It must clearly specify which of its information assets is confidential, ascertain the level of security provided to the data, the cloud providers business must be in good standing

and not have financial woes or risks of being shut down, creating a contract with the service provider that would cover the following - the provider is obliged to protect the data of the organization, consequences of failing to meet those obligations, geographic locations of the data, complying with all privacy and data protection laws, protocols when the data is lost and policies when data is to be erased or removed from the servers of the cloud service provider.

The privacy of the data can be preserved by means of encrypting the data. This is not preferred usually as encryption would prevent indexing and searching the data. Encrypted data can also not be processed in an efficient way. However it is possible to process data (although in an inefficient manner) by means of Yao's protocol for secure two-party computation or Gentry's fully homomorphic encryption scheme. Another approach is to simply use the cloud applications without bringing any personal information into the picture.

The use of standardized solutions would be an attractive option for the user as they would have a clear cut idea of what is being implemented, the APIs involved and where their data actually is. It would be pretty much impossible for the customers to identify the level of security that is being offered by the service provider simply because of the lack of information and high complexity involved with IT security that would result in them having to rely upon the reputation of that provider determined by means of evaluations and certifications. Thus standards would help a great deal in determining the cloud solution and level of privacy being offered to them.

What is worse than having personal data breach is not knowing the clear cause for it. This is where accountability comes into play in the cloud environment. The way to implement accountability is to have an audit system that keeps track of the data usage. The privacy risk of a user can be reduced by means of using a number of privacy policies and protocols thereby creating an accountable system that would bolster user trust.

There are times when the privacy requirements are to be enforced through a chain of cloud providers. In such scenarios we use clear contracts for accountability along with machine readable policies that are sent with the data. These policies may be read and the corresponding level of privacy securities or functionalities may be added to the private data.

Social and technological mechanisms may be used to increase the user trust in the cloud environment. Social mechanisms may include providing appropriate evaluations or certifications of the

cloud outsourcing business that would give the user an idea of what to expect by opting for the service. Technological mechanisms are the actual security features that the service provider possesses that may include sophisticated security softwares, hardware, audits and cryptographic techniques.

A combination of solutions may be used to provide a very secure infrastructure to the user. [17]

There are a few issues which are thought to have a significance in cloud computing security and privacy over the long term. Identity management is one of the paradigms spoken about here. It may be required of cloud subscribers to work towards establishing additional systems in order to extend their authentication processes into the cloud. For example, the SAML - Security Assertion Markup Language may be used to authenticate users before allowing them access to data and applications. In addition to authentication, access control may also be enforced by means of restricting the resources a user may be exposed to. For example, Extensible Access Control Markup Language may be used to control access to cloud resources.

Data protection is another important security feature in cloud computing which encompasses data isolation, sanitization and location. Data isolation is achieved by the regulation of access controls to the data. Database environments used in the cloud may either follow multi-instance or multi-tenant model. Data must be secured during transit and during rest. It may be secured during transit by means of cryptography but it is much harder to secure the data at rest. Data sanitization is the removal of sensitive data from a device when it is no longer needed. This must be done without leaving any trace of the data to be removed or it may be used in an unauthorized manner. Data location greatly affects decision of companies migrating to the cloud because it involves migrating private data from their data centers to that of the cloud vendors which is at a remote location and may be even in another country. [19]

A Privacy Manager is a piece of software that may be integrated to the clients system or be connected to multiple clients that helps prevent the personal data of the user from being breached and assists the service provider follow the privacy regulations. The first line of defense of the privacy manager is a technique called obfuscation wherein the data is in the encrypted form and processing is done on the same encrypted data and the result of the processing is de-obfuscated by the privacy manager. Obfuscation is different from encryption in the sense that some of the original data still remains in the obfuscated data. A key is used that is known only by the user and PM but not the CSP. Using this technique, the service provide will not be able to access the clients obfuscated data. Obfuscated data does not contain personal information of the client and can hence be processed the service provider. However during times when the user wishes

to upload private data to the cloud, the PM contains two features - preferences and personae. There are different possible ways to integrate the privacy manager to the system. There's the privacy manager in the client, privacy manager in a hybrid cloud wherein it is set up in a local network to handle information of multiple clients, then there is the privacy infomediary within the cloud that manages the data transmissions between different trust domains. [20]

This study is to highlight the importance of the data privacy in cloud computing system and how risks involving it can be managed. *Zhifeng Xiao* and *Yang Xiao* [22] compiled a detailed comparative study on the various traits of a secure cloud system and the current standards to ensure them. They provide an architecture centric approach on risk analysis and management and how various attacks on other traits compromise privacy as well. *Ashktorab* and *Seyed Reza Taghizadeh* [23] also expand on various security challenges and attacks. This report is a privacy focused study on its characteristics, the possible attacks on data privacy in cloud computing, the efficiency-performance trade-off of an approach accompanied by a bench mark analysis [25] and to bring forth a proposed solution for risk management in cloud computation using an Intelligent Track System [28].

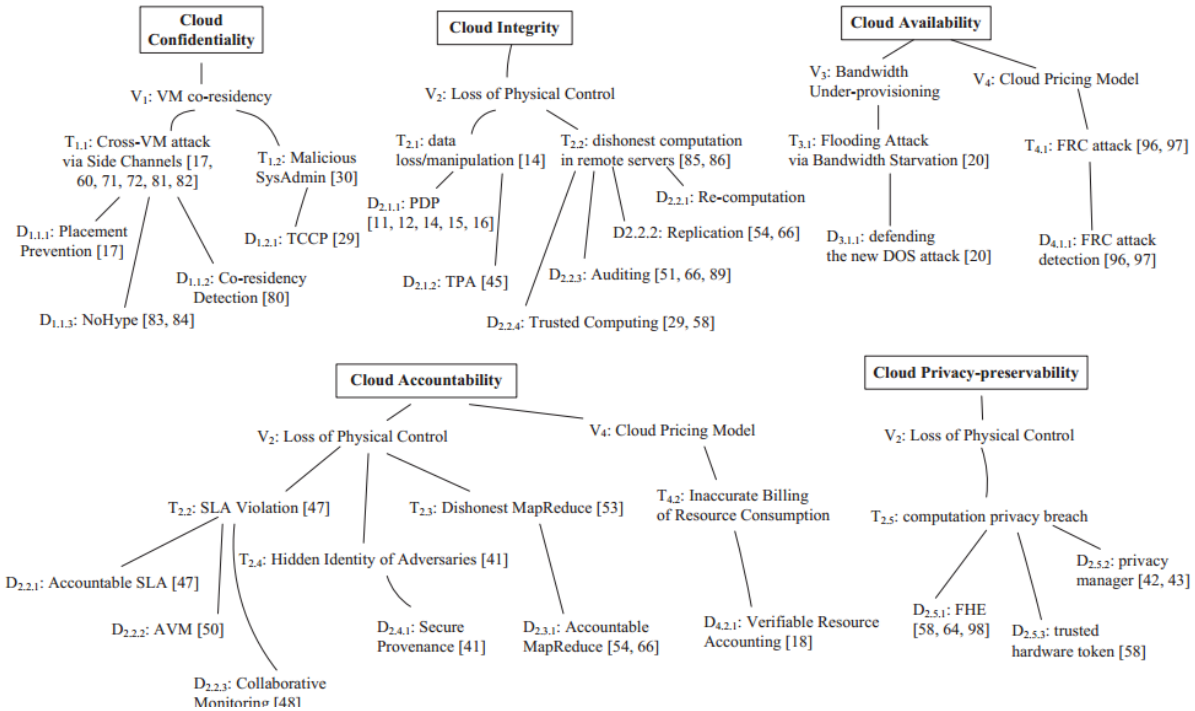

Figure 4.2.1 A Summary of research advances in Cloud Security and Privacy [22]

4.2.2 Summary of experimental or real-world data and analysis

To better understand what are the design principles of a secure system, *Meiko Jensen, Nils Gruschka* [26] explain lucidly the various attacks that redesigned the current standards of protocols used and increased the resistance of current systems against attacks on the security of a cloud system. The majority of the security threats fall on the shoulders of the underlying foundation of the system and these vary depending on the type of the cloud based system-from IAAS, PAAS to a SAAS. The service enabled fat clients work on the WS-Security and lay down principles to ensure integrity, confidentiality and authentication. The web browser at present works on NetScape's 1996 protocol TLS (SSL) which along with its handshake policy ensures authentication and system-side security. The cloud based security technologies work-atop these protocols and rely on them to function correctly. XML signature attacks work on the ability to wrap unauthorized content in authorized packets and forge the signature to avoid being detected. The paper then emphasizes the need for a web standard and not a platform dependent cloud service. As the browser cannot authenticate itself with cryptographically secure methods, any attempts to outsource authentication is also not a good idea and is proved by the breaking of Microsoft's passport. Thus this identity management problem on the client side is secured by combining TLS with SOP. This is documented as various methods ranging from web 2.0 Holder-of-Key-Assertion, TLS Federation to XML Encryption. The author then talks about the various integrity issues in the implementation. While an authenticated user is demanding resources on the fly, the metadata must be stored secured on the system and not prone to malware, metadata spoofing and flooding attacks. Apart from attacks to steal information, there are many attacks to prevent service like Denial-of-Service, Flooding attacks. The system must have exponential back-off to ward away spammed attempts at gaining service time from the cloud system.

We can then understand the possible attacks that can infiltrate the security of a cloud based system and to maintain privacy the major combating strategy is to perform encryption. Long since its origins, Cryptography has been greatly studied and has pulled in the research findings of number theory into the world of computing. However there still exists a great deal of uncertainty in the working of Fully Homomorphic Encryption which ambiguities the data in the cloud. Depending on the type of the cloud service, most of the functionalities and processing can be achieved with complete abstraction of the data. Encryption however has a compromise and it is in the form of a computation overhead and may sometimes may not reward in excessive investment. *Ji Hu* and *Andreas Klein* [25] developed a benchmark for a Transparent Data Encryption for migrating web applications to the cloud. Their study on the privacy-performance trade-off has been summarized into its characteristic strengths. These effects have also been documented as strengths and weaknesses.

Strengths and weaknesses

The expected level of privacy is vastly dependent on the nature of the cloud service and *Ji Hu* and *Andreas Klein* have stated the various requirements for privacy depending on the nature of the data being manipulated by the service. User Reference data are non-transaction data that are data regarding the operation specific settings, customizable configurations, user information and company meta-data. These do not take part in the transaction. The other is the main transaction data, the data that is processed by the cloud service as the primary business process. At a higher level both of the types require encryption and the difference lies at where the data is stored and how it is encrypted at that layer. A simple comparison between the various encryption schemes in the different layers is depicted in Figure 4.2.2.

TABLE II. COMPARISON OF ENCRYPTION ON FOUR LAYERS

	Storage layer	Database layer		Middleware layer	Application layer
		Database based	Column based		
Granularity	Coarse	Coarse	Fine	Fine	Fine
Performance penalties	Low	Low	High	High	High
Transparency	Yes	Yes	Mixed	Yes	No
Secure data at rest	Yes	Yes	Yes	Yes	Yes
Secure data at runtime	No	No	Yes	Yes	Yes
Vender lock-in	Yes	Yes	Yes	No	No
Products	Windows EFS, BitLocker, etc.	SQL Server 2008 TDE, etc.	PostgreSql, ,Mysql, Oracle, DB2, etc.	Hibernate / Jasypt	

Figure 4.2.2 Comparison of Encryption on Four Layers

The underlying astounding fact was that coarse encryption is not the best way to achieve better privacy. In other words despite the performance overhead in encrypting every input/output operation. Coarse encryption only secure the data in the file system. But data exists in more than just the storage drives and when dealing with cloud processing, even volatile memory like the RAM of the machine running the application, the session information or DBMS instances hold key information. Fine grained encryption involves every transaction to and from the system to be encrypted and thus is computationally intensive at run time. The authors then propose the transparent encryption scheme by first define the involved data in

the process. Master data: which is the personal business process data involved in transaction and personalized data or configuration and metadata values.

Their implementation uses a CBC-AES algorithm with a 256-bit key to perform symmetric encryption running on a x86 PC with a 2GHz Intel Core2 with 2GB RAM on a windows XP system, to simulate an ideal average household PC. They then performed a series of systematic tests on the encryption system when connected to a database. The results of the benchmark when performing 10, 50, 100, 500.. and tests on the database for each read, update and delete commands. The space and time requirements of the system when encryption was enabled and disabled were plotted to obtain the ideal level of encryption and resource feasibility. The output graphs of the benchmarks are shown in *figure af.3*

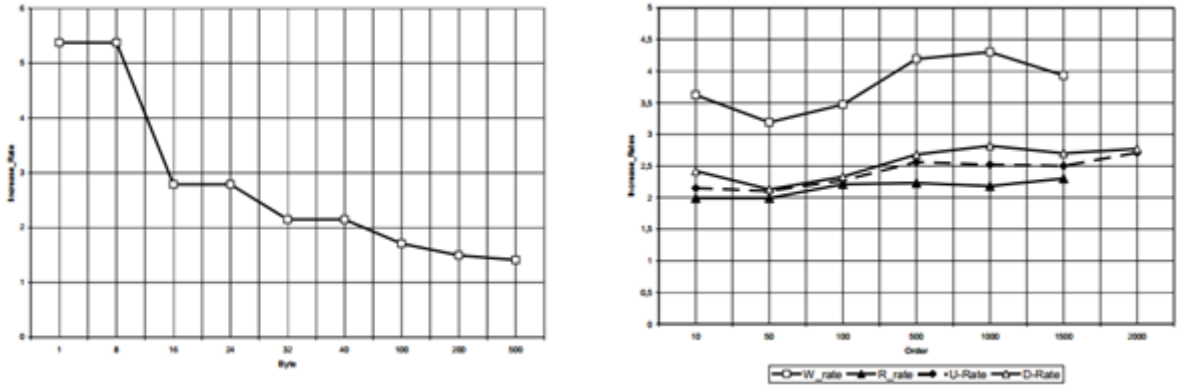

Figure 4.2.3 Space and Time requirements of system as encryption strength increases (key-bit strength)

4.3 Security in Cloud Computing

4.3.1 Browser-based Cloud Authentication

The paper [52] mainly focuses on the technical security issues in cloud computing. It mentions cloud layers and access technologies which include Software as a Service (SAAS), Platform as A Service (PAAS) and Infrastructure as A Service (IAAS). The main security issues in cloud computing focus mainly on data privacy, data safety and data confidentiality. The major technologies used for security in cloud computing are WS-Security (Web Services Security) and TLS (Transport Layer Security). WS-Security defines how to provide security to SOAP messages and also how the Security Standards such as XML Signature and XML encryption are applied. TLS is also known as Secure Socket Layer (SSL) and since it is implemented in all the web browsers, it is most important cryptography protocol. The paper also discusses main Cloud computing Security related issues as XML signature issues, browser security issues, cloud integrity and binding issues and flooding attacks. In XML signature wrapping attack the original message

is wrapped inside the header which is developed by the attacker and which can be used for malicious reasons. The WS security is used rarely so these attacks are rare but now a days some web services are vulnerable to them. The browser security can be improved if XML signature security is used within the browser along with TLS. The paper mentions browser security measures such as the legacy same origin policy, attacks on browser based cloud authentication, secure browser based authentication, future browser based enhancements.[52] The legacy same origin policy defines the needs to mentions the rights to write data when scripting languages are used in the web browsers. TLS authenticates both the data on transport to avoid phishing attacks. Attacks on Browser-based Cloud Authentication include the authentication in the web browser can secured with the help of third party as the browser can't generate the XML tokens by itself. The XML tokens can be secured with the help of TLS, which can be done using four methods TLS Federation, XML 2.0 Holder-of-Key Assertion Profile, Strong Locked Same Origin Policy, TLS session binding. The Browser security API can be enhanced by adding some enhancements in the web browsers i.e. XML encryption and XML signature.

Cloud security issues also contain Cloud integrity and Binding issues which ultimately include Cloud malware injection attack and Metadata spoofing attack. Cloud malware injection attack contains injection of a malware software or a virtual machine in the cloud computing software which does eavesdropping that might cause some data modification. Metadata spoofing attack manages to change the description of a web service's metadata. The paper mentions flooding attacks which focuses on the outsourcing the different service operations in the Cloud, which is a main part of Cloud computing. The impacts caused by the flooding attacks in Cloud computing are Direct denial of service i.e. if there is high load on the system it provides more computational power which works in the attacker's favor, indirect denial of service i.e. if one service is flooded it causes all the services from same server to stop and accounting and accountability it might increase the consumption of power and energy due to flooding. [52]

Result:

For resolving the security issues we need to enhance security capabilities in web technology domain and strengthen the foundation as a first step.

4.3.2 Data privacy through security in cloud computing

The paper [53] focuses on the important issues in cloud computing which can cause long term effect on the security and privacy in cloud computing dependent on different weaknesses and problems mentioned in the paper as the issues are related to the outsourcing in the organizational domain in public cloud. The issues related to privacy and security in Cloud computing which can cause long term effect are

divided into categories as Availability, Data protection, Software isolation, Identity management, Architecture, Trust. [53]

Availability defines the set of features and resources of an organization to be used. And it can be affected for short term or long term causing complete or partial loss in the system. The main threats to Cloud computing system due to this are natural disasters, equipment outages and denial of service attacks. The paper mentions different threats to Availability category in cloud computing which include temporary outages i.e. despite promising high level of availability the cloud computing services might experience performance slowdown due to outages for short period, Prolonged and Permanent Outages i.e. service providers might experience severe problem which might cause the service to shut down completely, Denial of Service can be caused in the public services as well as private services, Value Concentration i.e. the credentials of an account can be hacked using a cloud service for malicious attack into a system. [53]

Software Isolation includes Hypervisor complexity and attack vectors which includes isolation of user resources and various software in the public cloud. [53]

Identity management used to avoid the loss of data sensitivity and privacy of information due to unauthorized access to the resources. Identity management includes authentication and access control. Authentication administers and authenticates user before providing access and Access control makes sure that the access to resources is controlled. [53]

The System Architecture contains hardware and software present in the Cloud. The intercommunication components of Cloud that include Attack Surface, Virtual Network Protection, Ancillary Data, Client-Side Protection, Server-Side Protection. Since we have virtualized software implementation, when compared to the non-virtualized one the addition of the hypervisor causes growth in attack surface. Intra host attacks are pretty dangerous so to shun loss of protection and visibility against intra host attacks, physical network protection should be duplicated for virtual network protection. Along with the primary sensitive data the ancillary data should also be protected from being stolen. For a successful security protection of the information the data should be protected on both the sides on transport for which secure website and secure client is implemented in which the main emphasis is on the secure website infrastructure. All the server side applications and virtual servers should be protected in the cloud. [53]

The service provider inside the cloud computing paradigm must be trustworthy and here comes a category which is most necessary in the Cloud computing privacy and security. A higher level a trust is put in the service provider in public cloud. The factors Trust category comprises of are insider access, Composite services, visibility and risk management. Insider security threat is a main security issue for the organizations and comprise of high level of risk. There is no performance guarantee and liability in the composite cloud services as the security responsibilities have been given to the third parties and third party arrangements can be disclosed. It is challenging to manage and estimate risk in cloud services. The trust level must not be solely related to the organizational system security controls, other factors should be taken into account too. [53]

Result:

Determining the security threats in a complex computing system is a problem providing a list of common outsourcing provisions will be a good starting point. A balance must be maintained between benefits of cloud computing and related risks.

4.3.3 Mobile Cloud Computing (MCC)

MCC broadens the dimensions of cloud computing in an IT environment to include mobile devices on the cloud. Thus, MCC enables cloud computing services to be provided to mobile devices by including the benefits of cloud computing with the mobile environment. It also takes into consideration the issues w.r.t to Latency in network, limitation in bandwidth, security, confidentiality etc. [47]. Thus, there are also concerns of security of data stored on cloud which is now accessible to mobile devices. These risks include-

- There are no Standards of Security set aside for Mobile Cloud computing [47].
- Public cloud which implements MCC is considered unreliable and so, data owners are not forthcoming to have their sensitive data stored on these public clouds, as there is risk of security [47].
- Scalability of MCC is limited [47].
- There can be cases of breach in network, thus putting the data transmitted across the network at risk [47].

These risks are mitigated as following-

- Risk of security in mobile terminal can be mitigated using antivirus to detect and remove malware software [47].
- In case of physical systems used for MCC, vulnerabilities in software can be mitigated by patching the software [47].

- In case of security awareness, we need to monitor and regulate behavior of users [47].
- In case of mobile networks used, the risk of information leakage makes the network susceptible to security breach. This can be mitigated by enforcing encryption on information transmitted across the network or utilizing the security protocol to transmit data across the network [47].
- In case of security in physical systems in mobile cloud, there is issues of reliability in the platform as well as data confidentiality which can be mitigated by enforcing encryption on data in these systems, as well as security technologies.

Result-

MCC ensures cloud computing provides its services to the mobile users via mobile or portable devices.

4.3.4 Risk management of security – Overview of Risk Management

The security tool for mitigating the threats, vulnerabilities and security risks in cloud computing is the Risk management framework. This paper mainly explains the risk management framework to focus on critical areas in the Cloud computing environment. To protect the information well maintained and structured risk management strategies would be crucial. This paper explains various cloud deployment and cloud service models that are covered in the Risk management framework. [54]

The risk management framework has in all seven processes that include risk assessment, risk analysis, risk mitigation, assessing and monitoring program, processes-selecting relevant critical areas, strategy and planning and risk management review. Two major processes of for the planning and designing of this risk management framework are strategy and planning and selecting relevant critical area. In the strategy and planning process main goals are to establish direction, create meetings, define goals and proactively plan the requirements. In the Selecting relevant areas process the critical areas in cloud computing that need attention are selected or at least one crucial area is selected. Both the processes work in collaboration. There are three processes in the implementation and operation phase which are risk analysis, risk assessment, risk mitigation. The interrelated elements in the Risk analysis process are Threat identification and vulnerability identification. The output of threat identification contains threat source, motivation and threat problems. The vulnerability identification step output determines vulnerability, threat source and threat actions. Risk Assessment process is determination of qualitative and quantitative output from the risk analysis process. In risk assessment process contains four sub-processes as likelihood determinations, impact analysis, risk determination, Control Recommendations. Likelihood determinations

sub-process explains the possibility that a vulnerability may be experienced in the environment. So it defines likelihood level and likelihood definitions which have levels as high, medium and low that define the intensity of the vulnerability. Impact analysis process measures level of risks that untimely impacts caused due to unavoidable vulnerabilities. It defines the magnitude of impacts as high, medium and low and defines it as impact definition which is

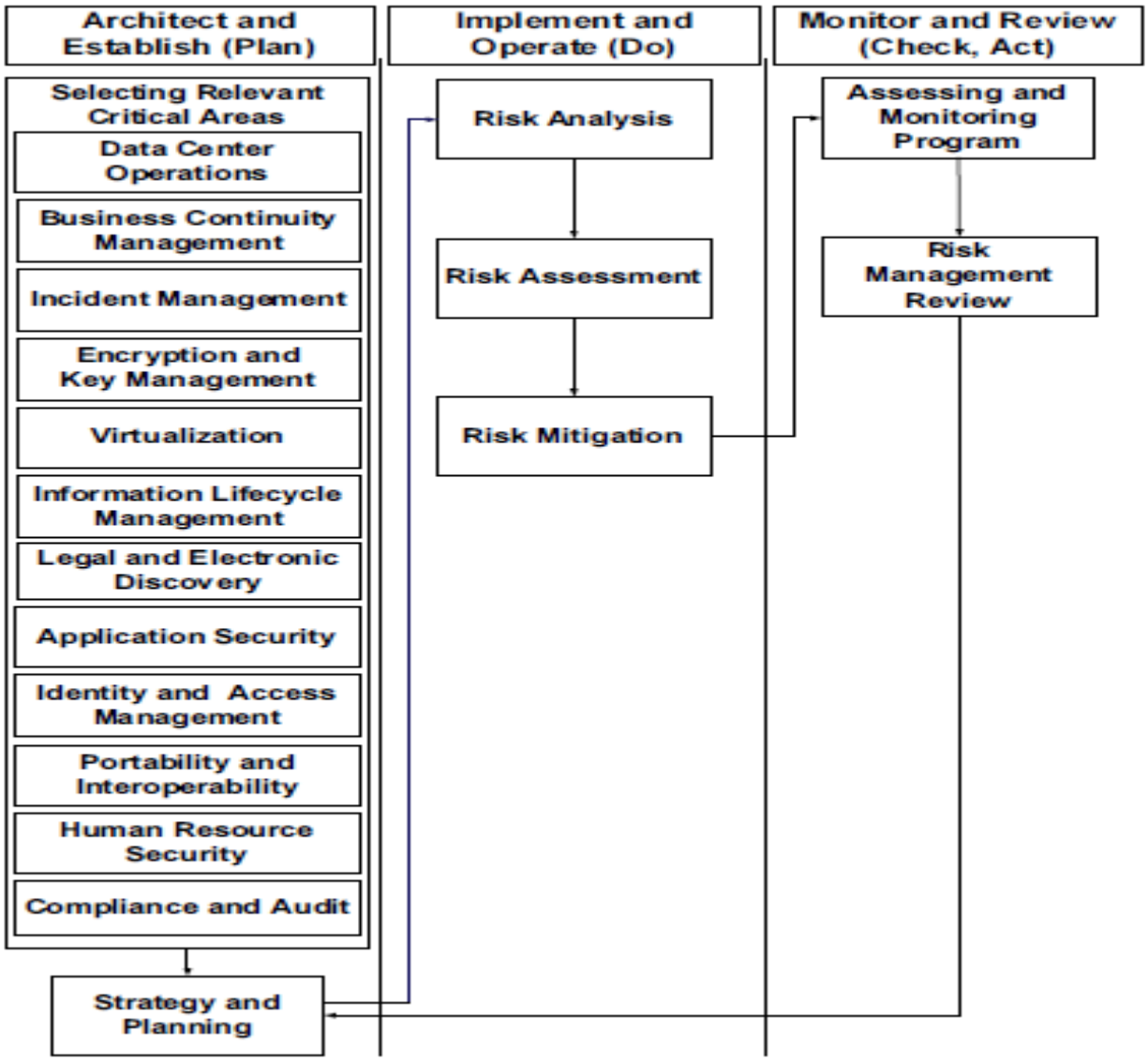

Figure 4.3.1: Overview of Risk management framework for computing environment [54]

called magnitude of impact definitions. Risk determination process focuses on the risks selected in Selecting Critical Area process and determines the risks related to it. It determines the risk level as high, medium or low depending upon the Threat likelihood and its impact and according to the level the solution is provided

Risk description and necessary actions to be taken. The goal of Control recommendation process is to lower the risks in the cloud computing domain to a certain level. Build and maintain a secure cloud infrastructure, Implement and maintain a security program, Implement strong access and identity management et cetera are some of the steps in doing so. Risk mitigation process gets output from the risk assessment process as different threats and vulnerabilities need different approaches to be dealt with them. The goal of Risk management review process to develop a set that defines baseline and sets goals and assesses the progress i.e. to help in the development of a process to loss prevention. [54]

Result:

A risk management infrastructure will be helpful for information security risk management in Cloud computing domain, which helps organizations to do risk analysis, risk assessment, and risk mitigation.

4.3.5 Security challenges in risk management

Cloud computing is growing domain with a high speed but the features provided ignore the security challenges so this paper concentrates on the considering risks and suggesting solutions to provide secure cloud computing environment. [55]

The unique security implications in Cloud computing are Outsourcing Data and Applications i.e. the data should be allowed to be accessed by the authorized personnel only as the third party services are involved the security can't be ensured, Extensibility and Shared Responsibility i.e. the responsibility of security of data should be shared by the customers and the service providers, Service-Level Agreements i.e. the level of service is defined using an agreement between the customer and service provider to control use of resources in cloud, Virtualization and Hypervisors i.e. using isolated VMs the virtualization concept provides the users abstract infrastructure and resources, different forms of Heterogeneity present in Cloud, Compliance and Regulations used to make sure the customers and service providers comply with the SLAs. [55]

For information security in cloud computing the approaches used for the previous mentioned challenges are explained in this paper [55]. The approaches include user centric IDM for Authentication and Identity Management challenge, Role based access control method for Access control challenges, building policy management framework in cloud for Trust Management and Policy Integration, using virtualization to separate application services from the infrastructure for Privacy and Data Protection, a trustworthy risk management framework for Organizational Security Management, automatic detection of

the conflicts among the services and cryptographic approaches. Cloud computing domain is a multi-domain environment so the security requirements for all domains are different. [55]

Result:

Even though currently exist solutions for security threats in cloud computing, more improvements in those solutions and newer and mature solutions are needed.

4.3.6 Risk management approaches

A) Identity and Access Management

Identity and Access Management [36] [37] aka IAM system is a processing framework implemented by businesses for managing electronic entities [32]. Although, the company is responsible for utilizing 3rd party services on the cloud, there still needs to policies governing the usage, rights and privileges of the individual users using these cloud services. These usage rights and privileges must be automatically revoked when the user resigns the organization or resigns the role he/she initially had [33]. Also, compliance auditing checks need to be performed on the companies using these services for adhering to these policies. With the increase of sensitive information being stored in the cloud, it causes more security and privacy concerns with the Cloud provider monitoring which user is authorized to access such sensitive information in an appropriate manner. The IAM technology isn't directly proportional to profits or gains from a monetary or functionality perspective, but inability to establish core IAM framework will pose tremendous security risks and concerns, thus amplifying the risk for security threats [32]. Added to this, threats targeted towards the organizations are becoming more and more sophisticated and extremely complex, thus allowing them to infiltrate the network to extract more valuable information over time.

There are several considerations to be looked at when using IAM in cloud computing. These include mapping identities of end-user to the system directories [34], document specific guidelines for privileged user access, and ensuring single-sign on capabilities. Also, revoking access to users no longer part of the organization, as well as removing their entries from the active directory. To ensure compliance to guidelines, access to applications should be monitored at the department level, with auditing of activities comprehensively and at a granular level [49].

Result-

IAM is very useful in enforcing security policies on the cloud computing end-users.

B) Service Level Agreement

Before the 3rd party cloud service provider provides cloud service to the organization[39] , they establish an agreement named the Service level agreement(SLA) which provides the service cost with respect to the Quality of service aka Qos with prices varying with respect to Qos [50][51]. Also, any side violating these guidelines will result in penalty. SLA provides a written legal document about the responsibilities of Cloud provider and the consumer or the organization. Apart from this, [38] [39] SLA defines the "what" and not the "how" i.e what level of service, what responsibility each party has etc. Following is the description of the SLA components [40] [41]

- Purpose of having an SLA between service provider and service consumer [40][41].
- Time period for which SLA is valid [40] [41].
- Scope of services provided by CSP aka Cloud service provider as well as out-of-scope services [40] [41].
- Penalty to ensure service performance doesn't fall below performance threshold [40] [41].
- Roles and responsibilities of the involved parties [40] [41].
- Non-mandatory services, which may be needed in the near future.

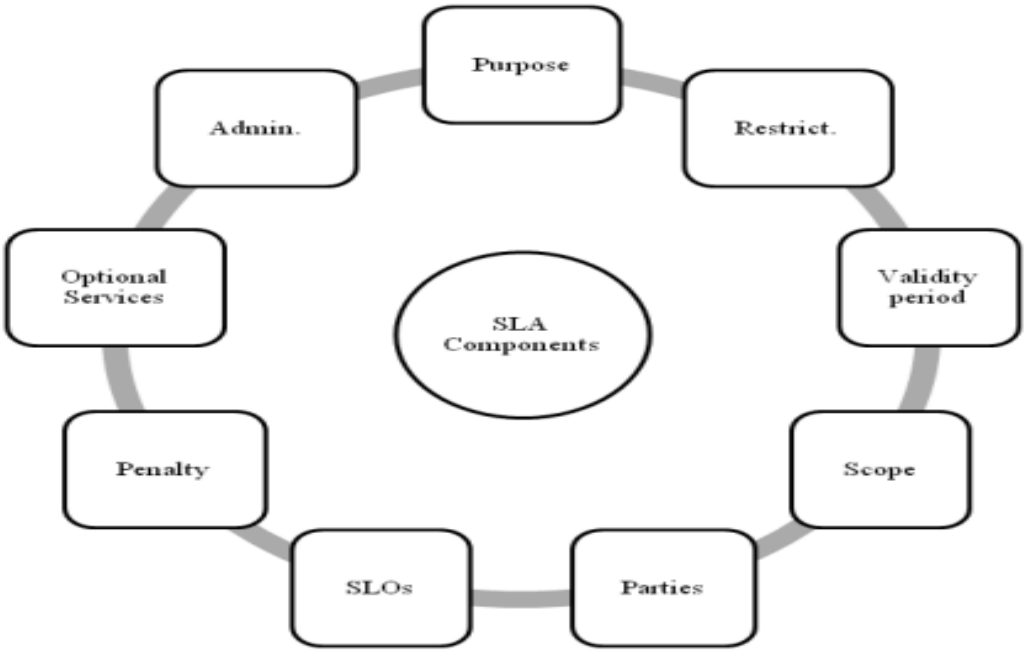

Figure 4.3.6. SLA components [40] [41]

Result-

SLA enables cloud service providers provide a better delivery of service.

C) Trusted Cloud Computing Platform

Although virtualization or VM's have numerous advantages from functionality perspective, it in no way mitigates the risks of physical systems, but may on the other hand give rise to risks which didn't exist in physical systems [45]. Thus, it becomes crucial to take note of these risks and manage them. These risks are classified as follows-

- Sprawl of VM's – The ability to create new VM's from existing VM's such that the newly created VM's spawn and create more VM sessions. This can result in wastage and over-usage of system resources [45]. In such a case, it becomes a necessity to document guidelines regarding which persons should be allowed to create and use VM sessions and what's the purpose behind it. This results in accountability for these systems.
- Confidential data within VM's – Since VM's are accessible from a remote machine, data which is confidential can be leaked to remote systems either through transport through VM's [45].
- Exhaustion of Resource- Availability of the physical system gets compromised since these systems are accessed through VM's which consumes the resources of these physical systems [45].
- Security of Hypervisor- Hypervisor is the software behind the VM. Thus, this ensures the hypervisor is secure [45].

These risks are mitigated with Trusted Cloud Computing Platform aka TCCP. TCCP is based on the concept of Trusted Platform, and implementing this concept to the Infrastructure-as-a-service (IaaS) backend. TCCP ensures that the data is secure, and maintains the integrity of the data.

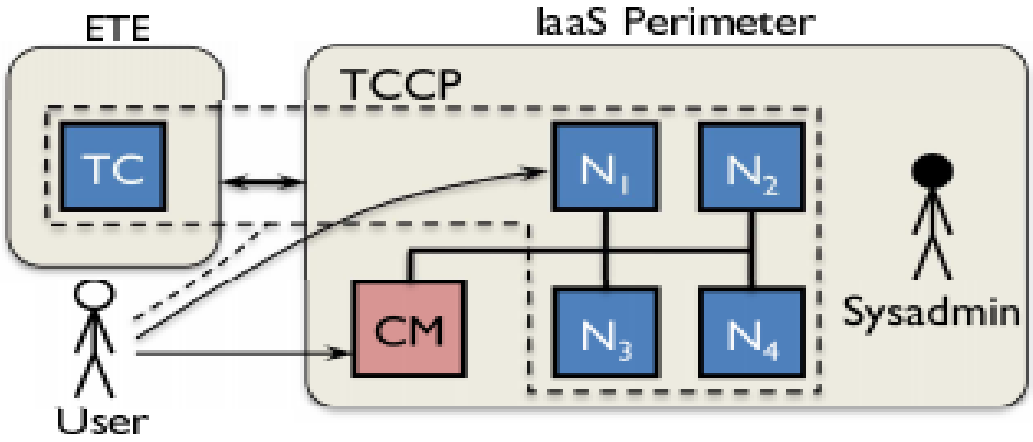

Figure 4.3.7 Components of TCCP [46]

Result-

TCCP enables protection of data from vulnerability due to virtualization.

4.4 Availability and Capacity Limitation

4.4.1Availability:

Availability in a nutshell means that the service should be available to all the users at all times. There will need to be some downtime in order to perform maintenance and fix problems but ideally it should not interfere with the productivity of the service.

An ideal high availability would mean that in if a service runs for a month (30 days), then the downtime should be not more than 4-5 minutes.

If the system is down for more than the ideal time then it is deemed as inefficient. Availability is a feature of cloud computing which is most visible and most obvious to users. Most users use the cloud because it is available whenever and wherever they want to. So the risks involved with availability are important to tackle as availability is the most attractive and desirable feature of cloud as a whole.

4.4.2 Capacity Limitation:

Most users use cloud for the main purpose of storing data. Therefore the capacity limitation of the cloud and the risks associated with it are a major concern for us. Capacity limitation mainly means the upper limit of the cloud capacity. In simpler words, the number of load the cloud can handle at one given point before its performance starts to degrade or worse it crashes completely.

4.4.3 Risk management for availability and capacity limitation

A survey of risks associated with government use of Cloud Computing by Paquette, Scott et al., various anomalies in the cloud services were observed and analyzed in their survey paper, these anomalies directly impact the risk factors of a Cloud System.

Four major outages were observed in 2008, they were of 1 hour or greater in length which was cause for concern as data was unavailable to the users for quite a long time and it agitated the users. The reasons for the outages were found out to be mainly due to overloading. This overloading mainly occurs because the risks of capacity limit of the cloud are not taken into consideration and are not given the attention they deserve.

One highly talked about and widespread outage was at Amazon in 2009. It was due to a lightning strike at their data centers, and it led to the services being unavailable for 4 hours.[73] This tells us that natural disasters are a major reason to compromise availability, and there is nothing that can be humanly done to prevent that. All that can be done is come up with ways to get the systems back up and running in good time.

Risk management techniques need to be exhaustively designed to cover all these possible risks, nothing should be left to chance. Whenever availability is compromised, it should be the highest priority of the recovery team to restore the cloud services and get it back online at the earliest.

The effectiveness of a cloud computing service can be measured not only by its performance but also by its availability. Almost all cloud services have security mechanisms integrated into them.[74] Data stored on the cloud may become prone to exploitation when the security mechanisms incorporated in the cloud aren't available at all times thus putting the integrity of users' data at risk. Availability also gets compromised when the cloud service providers fail to take into account the capacity limitation. Extensive research and surveys have been performed by Paquette, Scott et al. and it makes clear why the capacity of the cloud should not be taken for granted. When a cloud reaches 80% of its capacity, it starts to thrash, meaning the storage disks and memory start to move around the data in order to keep functioning accurately. [73] This puts more pressure on the system's performance. If a cloud's capacity is cited as "X", then it does not mean that the cloud services will always work well at 100% usage.

A threshold can be set, such that after the usage reaches that particular threshold, more computing power should not be granted to the applications. This will prevent the system from reaching the point of failure.

As we know, cloud computing services are not always provided by one big corporation, they are delegated to smaller vendors and companies. This brings into question what will happen to the availability of the data of the users once the company handling a particular service closes down or goes out of business. This needs to be addressed by risk management team. In 2008, a vendor abruptly closed down, this led to users being worried about retrieval and availability of their data. In the end about 55% of data was retrieved and the rest was not be found. This is the absolute worst thing that can happen, as it leaves the customer in the dark and can make the user lose faith in the cloud computing paradigm.

The techniques that are being used in the industry to improve the availability of cloud computing services are discussed below.

4.4.4 Load Balancing:

What exactly is load balancing and how is it accomplished? With respect to cloud computing - it can be defined as a way to balance the traffic on cloud to ensure high availability of network resources. It should also account for occasional failure of software, minimizing hardware use [10]. Load balancing is a computer networking technique to divide load (or in our case, data) among processors, drives and/or servers [75]. It is a very critical aspect of cloud computing. Data in a cloud would be easy to access if it is divided among its servers evenly.

Advantages that a balanced cloud brings are as follows: [75]

1. Primarily, it aids in maximizing the availability of cloud computing services.
2. It improves the performance of cloud computing.
3. Helps in optimizing the utilization of resources.
4. Helps access data faster by reducing the response time.
5. Improving the overall throughput of the system.
6. And avoiding overload of data.

Implementing load balancing can be a challenging task. Broadly load balancing can be done in two ways – the static approach and the dynamic approach. The static approach is a more generalized approach where each data unit is considered equal. And accordingly traffic data is split equally among servers (more popularly known as the round robin scheduling). On the other hand dynamic approach does the balancing of traffic on the fly [74] .

Below is a list of the most commonly used load balancing techniques in cloud computing:

1. *Round-Robin*
2. *Connection mechanism*
3. *Randomized*
4. *Equally spread current execution algorithm*
5. *Throttled load balancing algorithm*
6. *A task scheduling algorithm, based on load balancing*
7. *Biased random sampling*

8. *Min-min algorithm*
9. *Max-min algorithm*
10. *Token routing* [75]

Challenges in load balancing in the Cloud: [75]

a. To account for allocation and release of 'load' automatically.
b. Ensuring the economic nature of cloud computing services.
c. Maintaining low response time with the emergence of remote data centers.

4.4.5 HAIL Protocol:

Computing on the cloud is a necessity in today's world. Studies by reputed journals predict a boom in the cloud computing scenario in the years to come. In its present state though, there are innumerable risks associated with cloud computing. Data privacy, integrity, availability, capacity limitation among several other risks [78]. As discussed earlier, one of the major threats is we have a secure solution to ensure continuous availability of cloud data. This security solution called HAIL - High Availability and Integrity Layer Protocol. The idea for developing HAIL was to avoid the scenario where a particular cloud service provider fails or gets compromised [76].

An important purpose served by the HAIL protocol is that it divides iterative information among the cloud servers. It helps in balancing the load on the cloud servers and thereby maintains the availability of the cloud high. We can observe that in many ways HAIL is similar to RAID (redundant array of independent disks) – both help create trusting, highly available components from not so reliable sources.

HAIL is designed in such a manner that it works to mitigate the risks associated with cloud computing by quickly recovering from threats like – data corruption etc. HAIL operates in the following manner:

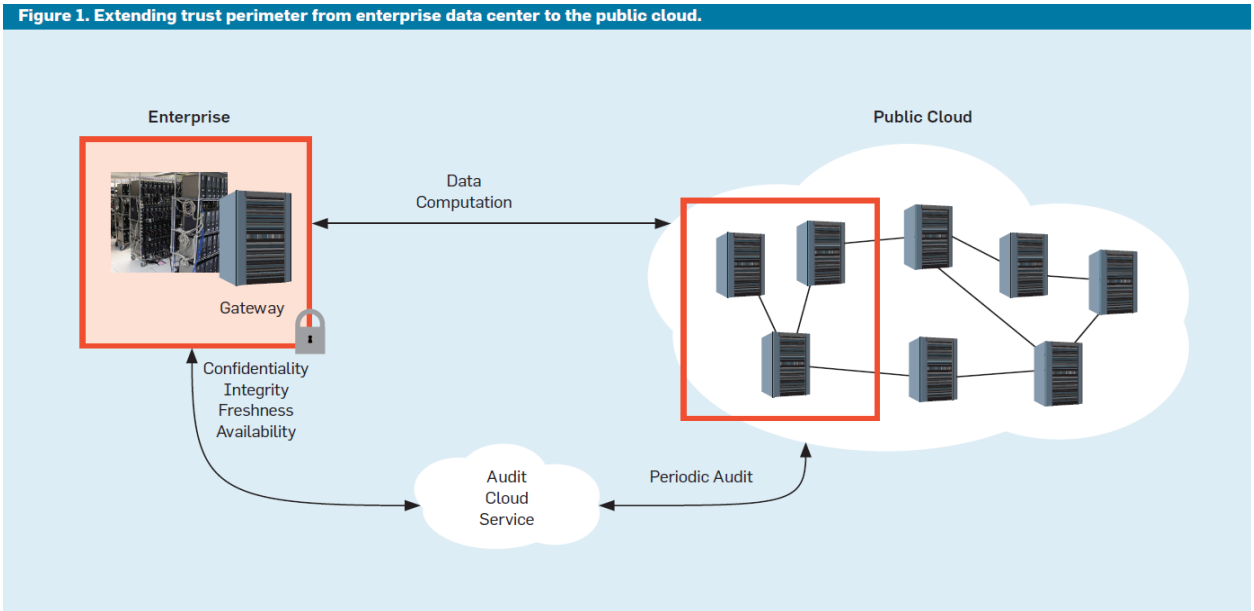

Figure 4.4.1 - Extending trust perimeter from enterprise data center to the public cloud [76]

a. The user uploads data to multiple cloud service providers. As shown in the Figure. 1 (ck) below - the data is uploaded to the public cloud.

b. The uploaded data is encoded in the gateway. The authors Ari Juels and Alina Oprea describe the encoding of data as in shown in Figure. 2 (ck). Singular encoding does not help ensure high availability [76].

c. In case of a failure, HAIL has a mechanism to review the data in cloud service providers for validity.

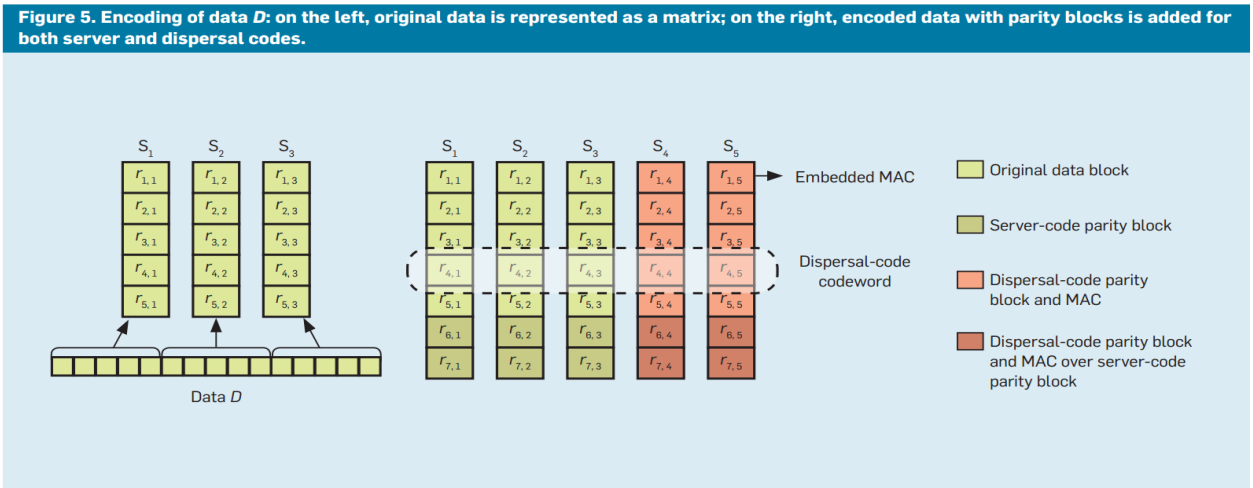

Figure 4.2 2 Encoding of data in the gateway [76]

It manages to create a distributed cryptographic system which handles the risk of availability.[77] Proof of retrievability is a tool proposed by the cryptographic community which helps the user to know

whether or not a particular piece of data is available to them and whether or not it is uncorrupted. How it works? The user sends a request asking for the availability of a file, if file is unavailable or corrupted, the user is informed and then the user can look elsewhere or refer to other sources for the file. HAIL uses this tool in its approach. [77]

Shortcoming of HAIL:

It cannot manage updates to files efficiently. [76]

4.5 Business Continuity in Cloud services

4.5.1 Business Continuity:

Many companies nowadays want their data to be very secure and available all the time and they simultaneously want to implement new technologies as well. This is a very difficult scenario. This problem can be overcome by implementing cloud and including the continuity services in it.Cloud computing mainly relies on hardware-independent virtualization technology, the companies are allowed to quickly back up data and the applications to the cloud. By using Cloud the total costs affiliated with the business continuity reduces drastically as the cloud off-loads all the responsibilities to experienced and professional expertise. Even in the case of worst natural disasters, the continuity in the cloud is properly maintained and there is no loss in data.[roshan_article-1]

4.5.2 Business process elasticity in cloud computing:

Cloud computing is emerging as a new delivery model for IT services. For deployment and execution cloud computing is very crucial.

Challenge: PaaS was not elastic in the earlier times when it was developed.

Solution: To solve the problem, the expertise developed a new model for service deployment called micro-container. In this approach a micro-container was dedicated for each deployed service in Cloud Environment. To manage the lifecycle of the deployed services, the generated micro-containers can provide minimal and personalized functionalities which helps in providing elasticity at the PaaS level.[58]

4.5.3 Elastic Multi-tenant Business Process:

Elasticity helps service providers to efficiently exploit cloud resources. Elasticity also plays a key role in reducing servicing costs. This makes multi-tenant business processes to be long-running and concurrently accessed. An auto scaling approach is proposed to tackle the problem of handling elasticity at

the process and services levels to scale-out and scale-in their service instances and to hold the promise of ensuring the elasticity of the multi-tenant business process.[59]

Activities in Elastic Multi-tenant Business Process Based Service Pattern:

- Elastic Service patterns
- Auto-Scaling Algorithm
  - Service Pattern Selection
  - Auto scaling Decision

The constraints between the multi-tenants service efficiency and the elasticity needs to be imposed by services providers which make the development tasks difficult.[59] A new approach in which the reusing the elastic service patterns as abstract specifications for MTBP at the SaaS level has been implemented. [59]

This study is based on service pattern and decision making on the execution of the elasticity mechanisms. The approach is based on the middleware layer (Middleware as a Service) between the application layer and the platform layer in the cloud architecture.[59]

4.5.4 Virtual business in cloud computing.

Configuration and Optimization of Virtual Business:

Establishing the Virtual business is very crucial and cloud computing makes sure that the virtual business are realized to online services through outsourcing business function [60]. The configuration and optimization of the virtual business becomes a major concern in a service-oriented business ecosystem because of the huge number of cloud service providers and business services.[60]

Objectives of **Service Process Stochastic Decision** Model:

- Cloud Service Providers Candidates Acquirement
- Problem Specification For Stochastic Decision
- Service processes stochastic decision under multiple QOS objectives
  - The sequential execution fragment
  - The concurrent execution fragment
  - The selectable execution fragment
  - The iterative execution fragment

At runtime in order to support the execution of virtual business effectively, the optimum service process scheme can be configured [60]. In this stochastic service processes configuration and optimization approach the execution performance of virtual business improves a lot. Considering the set of candidate business services which satisfy the end user preferences for the whole ecosystem is the most important part.. Moreover, the design and development of a suite of software tools to support the service processes optimization is very important for the spread and application of the service processes configuration and optimization approach.[60]

Application:

Xenserver is an example of how business continuity is implemented in cloud computing .Xenserver is implemented in cloud computing through the power of virtualization

Citrix Xenserver overcomes the concerns of organizations who want to maintain the proper running of their information infrastructure and thereby assuring that users have continuous access to fundamental resources, even in the worst scenarios such as natural disasters[61]. An organization's in order infrastructure and resilience can be improved with the use of virtualization technologies provided by the citrix xenserver[61]. This takes care about going on ensuring that not only the critical resources remain available but are always accessible to all users even in the weirdest location. With the help of virtualization solutions, business leaders can reduce the risks due to both IT service outages and workforce continuity disruptions like diminished efficiency, missed opportunity.[61] The virtualization technology also helps in building a very powerful foundation for compliance and security.

Characteristics of Xenserver :

- Non stop business operation
- Increased business agility
- Stronger data security
- Cost-efficient IT

4.5.5 Addressing challenges in business driven IT Models:

To be able to make business-continuity in cloud based systems it is important to have an efficient self-management of these cloud entities aware of business interests which in turn is a research challenge that needs to be addressed. Motivation for developing such management system are [62]:

1. Cloud infrastructures are evolving into very complex systems in terms of dimensions and management

2. There are several aspects to be tackled in order to efficiently manage cloud services during their whole life cycle
3. Adopting a Business Driven IT Management model is a significant requirement for an effective IT governance in businesses;
4. The increasing expectation from businesses that IT systems should assist in achieving their Business Level Objectives (BLOs). In this direction, the Business-Driven IT Management (BDIM) discipline is clearly very appropriate to be widely used in Cloud providers. It aims at rethinking IT management from a business point of view [62].

The paper [62] focuses on "how Cloud providers driven by business-level objectives should (self-) manage their Cloud entities in order to aggregate significant values to the business on top of it, as well as to their users (which actually may be other providers).The paper[5] talks about the BDIM metrics i.e. BDIM is responsible for producing Key Performance Indicators (KPI) of the business through synergetic evaluation of disparate business-level parameters (BLPs)".

The above approach differs from the previous approaches by the fact that earlier approaches did not provide dynamism when allocating resources to services, which is extremely required to deal with typical changes in the environment like dealing with demanding resources.
Solution: The visualization technology, which is the basis of any cloud environment, allows to overcome such limitations. Cloud providers are able to dynamically allocate resources to services in order to meet changing conditions (i.e. time-varying workloads) that affect their BLOs. More to the point, the services' life cycle can be self-managed (automated) through corrective low-level actions. In any case, the BDIM discipline is becoming a promising way for an accurate and efficient IT management in recent and future years, and in several disparate Cloud scenarios [62].

4.5.6 Security related risks in maintaining business continuity:

Security is one of the major concerns in business continuity and has to be maintained to the maximum. The following explains how to maintain security aspects in cloud computing.

Paper [63] describes the factors influencing employees' information security behavior. It argues that model should focus attentions on modifiable factors influencing behavior. It also describes how those theories will play an important role in the government information security management.

Employee's behavior plays a vital role in information security. As a matter of fact most of the activities in information management are done by employees' operations. It includes information collection, information storage, transmission and information usage and analysis involving employees' activities.[63]This paper addresses the issue of Information security regarding organizational information or information systems due to unauthorized access, use, disclosure, disruption, modification , perusal, inspection, recording or destruction [63]. The author talks from the perspective of behavior management or intervention that employees' information security activities are bundling with their psychological process.

Government information security management greatly depends upon employees' weak awareness which can be attributed to personal factors, knowledge scarcity on information security [63]. In most of the cases, employees are unaware about their information security situation, some don't realize that the possible destructive and disastrous consequence resulting from information security breaches until they happen [63]. So it is important that the top management should be conscious of information security issues such that they can prevent information being compromised by adopting reasonable steps in regards to the information security.

To increase worker efficiency it is necessary for the employees to be remain motivated which can be achieved through addressing the basic psychological needs of an organization's employees. Usually, incentives and/or peer pressure helps in creating motivation [63]. Alternatively, risk appraisals and self-assessments can be used to explain personal risk information besides incentive methods.[63]

Information security risk has a lot of uncertainty. There are situations where the organization and the employee may not be able to comprehend what are the consequences of not being able to handle the information security. So, behavior patterns generally work for them as it drive’s them for making a decision based on the trade-offs analysis. Thus people having strong and stable intentions are more likely to be motivated to take actions on their intentions.

Employees’ information security behavior is involving complex psychological activities (Ryan west, 2008). Culture plays a vital role in biasing people's opinion towards a particular organization and employees' actions.

To be able to maintain appropriate information security behavior, organizations should evolve with their culture. In the paper the author comes up with a summary of belief model figure below [63] which helps us to understand and predict behaviors.

The model proposed that people's likelihood of taking a specific security-related action is primarily motivated by the following perceptions, considerations, or beliefs [63]:

1. Perceived severity;
2. Perceived susceptibility;
3. Perceived threat or risk;
4. Perceived severity;
5. Perceived barriers
6. Self-efficacy;
7. External environment (organizational information security culture)

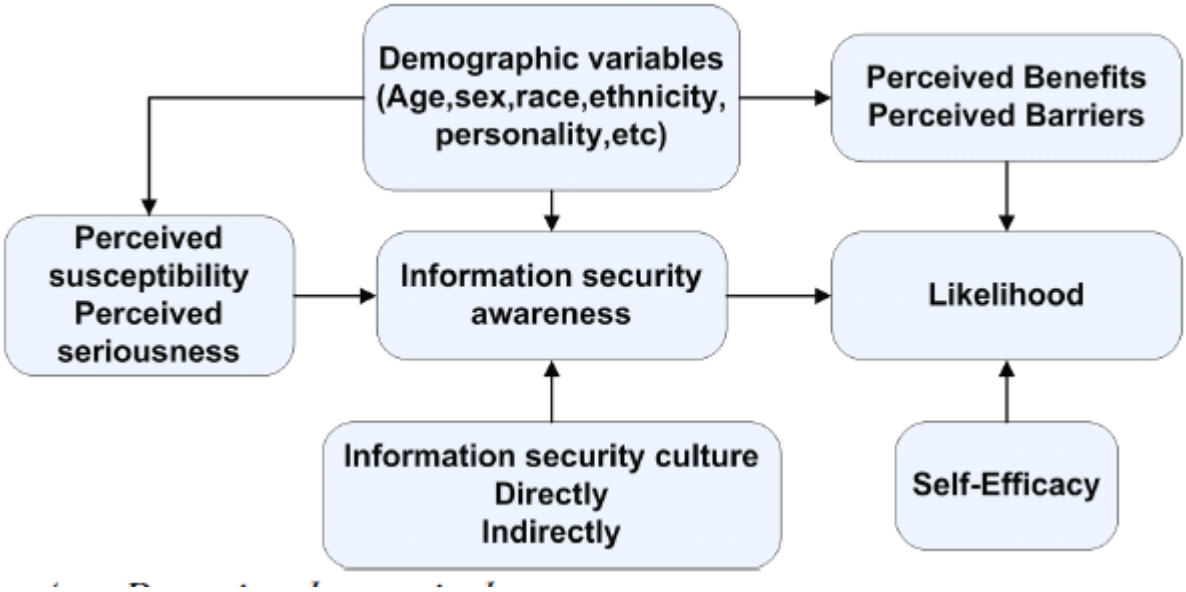

Figure 4.5.6 Model

This model also postulates that demographic variables such as age, sex, and ethnicity indirectly influence behavior through their impact on perceived threat or perceived benefits and barriers. In the same way, socio-psychological variables such as personality, socio-economic status, and peer and reference group pressure also influence behavior indirectly through their impact on perceived threat or perceived benefits and barriers [63].

Encryption and Decryption Service:

Cloud computing environments include three types of services: infrastructure, platform and software. So, for cloud service to expand, users must have a very high level of trust. This paper [64]

proposed a business model for cloud computing based on a separate encryption and decryption service which emphasized that the security of user's data. The data which has been encrypted and stored but the decryption algorithm does not have the capability to return the data in the cloud. The management of the key required for the user data is very crucial. In this model data is encrypted and then only saved and because of this implementation it makes it impossible for the algorithm to access the data.

Development of Business Processes:

This environment allows for a number of stakeholders to collaboratively specify business processes with security requirements and allow them to expose and share their business [65]. Even the security expertise that can be used for relevant business processes among the business organizations in the Cloud is also exposed in this environment and thus can be shared. This environment makes sure that the business processes are properly translated into web service composition artifacts. To deploy the business process in the Cloud with the enforcement of the security requirements, the Internal Features can be made use of. VTA (Virtual Travel Agency) was an example systems presented to illustrate the usage of the environment. [65] The utilization of web service composition is done via the business process. There are tools which can be used to ensure security of service composition in the Cloud. Security-related information can be shared among different users in the Cloud and also can be used to enable the activation and configuration of security mechanisms.

Future work of the paper [65] is as follows:

Business process can be simplified to be more scalable. Monitoring the business process execution in the Cloud using the monitored data which makes the expert to improve the business process quality by updating specific configurations [65].

4.5.7 Automating the delivery and positioning cloud computing

The recovery of IT services in the event of a disaster is a very important task. IT Service Continuity Management (ITSCM) delivers the recovery in such cases. ITSCM is usually considered as an expensive challenge for enterprise-class IT operations. [66].

These attributes brings cost-efficiency operation processes. The paper [66] summarizes the use of the Web Service BPEL in combination with Virtual Appliances. This implements the ITSCM processes. The results are compared and evaluated against collected data from manual recovery processes [66]**.**

General ITSCM Architecture and relying base services:

- Architecture Overview
- Service Catalogue
  - Cloud Services
  - Supporting Services
  - People Services
- BPEL Workflows

Delivery of ITSCM:

The delivery of ITSCM is a step by step process and the flow of the steps is as follows

- High-Level ITSCM process
- Implementation & Transition to On-Going Transition
- On-Going Operation
- Service replica VAP update workflow
- Invocation & Recovery

A novel approach for the delivery of ITSCM through orchestrating cloud services, supporting services and people services is elaborated [66]. The basic methodology is separating the IT services into Business Service Configuration Item (BSCI) and Service Business Data (SBD) and thus allowing replicating configuration state and business data on a Virtual Appliance[66].

The Approach has to be evaluated against ITSCM processes that utilize VM live migration and replication [66]. Focusing on Configuration Management of Virtual Appliance based IT landscapes and service migration into the cloud will be the immediate future work.

Positioning Cloud Computing in Machine to Machine Business Models:

Challenges:

Reliability of cloud technologies is one of the very important challenge in positioning the cloud. Due to this decision makers are still unwilling to take the migration path to the cloud infrastructure.

The paper [68] proposes to align business and IT solution required, one of the recommended tool is to use the Business Model Canvas. It is a strategic management template with a visual chart with elements describing a firm's value proposition,customers,infrastructure, and financial viability. The canvas can be a powerful tool to describe and manipulate the business models (defined as the description of the rationale

on how the organization creates, delivers, and capture value [67]). The canvas helps decision makers to design and understand how the business works without getting down in detail operational levels.

The paper [67] attempts to address cloud computing positioning inside the business model canvas framework. It also examines how cloud computing systematically creates values for the organization.

The author of the paper [67] selected Machine to Machine (M2M) as his field of study.M2M,similar to the cloud computing represents a new opportunity for the communications service providers(CSP) like XL Axiata to tap into.

4.5.8 Business model framework

Machine to Machine (M2M) is the concept to connect the traditionally standalone devices to the internet or other server based back-end systems using a variety of wireless as well as wired technology such as cellular [67]. While M2M solution represents a sizeable and growing market opportunity, it is slow to take off especially in the developing countries.

One of the major constraints is on the M2M service platform heavy investments. The investments are considered risky as the prospects of the M2M business are unknown and sometimes hardly predictable. Therefore, finding the right business model which include cloud computing is important. The inclusion of cloud computing can facilitate and accelerate the M2M service offerings [67] and provide a relief to the CSP to focus on the customer relationship management.

5. Conclusion and Recommendations

5.1 Environmental Security

5.1.1 Conclusions and Recommendation

Managing Security of virtual machine images in a cloud environment

To avoid the above mentioned three risks and other possible risks, the author has proposed and discussed Mirage, an image management system. Mirage helps solve several such risks and provides a concrete solution.

The risk management feature to tackle publisher's risk is an Access control framework to regulate VM Image sharing. Each image is owned by a member. The member will grant permission and access to

other users. There are two well defined permissions: Check-in and Checkout. Checkout permission is for a user to retrieve and use the image. If the user makes any changes to the image and wants to store it, he will have to need the check-in permission. Here, we need to know that, if an image is modified and stored as a new image, check-in permission will not be required. The tracking system discussed later will take care of it. By default, the access is set to only the owner and the admin. For any operation, access is needed. This will limit unauthorized access to images.

Image filters are another feature of Mirage where in the images are filtered when publishing and retrieving. These images remove unwanted information from the image like private information like credit card details, passwords, malwares or pirated software etc. The author talks about two types of filters. Repository specific filters talk about the system best practices. A few will be mandatory while the rest may be optional. The user specific ones are used to filter out the user content from the images. These filters are applied by the user of the image. To ensure integrity of the images, the user specific filters are never allowed to be executable code. A few examples of these filters can be “Find and replace” filters, pattern matching filters. Filters can also be applied during retrieve time. These filters are specified by the publisher who decides what content to filter and protect based on access permission of the user. Usually, the repository specific filters are run before the user specific filers to make sure that the user filters run without any problems. All three party’s risks are addressed here. Publisher’s risk of unknowingly giving out private information, retriever’s risk of using harmful or illegal content and admin’s risk of hosting malicious content is reduced.

A good tracking system is also a part of Mirage. We track the history and operations performed on an image. The tracking systems not only enables admin and publishers to audit the images but also help avoid the risk of introduction of malware into the images by malicious users. All updates to the image can also be tracked with the help of the tracking system. When a new image is created, its parent image details and history are also stored along with it. This way, if there is a risk or a vulnerability found in any image, all its parents and children are checked for the same. This way, the maintenance cost comes down. Similarly, security patches are applied to the images.

Finally, the author introduced maintenance operations into the system. The images should be considered as physical assets and should be checked for risks and vulnerabilities, scanned for malicious programs and be regularly updated with the latest security patches regularly. These services perform regular scans to check the health of the images and check for malware, viruses, vulnerabilities and other risks that

may crop up. The author has mentioned a few maintenance services that can be done quickly. This feature reduces the retriever's risk of using illegal content and also the admin's risk of hosting malware.

Security, Privacy and Trust Issues in Cloud Computing Environments

With the advance of cloud computing in practical usage, security, privacy and trust issues should be paid more attention. In order to protect private and sensitive data in the data centers, users need to verify: (1) privacy issues in cloud computing; (2) security information in cloud computing; (3) trustworthiness of the cloud computing.

Data Security and Privacy Protection Issues in Cloud Computing

Data security is important in every stage of the data life cycle in risk management. In addition, we should take steps to protect the privacy issues involving data in each stage.

Considering the service delivery models, deployment models as well as some key characteristics of cloud computing, data security issues should be paid more attention in practical usage. These security issues exist in each stage of data life cycle.

5.1.2 A survey on security issues in service delivery models of cloud computing

Users of cloud computing services should understand the risks of a variety of security issues in the cloud computing environment.

This survey paper gives a detailed explanation of different security issues that exist in each aspect of a cloud computing environment from the risk management perspective.

5.1.3 Case study: Amazon data center outage

The outage was considered one of the biggest roadblock to the growth of cloud computing. Questions were raised about the reliability of cloud and services like Infrastructure as a service. To avoid such a disaster again in the future, a seven risk mitigation steps were designed. We will look at them below:

Plan to fail. Prepare detailed cloud computing breakdown scenarios. Then, perform recovery tests. Make sure your risk mitigation strategy is put in place before starting with cloud environment. It is important to put the design of the risk mitigation before we start and get the cloud running. It is very difficult to predict the failure of a data center and assuming that the failure of a data center will lead

to the start of another data center is not the best risk mitigation strategy. There will be different levels of outages and failures and your solution or risk mitigation strategies should be designed to tolerate all levels of risks. It should also not be limited to the top level only.

Have domain experts with you. One of the myths/notions of cloud computing is that once the cloud is setup, you need not maintain the internal knowledge about the technologies that support the services. The Chief Infrastructure officers of every company should give importance to expert knowledge and research and development of their domain. If you lack the skills and in-house knowledge and capabilities, hire third party consultants and develop a business continuity plan and a disaster recovery plan and be prepared for a potential disaster like a long duration outage.

Test that plan. Test the plans in all possible environment. Just like drills in real-time scenarios, conduct drills with your plans. It is easy to create a test environment and test your plan. The tests will also be a good way to test the robustness of your system and also the performance of the cloud environment. The tests can vary from mild to critical level. Test the system several times and make sure that everything is working as expected.

Create internal back-up options. Never completely depend on the vendor's system. Always have an internal contingency plan and backup. The time to solve an outage will reduce if there are required information about the possibility of the outage. That way, the company can be prepared. All the Information Technology leaders should maintain capabilities to revert to the backup plan in case of an outage.

Reassess your sources and your internal strategy regularly. Many IT companies embrace the multi sourcing strategy wherein they get the sources in multiple companies. This may get confusing when it gets to cloud environment. It will lead to domino-effect during the outage and will lead to a complex situation. The domino effect will come into place because of the services built on cloud. Everything dependent on the cloud will collapse during the outage. At the same time, the responsibility of the infrastructure should not be limited to one person.

Don't be frugal. Most companies affected by the Amazon debacle would not or could not pay to run parallel systems in cloud. A good example of a company that escaped the Amazon debacle was Netflix. The company assumed that one of the 4 web service data centers would go down and were prepared. They made good use of the redundant cloud architecture in AWS and escaped the

consequences. Redundancy plays an important role in outages as the critical data will be found in multiple data centers. The servers are distributed at different locations and active servers make sure that the replications are updated. Definitely all this will be expensive. But the results will be very helpful in situations like outages. Make sure that your vendor is on his heels. The vendor should be the person of contact. The vendor should not be subleasing our contact to someone else. The point of authority should be the direct vendor.

5. 2 Data privacy

Thus by performing the benchmark tests on regular DDL and DML commands, it was found that the performance penalties for read, write and update were nearly in the same range. The creation/write transactions had a more adverse effect on the performance. The space complexity of the system was found to be infeasible with increasing size of input to the encryption. The general points that were taken back from the benchmark experiment was that the introduction of data privacy (encryption of data) had nearly no effect on the start-up time of the system. The greater the input size of the system, the more is the computational overhead of encrypting the data, especially while creation. Data migration on the cloud must rely on encryption for privacy. QoS parameters need to be considered when working with Encryption so as to arrive at the right trade-off between performance and security.

Recommendations and future work:

After understanding the expected quality-availability compromise, the study by *M.R. Aswin* and *M. Kavitha* [28] put forth a compelling risk and data privacy management system in cloud computing. The management of privacy is separated by the characteristic nature of the cloud; be it *private* or *Hybrid*. This is achieved through the use of a privacy manager, whose working process is best described through the following flow graph (*Figure af.4*). The encryption processes involved in the given recommendation is RSA but any strong encryption algorithm should work with the a given long enough key. Their system also involves a keyword generation algorithm that generates keys based on a PRNG function. The risk manager finally evaluates the scenario based on the probability of error, any request for retransmission and whence the data is accepted.

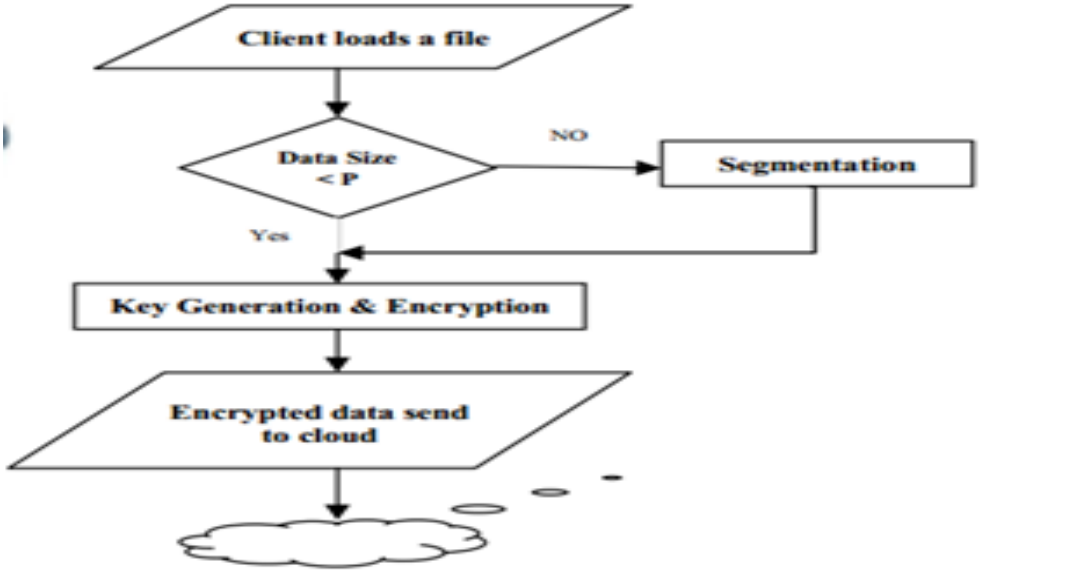

Fig 4 Working process of Data transfer from Client to Intelligent Cloud

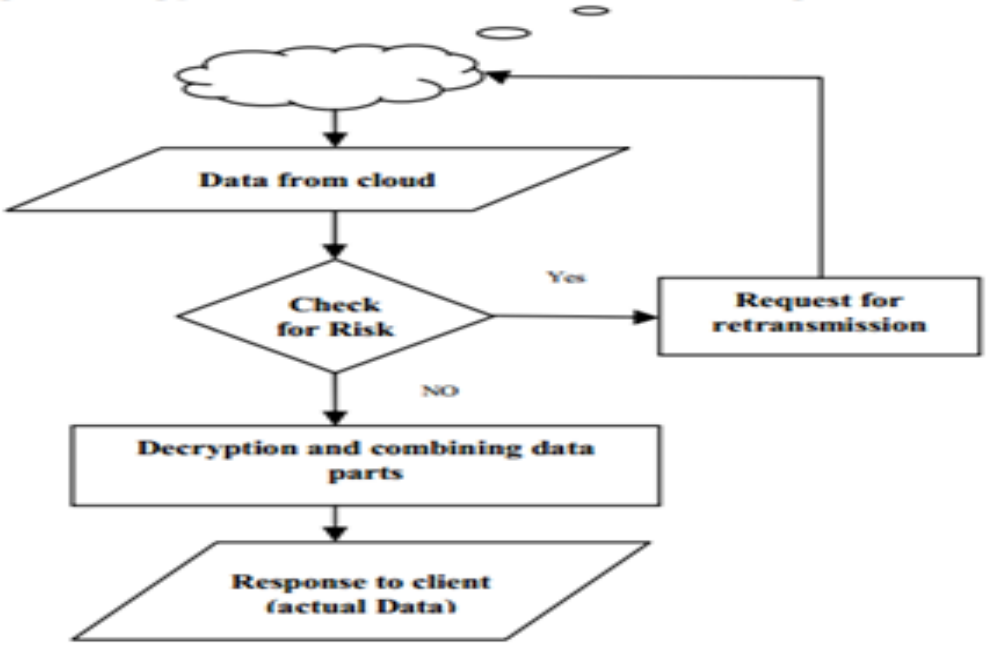

Figure 5.2.1 The Working process of Data transfer from Cloud to Client

Another possible outlook of an implementable model is the one presented by *Ming Li* and *Shicheng Yu* [30] . To assure privacy in searchable cloud data storage devices is a challenging and a much predominant challenge as the biggest outbreak of the cloud environment is cloud as an extended application storage mechanism for personal and private processing data. Whenever computation is outsourced to third parties, business officials often want to ensure proper handling of data and this is proposed as a searchable cloud based system with the placement of a tactical trap-door or overridden key escrow mechanism. This would

allow a first-hand monitoring of content that assures privacy in the processing of information. The above described model is depicted in *Figure 5.2.2.*

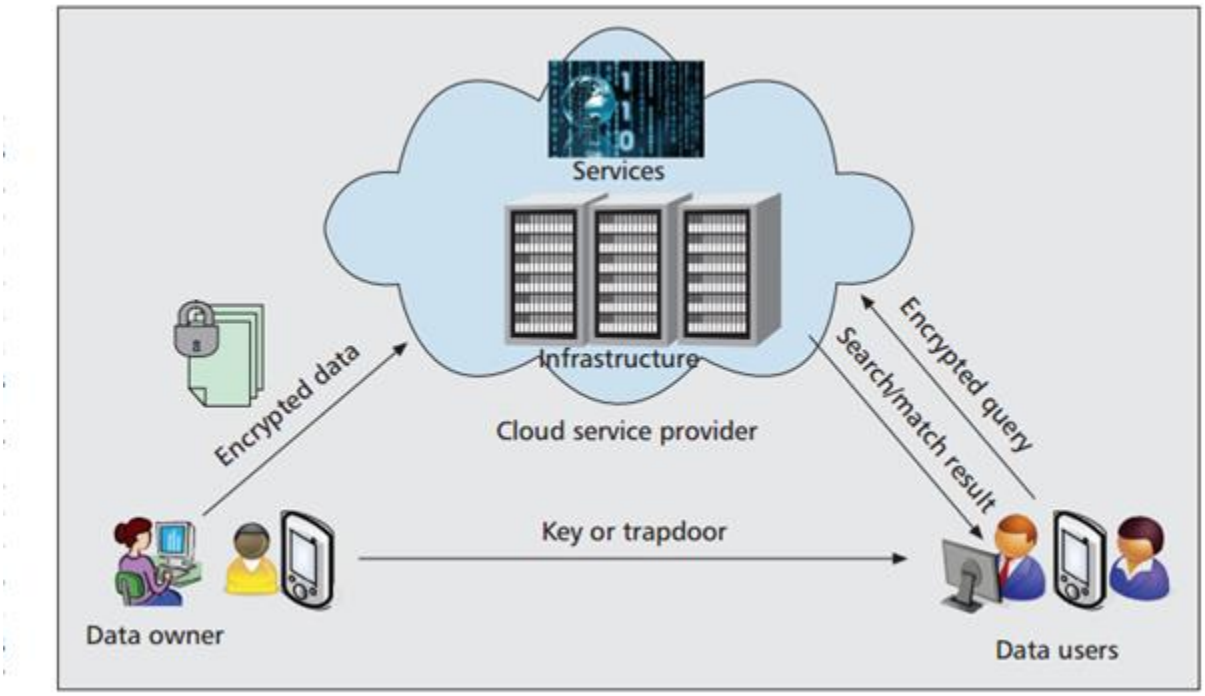

Figure 5.2.2 System Architecture for searchable cloud data storage devices [30]

Privacy deals with the protection of personal information. There are different types of personal information. Personally Identifiable information that may include a person's name, address and contact number. Sensitive information such as a person's religion, sexual orientation, biometric data, usage data and unique device identities.

The fact that the cloud is a very dynamic environment wherein users can change their cloud service on the fly results in data moved within or across the boundaries of an organization, which makes it very crucial to preserve privacy of the data at this point. Cloud provisions new service by combining existing services which may make privacy concerns arise when private data in one service is coupled with another service.

There are a number of principles to be kept in mind while designing a system to preserve the privacy of user data on the cloud. Users must be explicitly informed as to how their data will be used, what they will collect from it and how long it will be used. Users must be given a choice of whether they want to allow their data to be used or not by the cloud provider. At any point only the data that is needed is to be collected and nothing more. Users must have full access to their data at any point of time. There must be

safeguards on the data that prevent unauthorized access, copying or modification. The service provider should adhere to legal regulations in their transactions. The company must audit all activities that take place to the user data.

There are also guidelines for the software developers while designing the systems to keep in mind in order to enforce privacy preservation. Carry out a Privacy Impact Assessment to determine the privacy risks involved. Assess the privacy requirements in the different phases of design such as the initiation, execution, closure and decommission. Make use of privacy enhancing tools such as tools that can inspect server side policies about handling of private data, online access mechanisms for users to check the accuracy of the data and pseudonymization tools that allow individuals to hide their real identities when they are working on the cloud.

There are still a number of challenges that exist in the cloud environment. Enforcing the privacy policies, determining where exactly in the cloud the data processing takes place, determining the processors of the data and the changes in user plan are few issues to determine in the cloud.

It is quite convenient for developers to have privacy templates when designing and use them to fit the scenario. But in situations where additional privacy is needed, a greater analysis would be required during the production phase. A way forward is to bring accountability to the picture wherein the service providers would be obligated and legally bound to secure user data. Such contractual agreements would give customers greater trust in the service and would opt for it with fewer qualms. [4]

5.3 Security in Cloud Computing

- This paper [52] discusses various security threats in cloud computing. And related to real world cloud computing areas each of the threat requires proper analysis of their possible impact. The cloud computing security can be improved by enhancing the security measures for web service frameworks and web browsers, by integrating former into latter. [52]
- While stressing over the performance improvements in Cloud the main security issues are left untouched , some are not yet fully realized, security in complex large scale computing is not yet resolved, quality implementation is not yet achieved. Cryptography and trusted computing control the security of cloud infrastructure. Keeping in mind that liability of the security remains with the organization the risks must be equally distributed between the expected benefits and available safeguards. If the advantages are more than the related risks and costs then many controls related

to it are useless. [53]. MCC should be used in scenarios wherein the advantages of MCC overcome or outdo the disadvantages of MCC.

- As cloud computing is often provided as a service the security issues are handed over to the third part to develop a trustworthy relation between service providers and users. The risk management framework can be used for all the cloud deployment and service models and can be used for analysis, assessment and mitigation of the risks. The main goal is to apply this Risk management framework model successfully to cloud information systems which can cause admirable difference. [54]
- The third party services are used for handling security issues in the cloud computing environment which can provide efficient security and vulnerability management service. But the security concerns discussed are major and there is a need for critical reevaluation of the solutions. Many improvements are needed in the solutions to make the cloud computing benefits are utilized without any hazard. Cloud computing can excel further from its infancy if the security landscapes are changed. [55]
- IAM sets aside clearly defined guidelines with respective to application access, revoking access rights/privileges of users for application access etc. However, it also lacks monitoring of setups in IAM [35] which is tough to implement and lacks control over sensitive information. Thus, IAM should be enforced in scenarios where these cons can be taken care of or mitigated.
- SLA's should be oriented towards keeping all the parties interests into consideration, and not just the customers. TCCP is used to ensure VM's are run in trusted mode, in order to ensure data is not leaked or tampered with due to virtualization.

5.3.1 Strengths and Weaknesses of Risk management in Security in Cloud Computing

Strengths

- Main drivers for security in Cloud Computing are Economic benefits because it reduces the Operational and capital expenditure. [52]. For handling sensitive information on cloud proper auditing, encryption is used. The cloud security and privacy issues are addressed by using different categories which is more effective. [53]
- Your location doesn't hinder you from accessing the cloud, which provides significant flexibility in using the cloud computing services. It also allows you to access personal laptops, mobiles or any portable devices [48]. Data is available real-time, which means it can be available any time of the day [48]

- MCC provides support on multiple platforms, thus allowing the applications to be accessible on android phones, iPhones etc. [48]. There is no significant costs incurred on licensing, upgrades etc. [48].
- There are scalable, cost- effective and efficient ways to deliver organizations over internet provided by Cloud computing. Flexibility for delivering both new services and support for business functions there are various cloud computing models available. [54]
- Cloud computing enables suitable and necessary access to a shared pool of resources (all the computing paradigms). The access is with minimum hassle and can be provisioned quickly. The cloud computing model encourages availability and five characteristics as rapid elasticity, location-independent resource, on-demand self-service, pooling and measured service and ubiquitous network access. [55]
- IAM framework detects and prevents significant threats impacting the security of the organization, as every aspect of application access is properly documented in this framework, thus allowing the organization to pinpoint the area of security breach, and provide countermeasures to make it more secure in future. IAM also handles evolution in the IT environment space, by taking personal devices like laptops, and mobile phones into consideration, for which there needs to be efficient management of secure access to applications. IAM places consideration on employees migrating across different departments or roles, or even migrating to another organization. IAM architecture will support not only the services in the cloud ,but also the deployments which are on- premise .Thus, resources available on premise will also adhere to IAM guidelines to ensure no breach of security from external threats.
- Service providers covered in SLA's provide better delivery of service in terms of response time, quality than service providers not covered under SLA's [42]. Trusted Platform ensures the data is confidential, secure and maintains the integrity of data. Trusted Platform enables the user to predict whether the given VM system in Infrastructure-as-a-service (Iaas) has the ability to integrate the above mentioned properties into their system [46].
- TCCP is a closed box environment meaning that the architecture undergoes minimal changes throughout the process [46]. Trusted Virtual machine monitor (TVMM) is an integral component of TCCP, which enables the execution of these VM's to take place on a trusted node [46]. TVMM enables protection of the state of the VM from modification when in a network transit [46].

Weaknesses

- The user data leaves the protection area and released into cloud which has cross domain internet connections hence there are trust and security issues. [52] For maintaining complete security to the

cloud services outsourcing is used which can be which can cause issues because it doesn't guarantee that the arrangements will be maintained throughout the agreement. The needs of organizations and the cloud computing services available are not mentioned in any proper service contract. Which makes it difficult to manage the security as per the organization's rules. [53] Performance of these applications isn't up to the mark as the native applications. Thus in such cases, getting the reviews of the respective service providers can help make up your mind [48].

- Security of data needs to be protected from breach while transferring data across the mobile network [48]. Internet connectivity needs to fast in order to use the mobile cloud services [48]. As various cloud computing models are present for openness and flexibility, it has created a lot of security concerns. The security processes are invisible behind different levels of abstraction. [54]
- The threats increase as the amount of data increases in Cloud. Regulatory compliance in cloud computing security is a major concern. The system becomes vulnerable not only from the hackers but also from inside attacks and causes serious security issues. [57]
- Issue of Orphan accounts where there are accounts created for users but no ownership assigned to the user account [35]. These accounts are the ones rarely used or discrepancies when there are multiple users having same name or last name. Setups of IAM lacks from a monitoring perspective which is hard to implement [35]. IAM lacks control over users who have access to sensitive information in applications or the privileged access irrespective of numerous tools available. Performance goals which are not met are tolerated to a very little extent [42]. Not clearly defined guidelines can lead to dramatic increase in negative service experience [42].
- No appropriate approval is given to user identities and the privileges assigned to application access[35] which meant the newly recruited employees are assigned similar access level to applications although the skill level of previous employees may have earned them higher access , which shouldn't have been distributed to any other users.
- Virtualization leads to spawning of VM's which leads to high system resource utilization [46]. Virtualization risks the confidential data be compromised as the data can be leaked since the data is being accessed from a VM from a remote desktop [46].
- Recommended practices suggested by the vendor may not be used by the organization making it susceptible to security risks [46]. Integrity checks are not carried out by the system on loading in order to ensure if the hypervisor is still secure or its security has been compromised [46].

5.4 Availability and Capacity Limitation

Security aspects that are overlooked in the Cloud Computing realm is the lack of trust of end users in the cloud. Because of this, the users tend to not put sensitive data on the cloud, therefore need for private clouds arise. Private clouds are more expensive and require more efforts for maintenance.

In order to manage risks, we first and foremost need to identify them, in other words we need to extract the risk factors. Extraction involves categorizing risks into divisions and subdivisions according to the areas that they are affecting.

We observe that availability and capacity limitation is interlinked. So if the risks involved in capacity limitation are tackled then it will automatically help in the handling availability efficiently. The approaches mainly studied for availability are “HAIL” and “load balancing”. These approaches can ensure that there is no hindrance in the availability of the cloud services despite the challenges that come forth in the working of cloud in real time and if there are issues then ways and means to handle them dynamically with minimum down time.

5.5 Business Continuity in Cloud services

The security of user’s data is very critical in any organization. There are a number of risks associated with cloud computing. One of the major risks is the loss and misplacement of user data in any organization. In the worst case scenarios such as natural disaster there is a very high chance of the critical data being mispalced. So the organizations have started using the data on the cloud. By implementing the two services such as Business continuity and disaster recovery in cloud computing, this ensures that there is no loss and misplacement of critical data. The business are implemented virtually which makes the business more secure.

6. References

[1] Dimitrios Zissis and Dimitrios Lekkas. “Addressing cloud computing security issues.” Future Generation computer systems, 28(3):583–592, 2012.

[2] Lori M Kaufman. “Data security in the world of cloud computing. Security & Privacy”, IEEE, 7(4):61–64, 2009.

[3] Hassan Takabi, James BD Joshi, and Gail-Joon Ahn. “Security and privacy challenges in cloud computing environments.” IEEE Security & Privacy, (6): 24–31, 2010.

[4] Wenjuan Li and Lingdi Ping. “Trust model to enhance security and interoperability of cloud environment.” In Cloud Computing, pages 69–79. Springer, 2009.

[5] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, and Peng Ning. “Managing security of virtual machine images in a cloud environment.” In Proceedings of the 2009 ACM workshop on Cloud computing security, pages 91–96. ACM, 2009.

[6] Subashini Subashini and Veeraruna Kavitha. “A survey on security issues in service delivery models of cloud computing”. Journal of network and computer applications, 34(1):1–11, 2011.

[7] Dawei Sun, Guiran Chang, Lina Sun, and Xingwei Wang. “Surveying and analyzing security, privacy and trust issues in cloud computing environments.” Procedia Engineering, 15:2852–2856, 2011.

[8] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. “A view of cloud computing.” Communications of the ACM, 53 (4):50–58, 2010.

[9] Deyan Chen and Hong Zhao. Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, volume 1, pages 647–651. IEEE, 2012.

[10] http://www.cio.com/article/2408838/outsourcing/mitigating-the- risk-of- cloud-services- failure--how-to-avoid-getting- amazon-ed.html

[11] http://www.businessinsider.com/amazon-outage- enters-its- second-day- lots-of- sites still- down-2011- 4

[12] http://www.zdnet.com/article/seven-lessons- to-learn- from-amazons- outage/

[13] Y. Zhang and J. Joshi, “Access Control and Trust Management for Emerging Multi-domain Environments,” Annals of Emerging research in Information Assurance, Security and Privacy Services, S. Upadhyaya and R.O. Rao, eds., Emerald Group Publishing, 2009, pp. 421–452.

[14] D. Reimer, A. Thomas, G. Ammons, T. Mummert, B. Alpern, and V. Bala. Opening black boxes: Using semantic information to combat virtual machine image sprawl. In The 2008 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, March 5-7, 2008.

[15] Sun, Yunchuan, et al. "Data security and privacy in cloud computing." *International Journal of Distributed Sensor Networks* 2014 (2014).

[16] Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." *INFOCOM, 2010 Proceedings IEEE*. Ieee, 2010.

[17] Pearson, Siani, and Azzedine Benameur. "Privacy, security and trust issues arising from cloud computing." *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*. IEEE, 2010.

[18] Pearson, Siani. "Taking account of privacy when designing cloud computing services." Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. IEEE Computer Society, 2009.

[19] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. IEEE, 2011.

[20] Pearson, Siani, Yun Shen, and Miranda Mowbray. "A privacy manager for cloud computing." *Cloud Computing*. Springer Berlin Heidelberg, 2009. 90-106.

[21] Sun, Yunchuan, et al. "Data security and privacy in cloud computing." *International Journal of Distributed Sensor Networks* 2014 (2014).

[22] Xiao, Zhifeng, and Yang Xiao. "Security and privacy in cloud computing." *Communications Surveys & Tutorials, IEEE* 15.2 (2013): 843-859.

[23] Ashktorab, Vahid, and Seyed Reza Taghizadeh. "Security threats and countermeasures in cloud computing." *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* 1.2 (2012): 234-245.

[24] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. IEEE, 2011.

[25] Hu, Ji, and Andreas Klein. "A benchmark of transparent data encryption for migration of web applications in the cloud." *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on*. IEEE, 2009.

[26] Jensen, Meiko, et al. "On technical security issues in cloud computing." *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*. IEEE, 2009.

[27] Pearson, Siani, and Azzedine Benameur. "Privacy, security and trust issues arising from cloud computing." *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*. IEEE, 2010.

[28] Aswin, M. R., and M. Kavitha. "Cloud intelligent track-Risk analysis and privacy data management in the cloud computing." *Recent Trends In Information Technology (ICRTIT), 2012 International Conference on*. IEEE, 2012.

[29] Gourkhede, Manish H., and Deepti P. Theng. "Analysing Security and Privacy Management for Cloud Computing Environment." Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on. IEEE, 2014.

[30] Li, Ming, et al. "Toward privacy-assured and searchable cloud data storage services." Network, IEEE 27.4 (2013): 56-62.

[31] The Wall Street Journal online article:
http://www.wsj.com/articles/SB10048155787068412 80

[32] Margaret Rouse, “Identity Access management (IAM) system “, Mar 2015 , SearchSecurity Techtarget
http://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

[33] Ericka Chickowski, “Identity Management In The Cloud ”,Oct 2013, InformationWeek DarkReading. http://www.darkreading.com/identity-management-in-the-cloud/d/d-id/1140751

[34] Fran Howarth, “Identity management in the cloud: Top tips for security identities ”Apr 2014, IBM SearchIntelligence. https://securityintelligence.com/identity-management-cloud-tips-secure-identities-iam/

[35] Bryan Glick," The business challenges and benefits of identity and access management", Nov 2014, TechTarget ,Computerweekly. http://www.computerweekly.com/feature/The-business-challenges-and-benefits-of-identity-and-access-management

[36] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." *Journal of Internet Services and Applications* 4.1 (2013): 1-13.

[37] Younis, M. Y. A., and Kashif Kifayat. "Secure cloud computing for critical infrastructure: A survey." *Liverpool John Moores University, United Kingdom, Tech. Rep* (2013).

[38] De Chaves, Shirlei Aparecida, Carlos Becker Westphall, and Flavio Rodrigo Lamin, "SLA perspective in security management for cloud computing" In Networking and Services (ICNS), 2010 Sixth International Conference, IEEE, 2010, pp. 212-217.

[39] Muhammad Imran Tariq, Dr. Irfan Ul Haq, Javeed Iqbal, "SLA Based Information Security Metric for Cloud Computing from COBIT 4.1 Framework", Aug 2013, International Journal of Computer Networks and Communications Security.http://www.ijcncs.org/published/volume1/issue3/p4_1-3.pdf

[40] Wu, Linlin, and Rajkumar Buyya. "Service Level Agreement (SLA) in utility computing systems." *IGI Global* (2012).http://www.cloudbus.org/reports/SLA-UtilityComputing2010.pdf

[41] Jin, L. J., & Machiraju, V. A. (June 2002). Analysis on Service Level Agreement of Web Services. Technical Report HPL-2002-180, Software Technology Laboratories, HP Laboratories.

[42] Tom Sweeny, "The Benefits of Offering SLAs", 2015, ServiceXRG http://www.supportindustry.com/asktheexpert/benefits_slas.htm

[43] Younis, M. Y. A., and Kashif Kifayat. "Secure cloud computing for critical infrastructure: A survey." *Liverpool John Moores University, United Kingdom, Tech. Rep* (2013). https://www.researchgate.net/profile/Younis_A_Younis/publication/262817790_Secure_Cloud_Computing_for_Critical_Infrastructure_A_Survey/links/5465ed3e0cf2f5eb180130d5.pdf

[44] Popović, Krešimir. "Cloud computing security issues and challenges."*MIPRO, 2010 proceedings of the 33rd international convention*. IEEE, 2010. https://www.researchgate.net/profile/Ibikunle_Ayoleke/publication/259072387_Cloud_Computing_Security_Issues_and_Challenges/links/0deec529df37a5aa28000000.pdf

[45] Siddharth Coontoor,"Risk analysis and mitigation in virtualized environment", Feb 2015,ICST, EAI Endorsed Transactions. http://www.slideshare.net/SiddharthCoontoor/risk-analysis-and-mitigation-in-virtualized-environments

[46] Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. "Towards Trusted Cloud Computing." *HotCloud* 9 (2009): 3-3. https://mpi-sws.org/~gummadi/papers/trusted_cloud.pdf

[47] Donald, A. Cecil, and L. Arockiam. "Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues." *International Journal of Computer Applications* 94.1 (2014). http://research.ijcaonline.org/volume94/number1/pxc3895537.pdf

[48] "Mobile Cloud Computing – Pros and Cons",Dec 2014, GetCloudServices. http://www.getcloudservices.com/blog/mobile-cloud-computing-pros-and-cons/

[49] Angin, Pelin, et al. "An entity-centric approach for privacy and identity management in cloud computing." Reliable Distributed Systems, 2010 29th IEEE Symposium on. IEEE

[50] Al-Anzi, Fawaz S., Santosh Kumar Yadav, and Jignesh Soni. "Cloud computing: Security model comprising governance, risk management and compliance." Data Mining and Intelligent Computing (ICDMIC), 2014 International Conference on. IEEE, 2014.

[51] Tanimoto, Shigeaki, et al. "Risk management on the security problem in cloud computing." Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on. IEEE, 2011.

[52] Jensen, Meiko, et al. "On technical security issues in cloud computing."Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.

[53] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE, 2011.

[54] Zhang, Xuan, et al. "Information security risk management framework for the cloud computing environments." Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on. IEEE, 2010.

[55] Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and privacy challenges in cloud computing environments." *IEEE Security & Privacy* 6 (2010)

[56] Grobauer, Bernd, Tobias Walloschek, and Elmar Stöcker. "Understanding cloud computing vulnerabilities." *Security & privacy, IEEE* 9.2 (2011)

[57] Jude Chao, "Cloud computing and cloud security" , June 2014, Enterprise Networking Planet http://www.enterprisenetworkingplanet.com/netsysm/cloud-computing-and-cloud-security-tech-trends-cheat-sheet-part-2.html

[58] Amziani, Mourad, Tarek Melliti, and Samir Tata. "Formal modeling and evaluation of service-based business process elasticity in the cloud." Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2013 IEEE 22nd International Workshop on. IEEE, 2013.

[59] Sellami, Wael, Hatem Hadj Kacem, and Ahmed Hadj Kacem. "Elastic multi-tenant business process based service pattern in cloud computing. " Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. IEEE, 2014.

[60] Sun, Hongjun, et al. “Configuration and Optimization of Virtual Business in Cloud Computing Environment.” Cloud and Green Computing (CGC), 2012 Second International Conference on. IEEE, 2012.

[61] Staalinprasannah, N., and S. Suriya. “Implementation of Xenserver to ensuring business continuity through power of virtualization for cloud computing.”Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.

[62] Fitó, J. Oriol, and Jordi Guitart. "Initial thoughts on business-driven IT management challenges in Cloud computing providers." Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on. IEEE, 2011.

[63] Zhongping, Zeng, Yang Kaifeng, and Zhou Peipei. “Increasing Employees’ Awareness and Enhancing Motivation in E-Government Security Behavior Management.” 2013 Fourth International Conference on Digital Manufacturing & Automation (ICDMA). IEEE, 2013..

[64] Hwang, Jing-Jang, et al. “A business model for cloud computing based on a separate encryption and decryption service.” Information Science and applications (ICISA), 2011 International Conference on. IEEE, 2011.

[65] Lins, F., et al. “ Ssc4cloud tooling: An integrated environment for the development of business processes with security requirements in the cloud. “ Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.

[66] Klems, Markus, et al. “Automating the delivery of IT Service Continuity Management through cloud service orchestration.” Network Operations and Management Symposium (NOMS), 2010 IEEE. IEEE, 2010.

[67] Juliandri, Arkav, and Meis Musida. “ Positioning cloud computing in machine to machine business models.” Cloud Computing and Social Networking (ICCCSN), 2012 International Conference on. IEEE, 2012.

[68] A. Osterwalder & Y. Pigneur, “Business model generation,” New Jersey, John Wiley & Sons, 2010.

[69] Kurt Hilderbrandt. “Take Business continuity in cloud” http://www.cio.com/article/2871275/business-continuity/take-business-continuity-to-the-cloud.html,2015

[70] McNeil, Alexander J., Rüdiger Frey, and Paul Embrechts. *Quantitative risk management: Concepts, techniques and tools*. Princeton university press, 2015.

[71] Carroll, Mariana, Alta Van Der Merwe, and Paula Kotze. "Secure cloud computing: Benefits, risks and controls." *Information Security South Africa (ISSA), 2011*. IEEE, 2011

[72] Tanimoto, Shigeaki, et al. "Risk management on the security problem in cloud computing." *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on*. IEEE, 2011.

[73] Paquette, Scott, Paul T. Jaeger, and Susan C. Wilson. "Identifying the security risks associated with governmental use of cloud computing."*Government Information Quarterly* 27.3 (2010): 245-253.

[74] Chaczko, Z. C., et al. "Availability and load balancing in cloud computing."*International Conference on Computer and Software Modeling IPCSIT 2011,*. IACSIT Press, Singapore, http://www. ipcsit. com/vol14. htm, 2011. Analysis of Load Balancing Techniques in Cloud Computing

[75] Sidhu, Amandeep Kaur, and Supriya Kinger. "Analysis of load balancing techniques in cloud computing." *International Journal of Computers & Technology* 4.2 (2013): 737-41.

[76] Juels, Ari, and Alina Oprea. "New approaches to security and availability for cloud data." *Communications of the ACM* 56.2 (2013): 64-73.

[77] Bowers, Kevin D., Ari Juels, and Alina Oprea. "HAIL: a high-availability and integrity layer for cloud storage." *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009.

[78] Brender, Nathalie, and Iliya Markov. "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies."*International journal of information management* 33.5 (2013): 726-733.

[79] Sethi, Srinivas, Anupama Sahu, and Suvendu Kumar Jena. "Efficient load balancing in cloud computing using fuzzy logic." *IOSR Journal of Engineering*2.7 (2012): 65-71.

****