Vol No. III Issue No. IV APRIL 2015 ISSN: 2347 5587

CKPIM BUSINESS REVIEW

C.K. Pithawalla Institute of Management

Online ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Online ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Editorial Review Board Members

CKPIM BUSINESS REVIEW

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Index

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Security and Privacy issues in Cloud Computing

Siddharth Walia*

ABSTRACT

Cloud computing is a rapidly developing technology using internet and remote servers to maintain data and applications. The main aim of cloud computing is to provide on-demand services with scalability, reliability and availability. IBM, Amazon, Google, Microsoft are making millions of dollars each day by providing cloud services to users all over the world. In this paper, we provide an overview of cloud computing and then discuss some of the major security and privacy issues occurring in the cloud environment. We discuss about the techniques and approaches proposed by researches to tackle these problems. Some of the issues we discussed in the paper are privacy, integrity, security, trust, compliance and availability.

1. INTRODUCTION

Computers have always been in their evolving phase. From the very beginning of invention of computers, we see a constant evolution from bulky computers to small mobile de- vices we used these days. With the rapid success of internet and the large scale development in the hardware for storing and processing big data, the computing resources which once used to be highly expensive are now available at reasonable prices. This technological evolution had led to the development of new computing model called the cloud computing [?], in which the general utilities such as processors or external storage are leased or released by the users in an on-demand fashion.

According to the official NIST definition [24], "cloud computing is a model for enabling ubiquitous, convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and re- leased with minimal management effort or service provider interaction." Cloud computing enables users to access the resources via the internet without the restrictions of technical or physical issues of the resources. The users have the freedom to access the resources anytime, anywhere. Google, Amazon, Microsoft are paramount examples of cloud computing which enables users to access services from these firms to utilize their resources all over the world on mil- lions of machines connected to the internet.

The main reason for huge success of cloud computing is that the users do not have to worry about managing or maintaining the resources provided to them. They just have to pay on the go to use these services. These services are provided by cloud service providers (CSP) who are responsible for maintaining data at data centers (DC).

*Queen's University, Kingston, Canada

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

The data centers have high storage capacity for storing user data and these are placed in clusters over storage area networks (SAN)[26]. The leading service providers are Google AppEngine, Amazon EC2, Microsoft Azure providing high quality computational and data storage devices to the users at low cost.

With the growing popularity of cloud computing, the security of cloud computing has become a major research area for the researchers all over the globe. The users are becoming familiar with the risks of storing their valuable data at some place that they are not aware of (data centers). Also, there have been incidents indicating that the cloud computing services are not totally secure [9]. In 2009, failures occurred in Amazon and Google docs lead to forced stop of services that were relying on these service providers. Private information was aslo compromised from the Google server leading to a lot of insecurity among the users. Similar incident took place with Microsoft's Azure when it went out of service for almost 22 hours. Thus researchers are trying to find the reasons for these problems and proposing techniques/approaches to mitigate these risks. In this paper we will discuss about some of the major issues with cloud security and the solutions provided/proposed by the researchers to eliminate them.

2. CLOUD COMPUTING OVERVIEW

Cloud computing enables the user to access the shared pool of resources (e.g., networks, servers, storage, applications, and services) on-demand at any time. The high availability of resources is facilitated by the five essential characteristics of the cloud, three delivery models, and four deployment models [45][29][44].

A. The five main characteristics of cloud computing are:

• On-demand self-service: a customer can acquire re- sources such as processing, storage or software utilities with- out any human interaction with the providers.

• Resource pooling: a multi-tenant model is used for pooling the resources to provide multiple customers. The customers have no knowledge about the location of the re- sources.

• Rapid elasticity: the resources provided to the customers are scalable i.e. they can be scaled up or down according to the needs of the customers. These resources appear to be infinite from the customer's point of view so they do not have to worry about the depletion of these re- sources.

• Broad network access: the resources are made avail- able on all networks and can be accessed by any platform such as laptops, desktops, mobile phones and tablets.

• Measured Service: the usage of resources by the customers can be measured anytime by the customers to keep a check on their utilization. The monitoring,

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

controlling and reporting of resources is transparent to both customers and the providers[45].

A lot of new features have been added by Microsoft[8], Google[5] and other big companies to add high availability (making data available even in times of system failures) to their ser- vices so that the users can enjoy uninterrupted services 24*7. The need for such systems came into existence when some applications required strong ACID semantics and high fault- tolerance which could be provided by replicating the data over several datacenters.

For better understanding of the cloud, we will now take a look into the service[27][43] and deployment models of the cloud.

B. Service models

Software-as-a-Service (SaaS): Software as a service is the form in which the user is not required to purchase the software installed on their local machine or the server, but just leases the software. This is a "pay-as-you- go" model leased by specialized SaaS vendors. In some of the cases, the software is free, but the user gets limited functionality. This functionality can be expanded by paying more to the vendors so they can grant greater access to the users. SaaS services are accessed through the web browsers over the internet, thus web browser security is essentially important for proper deployment of SaaS model. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) are some of the options available for enforcing security in web browsers. The major applications of SaaS are e-mail services, web conference, network fax, online antivirus and on-line entertainment applications such as Web search, online games and online video and management services. SaaS is considered as the future of soft- ware industry; Microsoft, Salesforce and other big firms are launching their SaaS applications to provide services to the users.

Platform-as-a-Service (PaaS): Platform as a service is used for providing a complete platform for application de- signs, application development and application hosting. It works like IaaS, but provides an additional "rented" functionality.

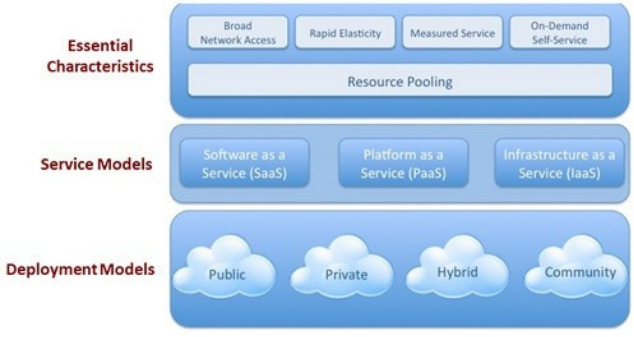

Figure 1: Cloud Architecture

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

The users using PaaS can build applications without actually installing hardware or software on their computer system. This largely reduces the cost of developing wen applications as compared to platforms based on data centers. PaaS is further useful in development of SaaS applications and adds to the efficiency of the development. The use of virtual machines highly increase the performance of PaaS, thus these virtual machines must be protected again malicious attacks. Some of the common examples of PaaS are the Facebook development platform and Microsoft Windows Azure platform.

Infrastructure-as-a-Service (IaaS): Infrastructure as a service refers to the service in which the users can use cloud computing technology without purchasing servers, software, data center space or network equipment. This is pay-per- use model which highly decreases the initial investment for cloud computing hardware. The users have to pay for consuming the processing power, disk space etc. Compared to SaaS, the application of IaaS needs more development and research for proper deployment. Some of the big IT giants providing IaaS services are Microsoft, Amazon, Century Internet and much more. Some of the common examples of IaaS services are Dropbox, Amazon Web Services, Mozy, Akamai.

Hardware-as-a-Service (HaaS): According to Nicholas Carr[17], "the idea of buying IT hardware or even an en- tire data center as a pay-as-you-go subscription service that scales up or down to meet your needs. But as a result of rapid advances in hardware virtualization, IT automation, and usage metering and pricing, I think the concept of hardware-as-a-service, let's call it HaaS, and may at last be ready for prime time."

C. Deployment Model

Public cloud: In public clouds, a single service provider provides computational resources to multiple customers. The customers can access the resources and pay for operating these resources. Public clouds are not as secure as private clouds because of their open structure. One of the options of enforcing security in public clouds are mutual agreements between the users and the cloud vendors in sharing joint responsibility for keeping a check across their own systems. In spite of numerous advantages of public clouds, the shortcomings of public clouds are security threats, regulatory compliance and quality of service (QoS).

Private cloud: The shortcomings of public clouds are re- moved by Private clouds by enforcing security, compliance and QoS. A private cloud is set up within an organization's internal enterprise data center. The cloud is managed and operated by the organization or a third party regardless of its locations. In a private cloud, the vendor provides scalability of resources and virtual applications to the users. Sometimes, only the designated stakeholders of an organization have access to the private cloud.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Hybrid cloud: A hybrid cloud is typically a private cloud combined with one or more external clouds. It is used for optimizing the resources by moving the less important business to a public cloud whereas keeping the core business to a private cloud. It is used for providing secure IT solutions to an organization. It can also be used to divide the workload of an organization and shift the business to a public cloud at peak times.

Community cloud: a community cloud is set up and shared by a number of organizations based on similar requirements and interests for reducing the utilization cost. The community cloud can be managed by a third party vendor or one of the organizations in the community.

D. Supporting techniques

Cloud computing has leveraged a large number of existing techniques for providing highly efficient services to the customers. Some of these techniques are Data Center Networking (DCN), Virtualization, distributed storage, MapReduce, web applications and services, etc.

Data center is a facility used for housing different components used for cloud computing, it has been practically employed as an effective carrier of cloud environments. Data centers are used by cloud service providers to store and process large chunks of data at different locations.

Virtualization means to create a virtual version of a de- vice, resource or even an operating system. Virtualization has been widely used in cloud computing to provide dynamic resource allocation and service provisioning.

MapReduce[11] MapReduce is a programming model for processing large data sets with a parallel, distributed algorithm on a cluster. It is composed of a Map() procedure that performs filtering and a Reduce() procedure that performs a summary operation. It breaks large data sets down into small blocks that are distributed to cloud servers for parallel computing. It is used for speeding up the computation power of the cloud environment.

Due to the large number of benefits attached to cloud computing, it is being extensively used by big IT giants like Amazon, Google, Microsoft, Yahoo and Facebook. Because of the little initial installation cost involved with cloud computing, the startup companies are using more of cloud computing resources to cut down their initial expenses. Dropbox uses cloud computing for its daily functioning. Other companies are also moving towards cloud computing for reducing their overall cost of storage and processing of resources. As more and more companies have started utilizing cloud resources, the question arises about the security of data being stored at the clouds. Is the valuable data of the user stored in a cloud safe? How users feel about storing his valuable data at some location which he is unaware of ? To answer these questions, we take a look into the various

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

security concerns related to cloud computing and the solutions proposed/provided by the researchers to conquer these is- sues.

3. CLOUD COMPUTING ISSUES

As the data is stored on the cloud, a lot of questions rise about the security of the data, especially the confidentiality of the data because the cloud users are utilizing the same infrastructure shared by other users. These issues hinder the progress of cloud computing as it bothers both users and the service providers. Researchers are developing techniques to tackle these problems from the point-of-view of both users and the service providers. This paper focuses the following major issues related to cloud computing:

- Security
- Privacy
- Confidentiality
- Integrity
- Availability
- Accountability
- Audit and Compliance
- Multi-tenancy

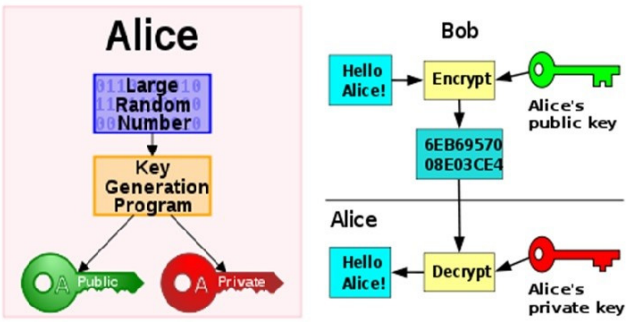

Figure 2

3.1 Security

As per Algirdas [4], security is ”the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of the unauthorized withholding of information”. One of the most common question that arises is, Is the data stored in the clouds secure or not? People have different

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

opinions on this; some say that the data is safer at their local computer where it can be managed internally by the users, whereas some say that the data is safer in the clouds because of the high security levels of the clouds. The cloud users do not know the location where there data is stored. It is generally distributed over different servers placed in different location. Based on this, it is very important to protect the user's data against theft or loss.

Figure 2: Cryptography

Security in cloud computing can be divided into Data security and Application Security. In Data security there is threat of misuse of user data stored on a shared drive used by other users. To protect the user data, the data is usually stored in scattered locations, and stored in plaintext form. Although firewalls are used for data protection, some of the data is lost or misused by malicious attack. Other way to protect users data is to used cryptography techniques (Figure 2) in cloud computing where a key is used to decrypt the encrypted data, this adds to the complexity of the system and the data is lost is the key is lost. But, this techniques adds to the security level of the cloud computing. Arora[2] discuss about various algorithms that can be used for making cloud computing more secure. In their study, they compared different algorithms (AES, DES, Blowfish and RSA algorithms) to find the best algorithm against cloud hackers.

In Application security, different application layers are made secure for better computing. In SaaS security mode, the security is provided by the service providers and the users do not have to pay much attention to it. For PaaS security, the users have to configure their infrastructure for imposing security in their system, the service providers do not have a great part to play in PaaS security, and they just guarantee the security of the software platform which is being utilized by the users. In IaaS security mode, the cloud providers are not at all responsible for securing the system; the users are responsible for safeguarding their systems.

Gartner highlighted a few security issues that the users should discuss with the cloud providers before using the services[16]: Privileged access to keep a check on who is using the cloud services

Regulatory compliance to check if the vendor is willing to undergo security certification

Data location to have a control over the datacenter

Data segregation for reliable encryption and decryption of data

Data recovery in case of disaster

Investigative support to keep a check on the illegal activities Data availability to check if the data is available all the time to the users

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

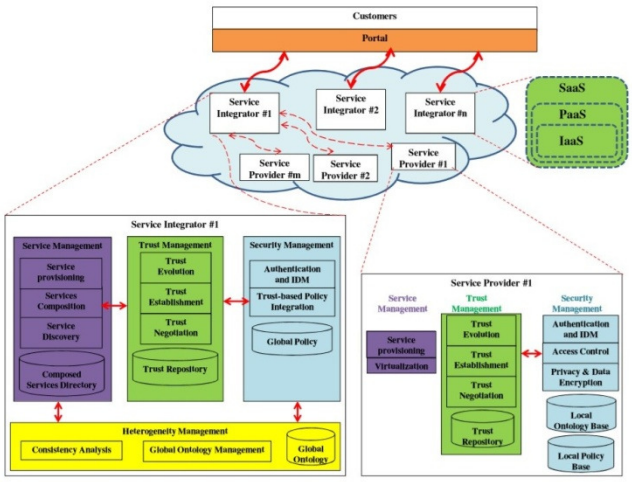

Figure 3: Security Framework For Cloud Computing Environments

Takabi[35] proposed a framework for cloud security as show in Figure 3. The Service integrator is used for combining various service providers by composing new services consisting of components enforcing trust between services pro- vided. The authentication and identify management module authenticates the users based on their credentials and characteristics. Other key modules like access control module, data encryption module, trust-based policy integration (TPI) module, service discovery module, service composition module are responsible for maintaining secure connection between the clients and the cloud service providers.

Wie[40] proposed Sec Cloud, an auditing scheme for securing the cloud environment based on probabilistic sampling techniques. The main aim of the author is to provide secure data storage, computation and privacy preservation. The authors were the first to investigate both computational and storage security of user data. They aimed at cutting down the auditing cost by optimizing the sampling size by taking into account multiple servers and cloud service providers. Experimentation conducted by the authors show that the protocol developed by the authors is secure and effective for achieving cloud security. In another paper, authors describe of having a privacy manager to protect data from being misused by an attacker. They suggested that the privacy manager can be placed at client's end or in the cloud for safeguarding the data. Researchers have proposed many frameworks[37] for enforcing data security in cloud computing environment, they discuss critical topics like confidentiality, integrity, privacy and trust which shall be discussed in the next sections of this paper.

Future work

Data security is a major concern of users, providers and re- searchers for securing the data in the clouds. Delegating most of the computation overhead to the cloud servers with high security is a major topic for future research. High confidentiality and user key accountability can be achieved[47]. A deep research can be carried out for unifying dependence of various components of cloud computing with security. Light-

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

weight homomorphhic encryption techniques need to be created as fully homomorphic encryption techniques are expensive and not feasible with the current cloud hardware[37].

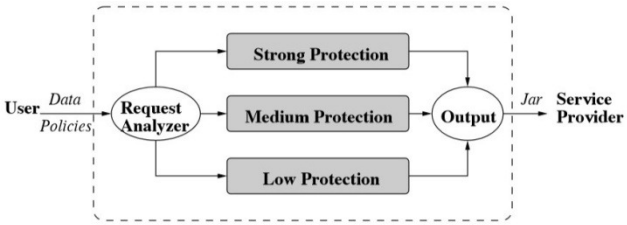

Figure 4: Overview of the Three-Tier Data Protection Architecture

3.2 Privacy

Privacy is the fundamental right of human being to be left alone without any interference. In terms of cloud computing, it can be defined as the desire of a person to have total control over their personal information. It also means that the personal data of the users shall not be misused by the service providers. The service providers or the organizations dealing with the personal data have to follow certain laws of the country for ensuring privacy of data. The risk related to privacy may vary for one cloud to another.

In general, the users need to know the location where there data is being stored. In some cloud environments, data is stored in different countries as in Windows Azure Storage[8], the data is stored in North America, Europe, and Asia. Un- doubtedly, this helps in recovering data during disasters, but this data needs to be protected carefully against attackers so as to keep the valuable information of the customers safe. Some of the applications and services do not face much security threats as compared to the dynamic services which include the personal information, location, social networks of the customers. These services need to be guarded against the attackers by using some security mechanisms. Thus protecting the privacy is an important task from users and ser- vice providers' point of view.

Chow[10] categorised the privacy preserving techniques into Information centric security in which data objects have data access control policies with them, Trusted computing in which the system behaves in an expected way with the hardware or software, and Cryptographic protocols for applying cryptographic techniques to the system.

Squicciarini[34] proposed a three-tier framework for tackling privacy issues caused by data indexing. In the framework, the main three components are strong protection, medium protection and low protection depending on the amount of access provided to the service provider by the users. Figure 4 depicts the architecture proposed by the authors. They also developed a technique for enforcing data privacy in cloud computing.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Itani[20] presented PaaS (Privacy as a Service); a set of protocols enforcing privacy in cloud environment. It uses the cryptographic coprocessors for securely storing and processing the data. The tamper proof ability of the cryptographic coprocessors provides a safe execution domain in the cloud computing for protecting data against unauthorized access. This model increases the user control over the data. it also provides a feedback to the users related to the privacy of their data making them aware of the privacy threats.

Gentry[13] proposed a Fully Homomorphic Encryption technique for securing the data in the clouds. It enables encryption of data user data stored in different servers and the data can be processed without decryption. The cloud servers have little or no knowledge about the data stored in the cloud. However, this approach might seem a powerful approach for securing the data; it is inefficient in practical use. Many other researchers have proposed homomorphic encryption techniques, adding speed and efficiency to Fully Homomorphic Encryption. Sadeghi[31] on the other hand argued about the privacy provided by Fully Homomorphic encryption as they suffer from high latency in a distributed cloud environment. They proposed to join trusted hardware tokens with Secure Function Evaluation for computing the arbitrary function on the information when it is in its encrypted state. The computation is secure as it does not give away any information. The authors focused on decreasing the latency of the system and making it safe and efficient. A hardware token is safe against physical strikes, thus it can be attached to the distributed servers where the computation can be performed.

Future work

For enhancing privacy in cloud computing,[10]proposed to extend control measures by introducing third party enterprise into the cloud environment through the use of trusted computing and better cryptographic techniques. Improved security techniques need to be implemented for facing new privacy threats in cloud computing. [20] proposed to design cloud computing frameworks that do not rely on trusted third-parties. They suggested that a deeper research needs to be carried out for better software division process and find an alternate distribution mechanism. The homomorphic encryption of data can be made more efficient and deployed in cloud for enhancing privacy in clouds. Experimentation need to be conducted on large scale so as to get some generalized results[34]. These measures should help in eliminating user's fears of utilizing cloud services.

3.3 Confidentiality

In terms of cloud computing, confidentiality is referred to as keeping the user data secret from the cloud service providers and the other customers. In a cloud, keeping the data confidential is one of the top priorities of the cloud service providers so as to make the users feel safe about their data. Therefore, confidentiality is necessary to ensure prevention of unauthorized access of customer data. In a cloud

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

environment, the users store their valuable data on cloud service provider's servers and have no control over their data. Most of the times, the location of data centers is unknown to the users. The large number of users, devices and resources add to the number of confidentiality threats in cloud computing. Confidentiality threats are more common in public clouds over the private clouds because a public cloud is shared by a number of users utilizing common resources. Data isolation and cryptography (as discussed earlier) are used for securing the user data.

In real, no actual data isolation can be achieved in the clouds; therefore virtual machines are deployed over the net- work to provide virtual isolation of data. For encryption, various encryption algorithms are used in the network, the users can also encrypt their data before uploading it to the cloud for better security. The cloud providers should follow certain standards[36] set by NIST. If the infrastructure is being reused, then careful measures should be taken to control any vulnerabilities. Sometimes, the confidentiality can be breached unintentionally by data permanence. Data permanence is the residual representation of deleted data, which could lead to disclosure of private data of one user to an- other unwillingly. Data confidentiality is directly related to user authentication. Various techniques have been deployed to ensure authenticated access to the data. Absence of such techniques can cause unauthorized users to access the customer's account in the cloud.

Inspite of all the efforts to employ confidentiality in clouds, there are some annoying factors[6] that we have to face in cloud computing:

- Insufficient authentication, authorization, and accounting (AAA) controls
- Inconsistent use of encryption and decryption keys
- Information persistence, disposal and reminisce challenges

Ristenpart[30] found that one of the major threats to confidentiality is the resource sharing technique used in cloud computing where multiple users are utilizing the same infrastructure for running their applications simultaneously. Undoubtedly, this increases resource utilization, but on the other hand, it affects the security and privacy of the users. Without proper security, the users do not feel safe in up- loading their data on to the cloud. The authors suggested a number of approaches to avoid these issues so that a distrustful user cannot access other users' data. One of the ways is to obfuscate the internal structure of the service and the placement policy to make it difficult for the attacker to place the virtual machine on the physical machine used by the target. Other solution is to focus on side-channel vulnerabilities and employ blinding techniques to minimizing information leakage. They also suggested that the user can request for an individual physical machine for their own us- age, thus no other user can utilize this physical machine.

Aviram[3] considers timing side-channel are a threat to cloud computing as (a) these threats are hard to control; (b) enables information stealing without leaving a

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

trail; and (c) these attacks can only be detected by the cloud providers. The authors proposed a new approach for controlling time channels using provider-enforced deterministic execution. They conducted experimentation with a prototype OS for deterministic cloud computing and got promising results. Cross- virtual machine attacks are not the only attacks that a user should be worried about; sometimes even the system admins have the privilege to access to the memory of the user's virtual machine.

Co-residency detection is another solution to confidentiality threats. Confidentiality can be maintained by eliminating co-residency of different virtual machines on a single physical machine. The users can request for their personal physical machine, which is expensive than normal computing, or the user can share a physical machine with "friendly" virtual machines, where "friendly" means known or trusted users. Zhang[48] developed a system for the above mentioned purpose called HomeAlone. HomeAlone helps the users to check if his isolation has been violated and does not require any support from the cloud provider. It helps in detecting the activity of the distrusted users by analyzing the cache us- age at the time when "friendly" virtual machines are coordinating with each other. For protecting user data from the cloud providers, presented a trusted cloud computing plat- form (TCCP) which provides a closed box execution environment to the guest users in cloud computing. A closed box computing environment means that a guest user in a cloud cannot be interfered by any other user with full privileges, thus providing guaranteed confidentiality to guest users.

The users nowadays, want maximum control over their data when using cloud computing, the rise in virtualization has raised users' interest in having a control over their data regardless of the physical location of the data. Descher[12] presented a method for retaining user access over the data. The authors conducted experimentation on the application of Nimbus as a cloud resource and used virtual machine images encrypted on client side for retaining control over the data. In the paper, the authors showed the implementation of their secure virtual machine consisting of an encrypted partition and a boot system. They further plan to apply their work within the "Austrian Grid Phase 2" project which is developed on the bases of technology used in Austrian Grid project.

Future work

For enforcing confidentiality, detection of co-residency is considered an areas of great interest in cloud computing so that the customers are able to keep a check on physical isolation[48]. There is a need to develop methods for targeting various side channels. The researchers need to make changes in the hardware for implementing better techniques to deal with cross-VM threats. These are the major threats in cloud computing that misuse cloud virtualization and co-residency and techniques need to be developed to face them. Besides this, a fully function protocol can be developed for implementing trusted cloud computing platform (TCCP)[32].

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

3.4 Integrity

Another key aspect of information security in cloud computing is integrity. Integrity means that the data stored in the clouds can be altered in an authorized manner. As with confidentiality, integrity is also associated with data, soft- ware and hardware. Data integrity means protecting the data against unauthorized erasure or alteration. Having a control over an entity's right to alter the data provides better protection against misuse of user information. It also makes clear to the user that what changes have been made to the data or the information stored. Cloud users have to be careful about data integrity along with confidentiality. One can try protecting the data by encrypting it, but there is no evidence if the data has been altered where it was residing or not. It is the responsibility of the cloud service providers to ensure data integrity in the system and to enforce ACID (atomicity, consistency, isolation and durability) properties in the cloud environment.

There are a number of threats faced by the users and service providers in the cloud environment. The cloud provider has to ensure sufficient security against these threats according to the legal obligations i.e. Service Level Agreements (SLAs), and any technical standards to which it has to con- form. This includes protecting the data in the clouds, both cryptographically and physically. Other issues related to data integrity are fault tolerance and failure recovery, so as to ensure the users that there data in the clouds is safe even in times of disaster or any other failures (hardware and soft- ware). A cloud service provider that does not replicated the data at multiple data centre's is not considered to be vulnerable to total failure[36][18].

In cloud computing, the applications provide storage as a service. Huge severs are used for storing user data. The servers cannot be trusted to be secure and reliable, thus the data has to be protected with some mechanism. As the users are unaware of the location of these servers, the users cannot trust them to behave faithfully and return accurate results. They might not be totally honest and act lazy in case of heavy computations. Bowerz[7] introduced HAIL (High-Availability and Integrity Layer) which allows a set of servers to prove that their storage is intact and retrievable. HAIL combines various cryptographic and distributed approaches used by different communities to provide secure cloud computing environment. It uses cryptography techniques for verifying and reallocating files to different servers. It is highly robust against attacks that might want to corrupt the set of servers. In their research, the authors show how HAIL improves the efficiency of tools, like Proofs of Retrievability (PORs) deployed on individual servers. The basic idea of HAIL is to copy all the data in each server in the given set of server. Then a completely random block is chosen from a server, if this block is identical to the blocks in other servers, then the data is intact, else it has been corrupted. However, instead of the customer checking the data integrity, it is possible to put shift this load to a third party which can be trusted by both customer and the cloud service providers. Wang[38] proposed an approach for using a

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

third party auditor (TPA) for keeping a check on integrity in cloud computing environment as shown in Figure 5.

Two fundamental requirements have to be fulfilled before introducing a TPA into the cloud environment: (1) TPA should audit the storage without demanding any local copy of the data and should not add extra burden to the cloud users; (2) TPA should not impose threats to data privacy. The basic technique used in the study is the combination of public key based homomorphic authenticator with random masking for achieving high integrity within the clouds. Experimentation conducted shows that the proposed technique is highly efficient and secure. The TPA cannot access the data while auditing, when homomorphic authenticator is combined with random masking.

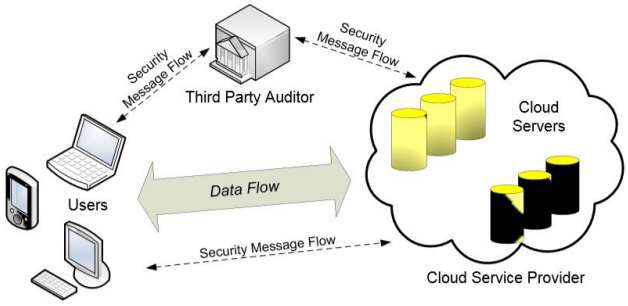

Figure 5: The architecture of cloud data storage ser- vice with TPA

Xiao[41] presented an accountable Mapreduce platform which check all the working machines and detects the malicious node in real time. The basic idea behind this approach is that the cloud provider establishes a trust domain consisting of multiple machines called as Auditors. The auditor uses determinism of MapReduce functions for applying an Accountable Test (A-Test) for each task on each machine. Then it compares the outputs of each machine with other machines. If there is a mismatch, then there is a possibility of a malicious node. The full replication of execution is expensive, thus only a part of the task is executed. If the parameters are selected carefully, then the proposed approach can achieve high detection rate with low computation cost. [31][32] enforces the computer systems to carry on reliably with hardware and software support. The key method of checking the integrity is known as remote attestation, which works by having the hardware create a certificate telling that which software is running. This certificate can be transferred to the viewers to notify them that the software is unaltered. One assumption of trusted computing is that some components like the hardware are not physically altered. With the data growing each second, it is hard for the cloud service providers to keep an integrity check on the data; it becomes expensive and complicated to get hold of large data stored in the servers. Computational integrity on the other hand is far more complex because of the lack of knowledge about computational internals of the system. A well designed integrity check

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

system should work in decreasing the load of the local machine than the actual load and, should impose little or no assumptions.

Future work

Cloud integrity is affected as the users do not have any physical control over their data. Large amount of data makes it difficult of the cloud service providers to keep a check on the data all the time. Research can be carried out for combining cloud integrity with existing cloud computing techniques[32]. A practical and unconditional verification method can be developed for enhancing integrity in cloud environment with low complexity and cost[38]. Different approaches proposed by researchers need to be implemented and evaluate in near future.

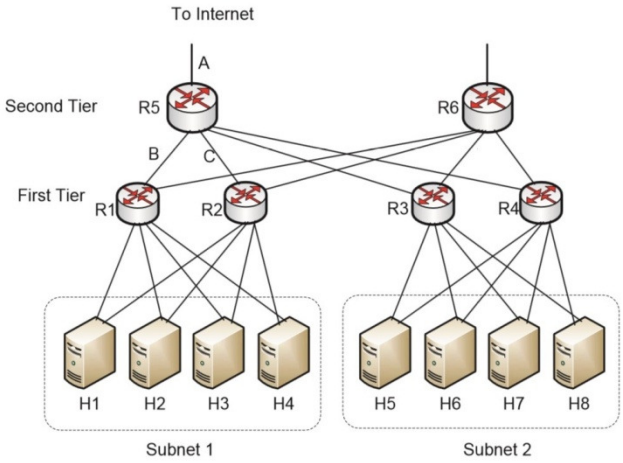

Figure 6: A typical data center network architecture

3.5 Availability

Availability is one of the critical information security issues in cloud computing. If a service is no longer available or the quality of service is not in accordance with the Service Level Agreement (SLA), then the users start losing faith in cloud computing. The goal of availability in cloud computing is to make resources available to the users all the time, irrespective of their location. Availability in clouds can be affected temporarily or permanently, depending on the types of threats. The types of threats can be broadly divided into Flooding Attack via Bandwidth Starvation and Fraudulent Resource Consumption (FRC) attack[42][6][36]. In a flooding attack, a lot of unwanted requested are made to the server which might hinder its normal working. These types of attacks can target a particular cloud or any random cloud for cutting down their availability to its respective users. The main problem in a flooding attack is that even when the cloud services go down, the cloud subscribers are still charged for the services. Thus there should a previously signed SLA to deal with such problems so as to save users from not paying for the services that they are not using. Even though data centers are taking measures for avoiding large-scale attackers, small attacks are still possible as they fewer precautions are taken to tackle them. Liu[22] proposed a dynamic

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

migration architecture leveraging the dynamic provisioning capability of the cloud for detecting similar Deny of Service(DoS) attacks. The authors also pro- posed a band estimation tools that works efficiently in high speed networks.

The open and less secure public clouds attract more attackers infiltrating the cloud by saturating the limited band- width of the cloud. As shown in Figure 6, links A, B, C are uplinks of router R5, R1, and R2, respectively. Suppose that link B is the active link and link C is the fail-over link (i.e.,a link will be activated when the active link is down). Due to under-provisioning, the aggregate capacity of H1, H2, H3, and H4 (which form the subnet 1) is a few times larger than any capacity for links A, B, or C. In order to saturate link B, attackers (which may be a few hosts controlled by the adversary) in subnet 1 only need to generate enough traffic to target the hosts in another subnet (e.g., subnet 2). Once link B is saturated by the non-sense traffic, hosts in subnet1 are unable to deliver services to cloud users.[42]. The three main steps for carrying out such an attack are: 1. Topology identification, 2. Gain access to the host, and 3. Carry out the attack.

In Fraudulent Resource Consumption (FRC) attacks, the attackers target the cloud for a long period of time so that they cannot provide services to their customers for a long period of time. The attackers act as legit cloud clients and send enormous requests to the clouds for utilizing the band- width of the cloud. These attacks are aimed to financially weaken the victim by not letting it provide services to the legit clients. It is difficult to differentiate FRC traffic from the legitimate traffic in cloud environment. Idziorek[19] pro- posed three detection metrics for identifying FRC attack from the legitimate cloud clients. The experimentation con- ducted with the three matrices show that the proposed FRC detection approach was able to detect attacks even in worst case scenario.

Data redundancy is one of the main factors responsible for maintaining high availability (A highly available DBMS is the database system which is available to the users all the time, even in times of hardware failure.) in the clouds. Amazon, Google Megastore, Microsoft Azure provide high avail- ability by storing data into the servers that are geographically scattered at different places. These servers are isolated from one another, thus failure in one does not propagate to other server. They provide inexpensive, low latency network connectivity to other locations. Google's Megastore is the structured data store supporting the Google Application Engine[5]. Megastore handles more than 3 billion write and 20 billion read transactions daily and stores a petabyte of primary data across many global datacenters. The basic idea of Megastore is to provide ACID semantics across different geographically-distant datacenters which highly partitioned datasets and an efficient replication scheme.

The need for Megastore came into existence when some applications required strong ACID semantics, which also required high fault-tolerance which could be provided by replicating the data over several datacenters. The already exist- ing data storage

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

techniques could not fulfill this requirement of managing and scaling the data simultaneously. This feature is provided by Megastore by dividing the data in smaller data entity groups i.e. the profile for one user, or a single blog account. All the operations within the groups get full ACID semantics and the cross group operations have to build their own consistency models. Thus, Megastore allows applications to do less-consistent reads for lower latency. the authors claimed Megastore achieves both consistency and availability, but we observed that the write availability suffers at times because of the partitions.

Minhas[25]presented an approach, RemusDB which deals with providing Highly Available (HA) DBMS at the virtual machine level. It uses two servers, Primary and Backup server. When the Primary server fails, the Backup server starts working as the Primary server. RemusDB uses HA in Virtual Machine which provides transparent, inexpensive and reliable failover capacities. The RemusDB takes care that no connection or transactions are lost in this process. RemusDB uses an epoch based checkpoint system for safeguarding the data, it sends the description of the primary database every 50ms to the buffer so that if a failure occurs, the machine can resume working from the latest state description sent to the buffer. In the paper, the authors showed that Remus and similar systems can protect a DBMS, database workloads incur a performance overhead of up to 32 percent as compared to an unprotected DBMS. They performed experimentations on two database systems and industry standards benchmarks showing that in some cases their optimized approach provided fast failover (less than 3 seconds of downtime) with low performance over- head as compared to an unprotected DBMS. Big IT giants are trying to make the data available to the users 24*7. New techniques are being developed to make this process secure, inexpensive and scalable.

Future work

The major threats to availability in cloud computing can be divided into internal and external attacks based on the nature of the attack. However, the way these attacks are executed are somewhat similar and research needs to be carried out to tackle them. Denial of service (DoS) threats are huge threat to availability and need to be tackled for smooth working of the clouds[22]. Better data centers need to be created for storing data are required for making data available to the users all the time. FRC method also needs to be enhanced as it cannot identify the attackers[19]. Study needs to be conducted against economic denial of sustain-ability (EDoS)so as to make financial institutions utilizing cloud services feel safer.

3.6 Accountibility

Accountability has become more popular in the recent years for increasing the trust within the cloud environment. Accountability is defined as the ability to identify the entity, with high accuracy, which is responsible for specific events. In cloud

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

computing, there always exists a threat of unauthorized access of client data. Neither the client, nor can the cloud service provider be held responsible for any kind of casualties in the system. Thus, the entity which has to be held responsible has to have a strong identity and the ability to store all the transactions occurring in the system, which can be used for auditing purpose. For the above mentioned purpose, a record of data transactions has to be maintained for periodic checking of the data. For instance, if a person performs a certain action A, then the action can be checked to see if the person has done anything wrong or not and can be held accountable. For achieving accountability, all the minute details of the system needs to be recorded and stored for future use in case of some accident. The details should have enough information to justify the traced action.

Accountability in cloud computing is considered a huge challenge because of the following[14]:

Misconfigured machines might provide inaccurate results. For example, the worker machines used for data processing in MapReduce[11] might be misconfigured, thus providing inaccurate results. The user has to run the task on local machine to check the accuracy of the task.

- Insufficient resources might be allocated which would to performance degradation.
- A virus released by third-party can damage the user data
- Inability to deliver data on time.

In the above mentioned cases, if the data is leaked to the competitors or some other error is caused in the system, neither the client nor the cloud service provider can be blamed. Unless they have any solid justification, they cannot point fingers at each other. In [14] the authors suggest that the cloud should be made accountable to both client and the service provider. They should both be mutually able to figure out the problem and report it to a third party of proving the presence of a problem. The authors proposed a primitive AUDIT (A,S,t1,t2) to allow customers to check if the SLA (denoted by A) has been fulfilled between time t1 an t2. The AUDIT will return OK if there is no fault found in the system, else it returns the verifiable evidence against the responsible entity. In the paper, the authors did not describe about the design of AUDIT, but provided a set of building blocks like tamper-evident logs, virtualization-based replays; trusted time stamping used for detecting performance fault and sampling that improves the quality of replay.

In another study[15], the authors presented Accountable Virtual Machine (AVM) for auditing the software execution on a remote machine. AVN can record non-repudiable in- formation for allowing the auditor to check if the software is working as it is supposed to be. The designed system has implemented prototype AVM monitor based on VMware Work- station for detecting cheats in Counterstrike (online game). The system was able to detect 26 cheats in Counterstrike. Wang[39] developed a

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

similar solution to AVM for validating the correctness of the data in a multi-tenancy environment. The authors defined service endpoints through which all the data transfer can take place for keeping a check on the data. The assumption was made that the data will be accessed through the endpoints specified by in the SLA between the cloud clients and the service providers. The basic idea is to keep track of the data accessed through these endpoints. This leads to better business transactions as a third party is involved in the process which keeps a check on all the trans- actions for smooth running of the organization.

Lack to accountability in cloud computing might lead to in- accurate billing of resource consumption. The clients are using the cloud services on a pay-as-you-go basis; it is quite difficult to keep track of the expenses of the resource consumption because of the black box nature of the clouds. As the cloud service providers want maximum profit from their resources, they choose to multiplex the applications belonging too different clients for high utilization of resources. At times, this multiplexing can cause incorrect resource consumption and the client has to bear extra cost because of this. Sekar[33]proposed a systematic approach for verifiable resource accounting. According to the authors, verifiability means that the application should use the resources for which it was paying and this consumption was legitimized under some policy. The authors analysed the different challenges and opportunities for realizing such a framework. Figure 7 describes the conceptual architecture of the framework proposed. The three logical participants are: the customer C, the provider P, and the verifier V. At a high-level, C asks P to run the computation task T. Subsequently, P provides a consumption report R to C describing what resources it thinks T consumed. For example, a provider may report a time series of consumption vectors, whose elements correspond to CPU usage, memory bandwidth, memory size, I/O bandwidth, network bandwidth, and energy, aggregated over pre-determined time quanta, for the duration of the task. C takes this report R together with the task T and additional data to the verifier V and checks if R is a valid resource re- port for T.

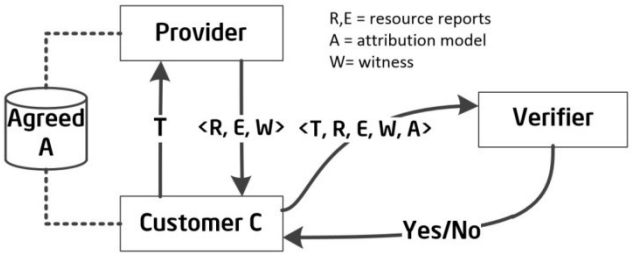

Figure 7: Conceptual Architecture

Accountability has become one of the most significant at- tribute of cloud computing for detecting the error causing entity in the cloud environment. It does not only deal with security threats, it also deals with various incidents like soft- ware bugs, hardware failure and misconfiguration. There- fore, an accountable cloud can be seen as a trustworthy cloud.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Future work

Enhancing the accountability of the clouds can significantly increase the trust of users in cloud computing. A new scheme needs to be developed in which the MapReduce can be ac- curate and efficient in pointing out the faulty node in the cloud environment[11]. One of the proposed technique is to use replication of data, but is slows down the system which I not liked in cloud computing. For implementing resource accountability relies on generating a consumption report which is verified by third party. Other solutions can be mining execution logs for predicting the workload or combining users to detect any violation in the system. However, when users are working together, it is hard to maintain user's privacy. Thus, research needs to be carried out in this direction to find better techniques for cloud accountability.

3.7 Audit and Compliance

For audit and compliance, the user's access to the data is monitored so as to keep a check on security breaches in the cloud environment. This helps the auditors to ensure the fulfillment of different policies, periodic auditing and reporting. Auditing is a programming approach to keep a watch on all the activities going on in the cloud system. This could be added as a layer on the virtual machine to keep track of the virtualization operations carried out in the machine. In such a case, factors like state changes and other factors affecting the system availability are audited. From legal point of view, many nations want their user's data and copyright material to be stored within the national boundaries, which makes auditability a legal issue.

Auditing can also be defined as, "the process of reviewing and examining the authorization and authentication records in order to check whether compliances with predefined security standards and policies are assured"[36]. It helps in detecting security breaches in the cloud environment. The users should have authority to control the access of data. Lack of user control over the data is a hindrance in data auditing. Compliance can address the rising cloud service

providers and user's requirements. The cloud service providers need a strong internal control monitoring system in addition

to a robust external auditing system. This is necessary for a service provider to gain comfort over their in-cloud activities[28].

There is little transparency in auditing process of the cloud service providers. The question is that how is the distributed data spread all over the world in different machines audited from one place by the providers? A cloud service provider needs to follow strict rules and legal issues for data auditing and the customers should be aware of these rules and legal is- sues so as to better trust the cloud services. The legal issues and rules include auditing, data security and export, data retention and destruction, legal discovery and compliance. No matter how much security is

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

provided by the cloud ser- vice providers, the customers in the end are responsible for their own data security and integrity. The customers need to prove compliance with the security standards. It should be made certain that external auditing is provided by the cloud service providers. The cloud computing model is based on providing services specified in the SLA; the SLA should cover all the issues related to security, privacy and performance. Providing high level security is one of the main objectives of SLA, but there is a trade-off between performance and security provided in cloud computing. If the security is in- creased, then it utilizes the resources of the performance, thus slowing down the system in one way or the other.

Currently, organizations have well-established processes for compliance monitoring and enforcement. The main problem faced in the cloud environment is the division of compliance responsibilities between the cloud service provider and the customers. It is easier to implement compliances when only one of the parties has the control over the data. In a business environment an organization uses the services provided by a third party. Existing regulations do not take into account the audit responsibility of a third-party service provider[1]. The Cloud Security Alliance states that the SLA between the cloud customer and provider should include a Right to Audit clause so as to provide the cloud customers control over the rules and regulations specified in the SLA. The Cloud Security Alliance specifies the general approach to involve legal regulations, but no formal APIs or frameworks have been defined for integrating multiple audit systems into the cloud environment. Additionally, there have been no standards or techniques set up for dividing the responsibilities between the customers and the cloud service providers. Adopting cloud model results in loss of control from individual parties, the cloud service providers and the cloud customers. SLA tries to cover this issue, but does not specify any measures to tackle these issues. SLAs are useful for developing trust relationship between the service providers and the customers as the customer can understand the implementation, deployment and security measures though the SLA. This customer-provider relationship is critical because still the customer is ultimately responsible for compliance and protection of their valuable data, even after moving the data to the cloud.

Each year, the compliance requirements are becoming stricter, the cloud providers can try to meet these requirements and gain significant advantage. There is a large range of IT procedures covered by compliance, these are system logging, log analysis, user-administrator authentication, authorization and audit and much more. The cloud service providers need to develop a system for making the cloud compliant which proves the compliance of the individual during a compliance audit. Some of the laws prohibit cloud service providers to store the personal information of their citizens in some other nation, thus, this data could be stored within the country. One popular auditing guideline is the SAS-70, guiding auditors to assess the internal controls over the processing of vital information. US government agencies generally need to follow guidelines from FISMA - Federal In-

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

formation Security Management Act, NIST - National Institute of Standards and Technology, and FIPS - Federal Information Processing Standard. The main aim of compliance is to ensure data privacy and compliance; the providers use various methods to implement them. Some of the government regulations like HIPPA, Federal Financial Institutions Examination Council, Basel II, and PCI are set down for adoption security measures globally[36].

Future work

Auditing can be enforced in cloud computing in a number of ways. One of the most common way is through third party auditors or automated auditing mechanism for improving trust in cloud computing. Tools or techniques need to be developed for identifying true integrity and authenticity without compromising the data privacy. Better certification techniques need to be developed to implement better policies in cloud computing[36]. For including multiple auditing mechanism in the clouds, APIs and frameworks need to be developed.

3.8 Multi-tenancy

Multi-tenancy is an essential property of cloud computing which allows maximum usage of the underlying hardware in cloud environment for efficient resource provisioning. In a multi-tenancy environment, a single instance of software runs on a SaaS vendorâĂŹs server; the server is serving multiple number of clients. The software is virtually partitioned so that each client gets to work with a virtual application instance[28]. The multi-tenancy model poses a threat to the user data as multiple users store their personal data in the cloud, thus it is the responsibility of the cloud service provider to safeguard this data from any unauthorized access. Many of the cloud service providers use job scheduling algorithms to avoid these security threats, but most of the cloud providers use virtualization so as to get the maximum benefits from their underlying hardware.

Virtual machines are considered safe as they are completely isolated from other virtual machines. However, security breach can occur in some cases, where the attacker can penetrate into other virtual machines and get access of the vital data of other users[21]. As the components like CPU cache and GPUs are not designed to provide strong isolation of data. Some of the vulnerable areas are passwords, distributed denial of services (DDoS), hosting malicious data. As the number of users running on a single hardware in- crease, the number of security threats related need to considered. As multiple users are running on a single hardware, it can be hard for the cloud service provider to keep track of all the users and their related activities, thus causing security threats in the system. Sometimes, the guest might try to run a malicious code and try to bring down the system or block some functionalities of the cloud[23].

[46] provides an example of such threats; one of the threats is malicious use of command for âĂIJVMware SVGA2âĂİ where SVGA is Super Video Graphics

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

Array. This command is used by the guest to execute the code on the host side. It copies the source rectangle into the frame buffer of the given destination. There are different ways by which this command can be abused by the attackers to get access of the user data. The use of virtualization technique is also vulnerable to numerous security threats such as cross-

VM side-channel attack for getting access of the user data stored on same virtual machine[30]. Thus, there is a strong need for better virtualization to secure user data.

Future work

As cloud vendors use multi-tenancy for maximum utilization of their available resources, this process needs to be safe so as to avoid malicious user to access personal information of users on the same physical machine. Robust algorithms need to be developed to provide isolation to each virtual machine using a common physical machine. Different virtualization and security models can be combined to see how they per- form to enhance the security in virtualization of components in cloud computing[23]. As the clouds are scaling each day, more and more machines will be required to accommodate this increasing number of users, thus users face numerous security threats and research needs to be done in this area.

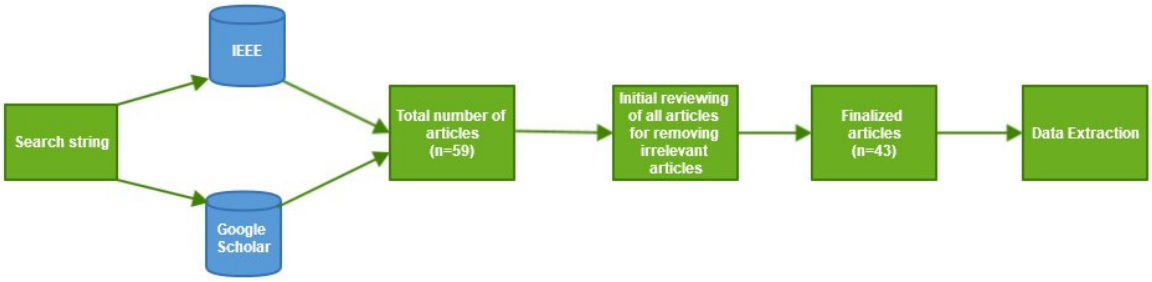

Figure 8: Literature review

4. INCLUSION CRITERIA

We plan to search research papers from ”www.ieee.org” and

”Google scholar” using keywords ”cloud computing”, ”security” and ”privacy”.

Download the papers relevant to the searched keywords between 2009-2014. Prune out relevant papers by reading the Abstract and Introduction section of the research papers. Extract the main idea of the research papers from the selected paper and categorizing them under different predefined sections.

Find more relevant papers from the references of the selected papers and check if they can be included in the survey. Search for more papers published before 2009 if the topic needs more explanation.

Figure 8 represents the literature review of the research conducted.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

5. CONCLUSION

In this report, we have surveyed the past 5 years of cloud computing literature related to security and privacy. The study was carried out to determine the major security is- sues prevailing in cloud computing and the solutions pro-posed/presented by researchers to tackle these problems. We downloaded research papers by running queries on different articles to gain access of all the papers relevant to our research topic. We considered articles mostly from famous conferences and journals so as to get better understanding of the topic. Papers are downloaded from ”www.ieeexplore.ieee.org” and ”Google scholar” by using keywords like ”cloud computing”, ”security ” and ”privacy”. We downloaded all the papers that seem relevant to the research topic. After initial review, pruned out the irrelevant i.e. the articles related to medical, army or such irrelevant field. After pruning out the irrelevant papers, we were left with around 45 papers. The major task was to select the issues for discussion in paper. After reviewing the final papers, the papers we characterized into eight basic issues: security, privacy, integrity, confidentiality, availability, multi-tenancy, accountability and, audit and compliance. Our results summarize the literature into the above mentioned issues, allowing interested readers to quickly find articles of interest. Finally, future opportunities are presented in the end of each section related to the concerned issue.

6. ACKNOWLEDGEMENT

Thanks to Professor Patrick Martin for giving us an opportunity to conduct the survey and Queen’s University to provide access to online articles.

7. REFERENCES

[1]https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[2] R. Arora, A. Parashar, and C. C. I. Transforming.Secure user data in cloud computing using encryption algorithms. International Journal of Engineering Research and Applications (IJERA), 3(4):1922–1926,2013.

[3] A. Aviram, S. Hu, B. Ford, and R. Gummadi.Determinating timing channels in compute clouds. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pages 103–108. ACM,2010.

[4] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. Dependable and Secure Computing, IEEE Transactions on, 1(1):11–33, 2004.

[5] J. Baker, C. Bond, J. Corbett, J. Furman, A. Khorlin, J. Larson, J.-M. Léon, Y. Li, A. Lloyd, and V. Yushprakh. Megastore: Providing scalable, highly available storage for interactive services. In CIDR, volume 11, pages 223–234, 2011.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

[6] A. Behl and K. Behl. Security paradigms for cloud computing. In Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on, pages 200–205. IEEE, 2012.

[7] K. D. Bowers, A. Juels, and A. Oprea. Hail: a high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM conference on Computer and communications security, pages 187–198. ACM, 2009.

[8] B. Calder, J. Wang, A. Ogus, N. Nilakantan, A. Skjolsvold, S. McKelvie, Y. Xu, S. Srivastav, J. Wu, H. Simitci, et al. Windows azure storage: a highly available cloud storage service with strong consistency. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, pages 143–157. ACM, 2011.

[9] D. Chen and H. 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] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security, pages 85–90. ACM, 2009.

[11] J. Dean and S. Ghemawat. Mapreduce: a flexible data processing tool. Communications of the ACM, 53(1):72–77, 2010.

[12] M. Descher, P. Masser, T. Feilhauer, A. M. Tjoa, and D. Huemer. Retaining data control to the client in infrastructure clouds. In Availability, Reliability and Security, 2009. ARES'09. International Conference on, pages 9–16. IEEE, 2009.

[13] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.

[14] A. Haeberlen. A case for the accountable cloud. ACM SIGOPS Operating Systems Review, 44(2):52–57, 2010.

[15] A. Haeberlen, P. Aditya, R. Rodrigues, and P. Druschel. Accountable virtual machines. In OSDI, pages 119–134, 2010.

[16] http://www.infoworld.com/d/security-central/gartner- seven-cloud-computing-security-risks 853.

[17] http://www.roughtype.com.

[18] I. Iankoulova and M. Daneva. Cloud computing security requirements: A systematic review. In Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on, pages 1–7. IEEE, 2012.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

[19] J. Idziorek, M. Tannian, and D. Jacobson. Detecting fraudulent use of cloud resources. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pages 61–72. ACM, 2011.

[20] W. Itani, A. Kayssi, and A. Chehab. Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. In Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on, pages 711–716. IEEE, 2009.

[21] R. Latif, H. Abbas, S. Assar, and Q. Ali. Cloud computing risk assessment: A systematic literature review. In Future Information Technology, pages 285–295. Springer, 2014.

[22] H. Liu. A new form of dos attack in a cloud and its avoidance mechanism. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pages 65–76. ACM, 2010.

[23] S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen. Virtualization security for cloud computing service. In Cloud and Service Computing (CSC), 2011 International Conference on, pages 174–179. IEEE, 2011.

[24] P. Mell and T. Grance. The nist definition of cloud computing. National Institute of Standards and Technology, 53(6):50, 2009.

[25] U. F. Minhas, S. Rajagopalan, B. Cully, A. Aboulnaga, K. Salem, and A. Warfield. Remusdb: Transparent high availability for database systems. The VLDB Journal, 22(1):29–45, 2013.

[26] A. K. Mishra, P. Matta, E. S. Pilli, and R. Joshi. Cloud forensics: State-of-the-art and research challenges. In Cloud and Services Computing (ISCOS), 2012 International Symposium on, pages 164–170. IEEE, 2012.

[27] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby. Enhanced data security model for cloud computing. In Informatics and Systems (INFOS), 2012 8th International Conference on, pages CC–12. IEEE, 2012.

[28] S. Pearson and A. Benameur. Privacy, security and trust issues arising from cloud computing. In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, pages 693–702. IEEE, 2010.

[29] S. Ramgovind, M. M. Eloff, and E. Smith. The management of security in cloud computing. In Information Security for South Africa (ISSA), 2010, pages 1–7. IEEE, 2010.

[30] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security, pages 199–212. ACM, 2009.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

[31] A.-R. Sadeghi, T. Schneider, and M. Winandy. Token-based cloud computing. In Trust and Trustworthy Computing, pages 417–429. Springer, 2010.

[32] N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. In Proceedings of the 2009 conference on Hot topics in cloud computing, pages 3–3. San Diego, California, 2009.

[33] V. Sekar and P. Maniatis. Verifiable resource accounting for cloud computing services. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pages 21–26. ACM, 2011.

[34] A. Squicciarini, S. Sundareswaran, and D. Lin. Preventing information leakage from indexing in the cloud. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pages 188–195. IEEE, 2010.

[35] H. Takabi, J. B. Joshi, and G.-J. Ahn. Securecloud: Towards a comprehensive security framework for cloud computing environments. In Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual, pages 393–398. IEEE, 2010.

[36] H. Tianfield. Security issues in cloud computing. In Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on, pages 1082–1089. IEEE, 2012.

[37] A. Ukil, D. Jana, and A. De Sarkar. A security framework in cloud computing infrastructure. International Journal of Network Security & Its Applications, 5(5), 2013.

[38] C. Wang, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for data storage security in cloud computing. In INFOCOM, 2010 Proceedings IEEE, pages 1–9. IEEE, 2010.

[39] C. Wang and Y. Zhou. A collaborative monitoring mechanism for making a multitenant platform accountable. Proc. HotCloud, 2010.

[40] L. Wei, H. Zhu, Z. Cao, W. Jia, and A. V. Vasilakos. Seccloud: Bridging secure storage and computation in cloud. In Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on, pages 52–61. IEEE, 2010.

[41] Z. Xiao and Y. Xiao. Accountable mapreduce in cloud computing. SCNC 2011, 2011.

[42] Z. Xiao and Y. Xiao. Security and privacy in cloud computing. Communications Surveys & Tutorials, IEEE, 15(2):843–859, 2013.

[43] Z. Yandong and Z. Yongsheng. Cloud computing and cloud security challenges. In Information Technology in Medicine and Education (ITME), 2012 International Symposium on, volume 2, pages 1084–1088. IEEE, 2012.

ISSN: 2347 5587
Peer Reviewed International Journal Vol. No. III Issue No. 04 April 2015

[44] J. Yang and Z. Chen. Cloud computing research and security issues. In Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on, pages 1–3. IEEE, 2010.

[45] P. You, Y. Peng, W. Liu, and S. Xue. Security issues and solutions in cloud computing. In Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, pages 573–577. IEEE, 2012.

[46] H. Yu, N. Powell, D. Stembridge, and X. Yuan. Cloud computing and security challenges. In Proceedings of the 50th Annual Southeast Regional Conference, pages 298–302. ACM, 2012.

[47] S. Yu, C. Wang, K. Ren, and W. Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In INFOCOM, 2010 Proceedings IEEE, pages 1–9. Ieee, 2010.

[48] Y. Zhang, A. Juels, A. Oprea, and M. K. Reiter. Homealone: Co-residency detection in the cloud via side-channel analysis. In Security and Privacy (SP), 2011 IEEE Symposium on, pages 313–328. IEEE, 2011.