A Seminar Report on SECURITY IN CLOUD COMPUTING Prepared by

Adeeb P.A
National Institute of Technology Calicut

A Seminar Report on

SECURITY IN CLOUD COMPUTING

Prepared by

ADEEB P A
Roll No. B100118EC

B.Tech (Electronics and Communication Engineering)

Department of Electronics and Communication Engineering
NATIONAL INSTITUTE OF TECHNOLOGY, CALICUT
Kozhikode, Kerala - 673 601

Winter 2014

Department of Electronics and Communication Engineering

NATIONAL INSTITUTE OF TECHNOLOGY, CALICUT

Certificate

This is to certify that this seminar report entitled **”Security in Cloud Computing”** is a bonafide record of the seminar presented by **Mr. Adeeb P A**, Roll No. B100118EC, during Winter 2014 in partial fulfilment of the requirement for the award of B.Tech degree in Electronics and Communication Engineering by the National Institute of Technology Calicut, India.

Dr. P. S. Sathidevi

Department of Electronics and

Communication Engineering

N.I.T. Calicut

Date : February 3, 2014

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to our Faculty-in-charge of seminar Dr. P. S. Sathidevi for her proper guidance and valuable suggestions which helped me to improve my works. I am also greatly thankfull to our Electronics and Communication Engineering department and other faculty members for giving me this unique opportunity to do this seminar.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

SECURITY IN CLOUD COMPUTING

Cloud computing is an internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. It is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud computing is a virtual pool of computing resources. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Security concerns have given rise to immerging an active area of research due to the many security threats that many organizations have faced at present.

This seminar provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing. Then this seminar discusses some current solutions and finally describes future research work about data security and privacy protection issues in cloud.

1. INTRODUCTION

Cloud computing is an internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet. Cloud computing, as an emerging computing paradigm aiming to share storage, computation, and services transparently among a massive users. The exact definition of cloud computing is *A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet* [5].

Current cloud computing systems pose serious limitation to protecting users data confidentiality. Since users sensitive data is presented in unencrypted forms to remote machines owned and operated by third party service providers, the risks of unauthorized disclosure of the users sensitive data by service providers may be quite high. There are many techniques for protecting users data from outside attackers. An approach is presented to protecting the confidentiality of users data from service providers, and ensures service providers cannot collect users confidential data while the data is processed and stored in cloud computing systems. Cloud computing systems provide various Internet based data storage and services. Due to its many major benefits, including cost effectiveness and high scalability and flexibility, cloud computing is gaining significant momentum recently as a new paradigm of distributed computing for various applications, especially for business applications. Along with the rapid growth of the Internet. With the rise of the era of cloud computing, concerns about Internet Security continue to increase. To address this problem we propose the design of a system that will capture the movement of information on the cloud. We will be identifying whether there is a need for some type of security capture device/measure on the cloud, which will allow users to know whether their information is secure and safe without comprising from threats and attacks.

2. EVOLUTION OF CLOUD COMPUTING

Cloud computing began to get both awareness and popularity in the early 2000s. When the concept of cloud computing originally came to prominence most people did not fully understand what role it fulfilled or how it helped an organization. In some cases people still do not fully understand the concept of cloud computing. Cloud computing can refer to business intelligence (BI), complex event processing (CEP), service-oriented architecture (SOA), Software as a Service (SaaS), Web-oriented architecture (WOA), and even Enterprise 2.0. With the advent and growing acceptance of cloud-based applications like Gmail, Google Calendar, Flickr, Google Docs, and Delicious, more and more individuals are now open to using a cloud computing environment than ever before. As this need has continued to grow so has the support and surrounding infrastructure needed to support it. To meet those needs companies like Google, Microsoft, and Amazon have started growing server farms in order to provide companies with the ability to store, process, and retrieve data while generating income for themselves. To meet this need Google has brought on-line more than a million servers in over 30 data centers across its global network. Microsoft is also investing billions to grow its own cloud infrastructure. Microsoft is currently adding an estimated 20,000 servers a month. With this amount of process, storage and computing power coming online, the concept of cloud computing is more of a reality than ever before. The growth of cloud computing had the net effect of businesses migrating to a new way of managing their data infrastructure. This growth of cloud computing capabilities has been described as driving massive centralization at its deep center to take advantage of economies of scale in computing power, energy consumption, cooling, and administration.

3. CLOUD ARCHITECTURE

The architecture of cloud involves multiple cloud components communicating with each other over the application programming interfaces (APIs), usually web services. The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e. the customer. This includes the clients network or computer, and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the cloud itself, which comprises of various computers, servers and data storage devices.

The general architecture of cloud platform is also known as cloud stack given in figure 3.1 [5]. Cloud services may be offered in various forms from the bottom layer to top layer in which each layer represent one service model. The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, where resources are aggregated and managed physically (e.g., Emulab) or virtually (e.g., Amazon EC2), and services are delivered in forms of storage (e.g., GoogleFS), network (e.g., Openflow), or computational capability (e.g., Hadoop MapReduce). The middle layer delivers Platform-as a-Service (PaaS), in which services are provided as an environment for programming (e.g., Django) or software execution (e.g., Google App Engine). Software- as-a Service (SaaS) locates in the top layer, in which a cloud provider further confines client flexibility by merely offering software applications as a service. Apart from the service provisioning, the cloud provider maintains a suite of management tools and facilities (e.g., service instance life-cycle management, metering and billing, dynamic configuration) in order to manage a large cloud system.

Cloud deployment models include public, private, community, and hybrid clouds which is shown in figure 3.2. Public clouds are external or publicly available cloud environments that are accessible to multiple tenants, whereas pri-vate clouds are typically tailored environments with dedicated virtualized resources for particular organizations. Similarly, community clouds are tailored for particular groups of customers [3].

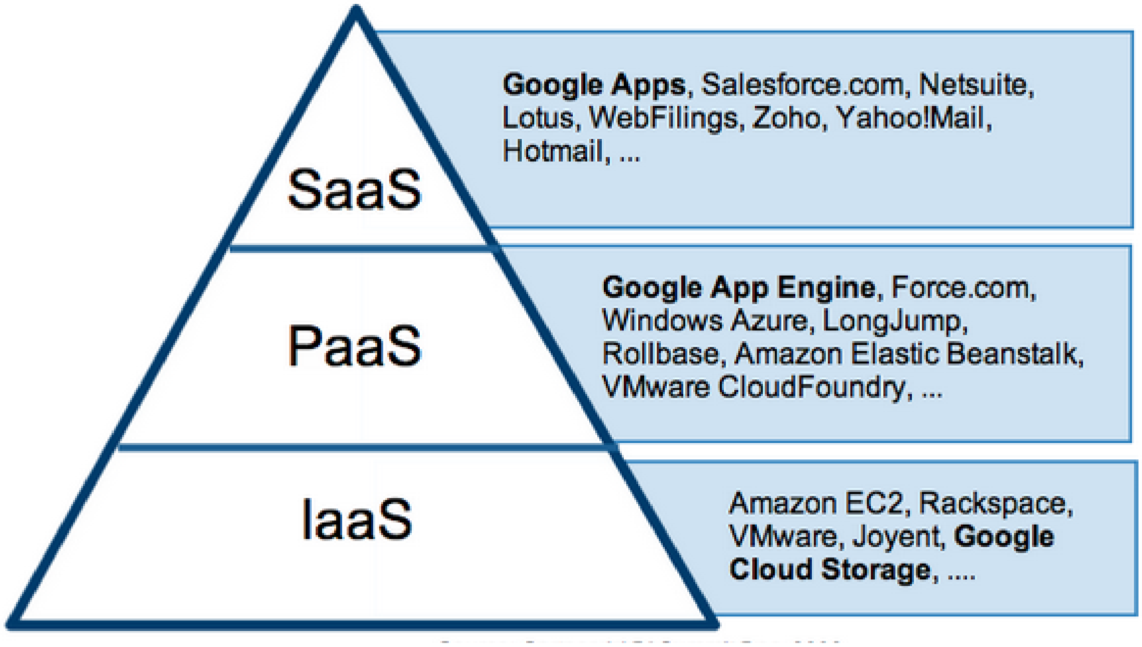
SaaS
Google Apps, Salesforce.com, Netsuite, Lotus, WebFilings, Zoho, Yahoo!Mail, Hotmail, ...
PaaS
Google App Engine, Force.com, Windows Azure, LongJump, Rollbase, Amazon Elastic Beanstalk, VMware CloudFoundry, ...
IaaS
Amazon EC2, Rackspace, VMware, Joyent, Google Cloud Storage, ...

Figure 3.1: Cloud delivery model

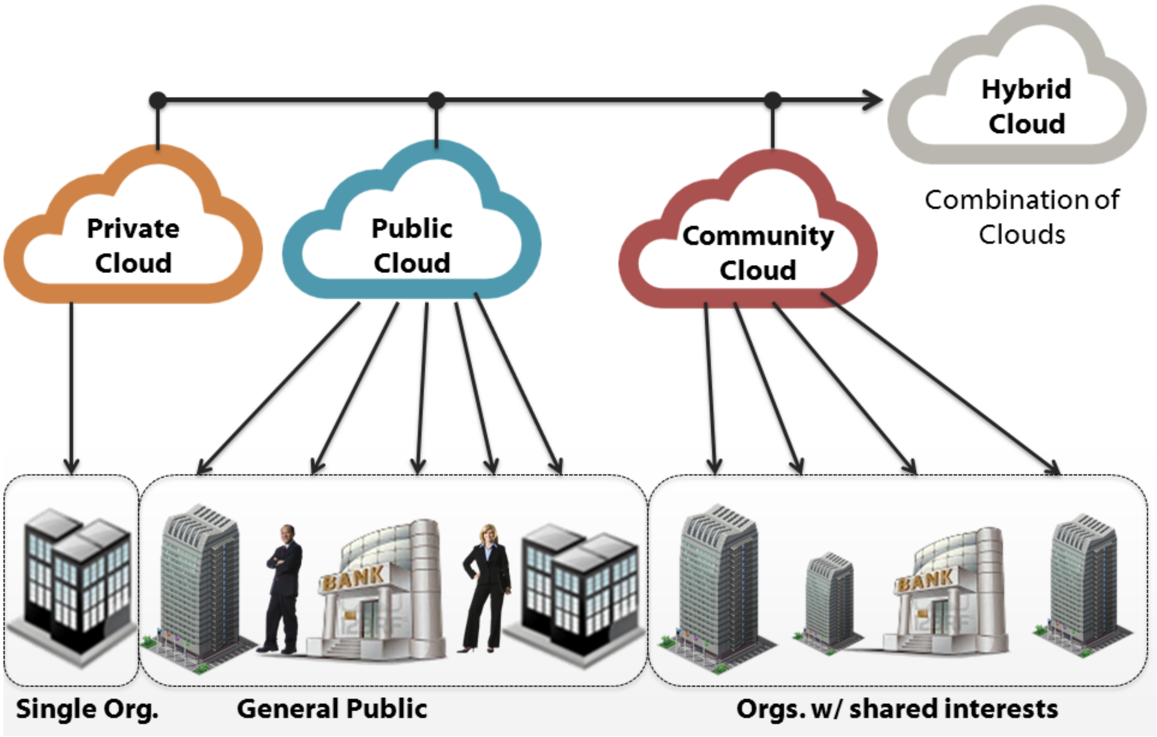

Figure 3.2: Cloud deployment model

4. CLOUD SECURITY CHALLENGES

The world of computation has changed from centralized to distributed systems and now we are getting back to the virtual centralization which is the Cloud Computing. Location of data and processes makes the difference in the realm of computation. We have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. The cloud computing uses the internet as the communication media. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues. Organizations use cloud computing as a service infrastructure, critically like to examine the security and confidentiality issues for their business critical insensitive applications. What are the security concerns that are preventing companies from taking advantage of the cloud? This section deals with the taxonomy of the security concerns.

Traditional security issues are still present in cloud computing environments. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer suitable for applications and data in cloud. Traditional concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats In addition, it may be easier to enforce security via contracts with online services providers than via internal controls. Due to the openness and multi-tenant characteristic of the cloud, cloud computing is bringing tremendous impact on information security field [2].

Availability concerns center on critical applications and data being available. Well-publicized incidents of cloud outages include Gmail. As with the Traditional Security concerns, cloud providers argue that their server uptime compares well with the availability of the cloud users own data centers. Cloud services are thought of as providing more availability, but perhaps not there are more single points of failure and attack. Third-party data control the legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud [5], [6].

4.1 CHARACTERISTICS OF CLOUD COMPUTING

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches: [6]

- **On-demand self-service** - A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.

- **Broad network access** - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud based software services.

- **Resource pooling** - The providers computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.

- **Rapid elasticity** - Capabilities can be rapidly and elastically provisioned in some cases automatically to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- **Measured service** - Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the service.

4.2 SECURITY CHALLENGES

Cloud computing becomes a successful and popular business model due to its charming features. In addition to the benefits at hand, the former features also result in serious cloud-specific security issues. The people whose concern is the cloud security continue to hesitate to transfer their business to cloud. Security issues have been the dominate barrier of the development and widespread use of cloud computing. Understanding the security and privacy risks in cloud computing and developing efficient and effective solutions are critical for its success. Although clouds allow customers to avoid start-up costs, reduce operating costs, and increase their agility by immediately acquiring services and infrastructural resources when needed, their unique architectural features also raise various security and privacy concerns. There are three main challenges for building a secure and trustworthy cloud system:

- **Outsourcing** - Outsourcing brings down both capital expenditure (CapEx) and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive/classified data is out of the owners control [5].

  - **Data service outsourcing security** - Cloud computing provides access to data, but the challenge is to ensure that only authorized entities can gain access to it. When we use cloud environments, we rely on third parties to make decisions about our data and platforms in ways never seen before in computing. Its critical to have appropriate mechanisms to prevent cloud providers from using customers data in a way that hasnt been agreed upon. It seems unlikely that any technical means could completely prevent cloud providers from abusing customer data in all cases, so we need a combination of technical and nontechnical means to achieve this. Clients need to have significant trust in their providers technical competence and economic stability [3].

For the former concern, data encryption before outsourcing is the simplest way to protect data privacy and combat unsolicited access in the cloud and beyond. But encryption also makes deploying traditional data utilization services such as plaintext keyword search over textual data or query over database a difficult task. The trivial solution of downloading all the data and decrypting it locally is clearly impractical, due to the huge bandwidth cost resulting from cloud scale systems. This problem on how to search encrypted data has recently gained attention and led to the development of *searchable encryption* techniques. At a high level, a searchable encryption scheme employs a prebuilt encrypted search index that lets users with appropriate tokens securely search over the encrypted data via keywords without first decrypting it. However, considering the potentially large number of on-demand data users and the huge amount of outsourced data files in the cloud, this problem is still particularly challenging because meeting performance, system usability, and scalability requirements is extremely difficult [4].

Another important issue that arises when outsourcing data service to the cloud is protecting data integrity and long-term storage correctness. Although outsourcing data to the cloud is economically attractive for long-term, large-scale storage, it doesnt immediately guarantee data integrity and availability. This problem, if not properly addressed, can impede the successful deployment of a cloud architecture. Given that users no longer locally possess their data, they cant utilize traditional cryptographic primitives to protect its correctness. Such primitives usually require a local copy of the data for integrity verification, which isnt viable when storage is outsourced. Furthermore, the large amount of cloud data and the users constrained computing capabilities make data correctness auditing in a cloud environment expensive and even formidable. So, enabling a unified storage auditing architecture is important for this nascent cloud economy to become fully established; users will need ways to assess risk and gain trust in the cloud. From a system-usability viewpoint, such a design should incur very limited auditing overhead in terms of computation and bandwidth, incorporate cloud datas dynamic features, and preserve users privacy when a specialized third-party auditor is introduced [1].

- **Computation outsourcing security** - Another fundamental service enabled within the cloud paradigm is computation outsourcing. By outsourcing workloads to the cloud, users computational power is no longer limited by their resource-constrained devices. Instead, they can enjoy the clouds literally unlimited computing resources in a pay-per-use manner without committing any large capital outlays locally.
  However, current outsourcing practice operates in plaintext that is, it reveals both data and computation results to the commercial public cloud. This can raise big security concerns, especially when the outsourced computation workloads contain sensitive information, such as a businesss financial records, proprietary research data, or even personally identifiable health information. Furthermore, the clouds operational details arent transparent enough to users. Consequently, various motivations can cause the cloud to behave unfaithfully and return incorrect results. These range from possible software bugs, hardware failures, or even outsider attacks to cloud servers deliberately being lazy to save computational costs. Thus, were in great need of secure computation outsourcing mechanisms to both protect sensitive workload information and ensure that the computation results returned from the cloud are correct. This task is difficult, however, due to several challenges that the mechanism design must meet simultaneously. First, such a mechanism must be practically feasible in terms of computational complexity. Otherwise, either the users cost can become prohibitively huge, or the cloud might not be able to complete the outsourced computations in a reasonable amount of time. Second, it must provide sound security guarantees without restricting system assumptions. Namely, it should strike a good balance between security guarantees and practical performance. Third, this mechanism must enable substantial computational savings at the user side compared to the amount of effort required to solve a problem locally. Otherwise, users have no reason to outsource computation to the cloud. A recent breakthrough in fully

homomorphic encryption (FHE) has shown the general results of secure computation outsourcing to be viable in theory. But applying this general mechanism to everyday computing tasks is still far from practical due to FHE operations extremely high complexity, which cant yet be handled in practice [4].

- **Multi-tenancy** - Multi-tenancy means that the cloud platform is shared and utilized by multiple customers. Moreover, in a virtualized environment, data belonging to different customers may be placed on the same physical machine by certain resource allocation policy. Adversaries who may also be legitimate cloud customers may exploit the co-residence issue. A series of security issues such as data breach, computation breach, flooding attack etc., are incurred. Although Multi-tenancy is a definite choice of cloud venders due to its economic efficiency, it provides new vulnerabilities to the cloud platform [5]. From a customers perspective, the notion of using a shared infrastructure could be a huge concern. However, the level of resource sharing and available protection mechanisms can make a big difference. For example, to isolate multiple tenants data, Salesforce.com employs a query rewriter at the database level, whereas Amazon uses hypervisors at the hardware level. Providers must account for issues such as access policies, application deployment, and data access and protection to provide a secure, multi-tenant environment [3].

  Multi-tenancy security and privacy is one of the critical challenges for the public cloud, and finding solutions is pivotal if the cloud is to be widely adopted. However, little work exists today that not only addresses these problems but also consistently and scalably maintains this dynamic computing environments scalability.

- **Massive data and intense computation** - Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected [5].

5. NEED FOR SECURITY IN CLOUD

A users dependence on cloud is analogous to a persons dependence on public transportation as it forces one to trust over which one have no control, limits what one can transport, and subjects us to rules and schedules that wouldn't apply if one had their own vehicles. On the other hand, it is so economical that one doesnt realistically have any alternative.Users of the cloud arent aware about the location of the data and ultimately have to rely on the cloud service provider for exercising appropriate security measures. Therefore cloud security issue is the most important and elicited topic among the IT professionals.
Security in cloud computing is of two types:

- **Data security** It focuses on protecting the software and hardware associated with the cloud. It deals with choosing an apt location for data centers so as to protect it from internal threats, different types of weather conditions, fire and even physical attacks that might destroy the center physically and external threats avoiding unauthorized access and break ins.

- **Network security** Protecting the network over which cloud is running from various attacks DOS, DDOS, IP Spoofing, ARP Spoofing and any novel attacks that intruders may device. Attack on data affects a single user whereas a successful attack on Network has the potential to affect multiple users. Therefore network security is of foremost importance.

5.1 SECURITY AND PRIVACY ATTRIBUTES

Five most representative security and privacy attributes are confidentiality, integrity, availability, accountability, and privacy-preservability, which is shown in figure 5.1. Within the enterprise boundaries, data transmission usually does not require encryption, or just have a simple data encryption measure. For data transmission across enterprise boundaries, both data confidentiality and integrity should be ensured in order to prevent data from being tapped and tampered with by unauthorized users. In other words, only the data encryption is not enough. Data integrity is also needed to be ensured .Therefore it should ensure that transport protocols provide both confidentiality and integrity. Confidentiality and integrity of data transmission need to

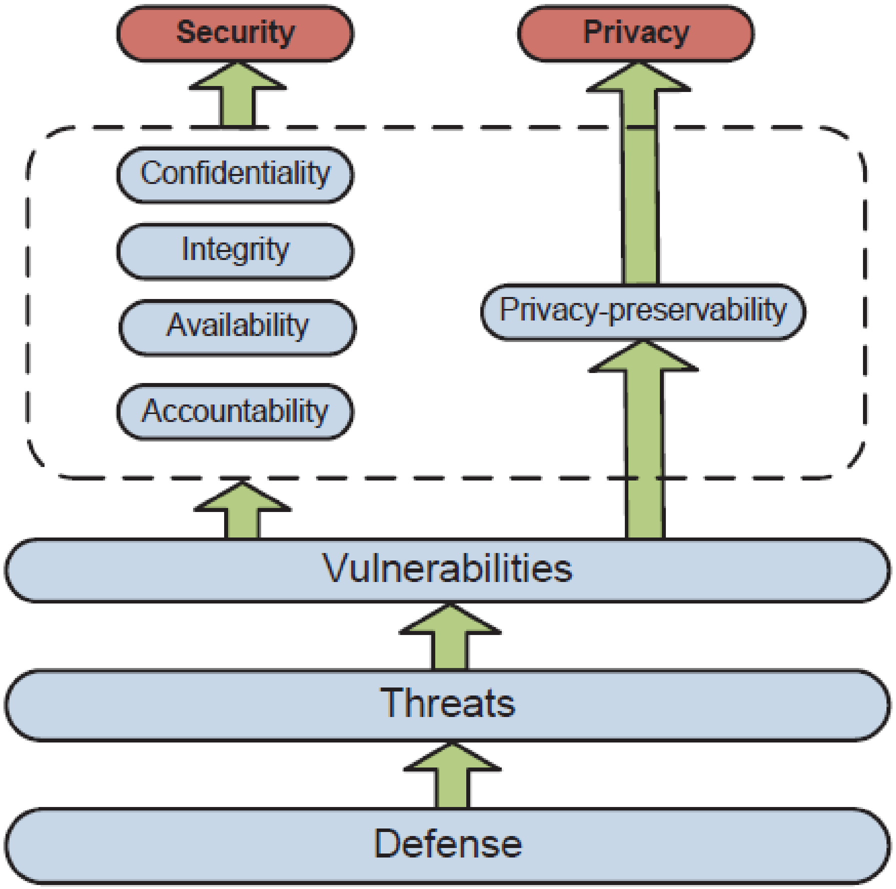

Figure 5.1: Security and privacy attributes

ensure not only between enterprise storage and cloud storage but also between different cloud storage services.[2].
Threats to these attributes and Defence strategies are discussing below.

5.1.1 Cloud confidentiality

Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or Devices. i.e, customers data and computation tasks are to be kept confidential from both the cloud provider and other customers. Confidentiality remains as one of the greatest concerns with regards to cloud computing. This is largely due to the fact that customers outsource their data and computation tasks on cloud servers, which are controlled and managed by potentially untrustworthy cloud providers [5].

User's confidential data is disclosed to a service provider if all of the following three conditions are satisfied simultaneously

- The service provider knows where the users confidential data is located in the cloud computing systems.
- The service provider has privilege to access and collect the user's confidential data in cloud.
- The service provider can understand the meaning of the user's data.

Threats to cloud confidentiality

- *Cross-Virtual Machine(VM) attack via Side Channels* - A Cross-VM attack exploits the nature of multi-tenancy, which enables that VMs belonging to different customers may co-reside on the same physical machine. Timing side-channels as an insidious threat to cloud computing security due to the fact that a) the timing channels pervasively exist and are hard to control due to the nature of massive parallelism and shared infrastructure; b) malicious customers are able to steal information from other ones without leaving a trail or raising alarms.
- *Malicious sysAdmin:* The Cross-VM attack discusses how others may violate confidentiality cloud customers that co-residing with the victim, although it is not the only threat. Privileged sysadmin of the cloud provider can perform attacks by accessing the memory of a customers VMs. For instance, Xenaccess enables a sysadmin to directly access the VM memory at run time by running a user level process in Domain0.

Defence strategies

Approaches to address cross-VM attack fall into six categories: a) placement prevention intends to reduce the success rate of placement; b) physical isolation enforcement; c) new cache designs; d) fuzzy time intends to weaken malicious VMs ability to receive the signal by eliminating fine-grained timers; e) forced VM determinism ensures no timing or other non-deterministic information leaking to adversaries; f) cryptographic implementation of timing-resistant cache [5].

- *Placement prevention:* In order to reduce the risk caused by shared infrastructure, a few suggestions to defend the attack in each step are given in . For instance, cloud providers may obfuscate co-residence by having Dom0 not respond in traceroute, and/or by randomly assigning internal IP addresses to launched VMs. To reduce the success rate of placement, cloud providers might let the users decide where to put their VMs; however, this method does not prevent a brute-force strategy.

- *Co-residency detection:* The ultimate solution of cross-VM attack is to eliminate co-residency. Cloud customers (especially enterprises) may require physical isolation, which can even be written into the *Service Level Agreements* (SLAs). However, cloud vendor may be reluctant to abandon virtualization that is beneficial to cost saving and resource utilization. One of the left options is to share the infrastructure only with friendly VMs, which are owned by the same customer or other trustworthy customers. To ensure physical isolation, a customer should be enabled to verify its VMs exclusive use of a physical machine. HomeAlone is a system that detects co-residency by employing a side-channel (in the L2 memory cache) as a detection tool. The idea is to silence the activity of friendly VMs in a selected portion of L2 cache for a certain amount of time, and then measure the cache usage to check if there is any unexpected activity, which indicates that the physical machine is co-resided by another customer.

- *NoHype:* It attempts to minimize the degree of shared infrastructure by removing the hypervisor while still retaining the key features of virtualization. The NoHype architecture provides a few features: i) the one core per VM feature prevents interference between VMs, eliminates side channels such as L1 cache, and retains multi-tenancy, since each chip has multiple cores; ii) memory partition restricts each VMs memory access on a assigned range; iii) dedicated virtual I/O devices enables each VM to be granted direct access to a dedicated virtual I/O device. NoHype has significantly reduced the hypervisor attack surface, and increased the level of VM isolation. However, NoHype requires to change hardware, making it less practical when consider applying it to current cloud infrastructures.

- *Trusted cloud computing platform(TCCP):* It offers a closed box execution environment for IaaS services. TCCP guarantees confidential execution of guest virtual machines. It also enables customers to attest to the IaaS provider and to determine if the service is secure before their VMs are launched into the cloud. The design goals of TCCP are: 1) to confine the VM execution inside the secure perimeter; 2) that a sysadmin with root privileges is unable to access the memory of a VM hosted in a physical node. TCCP leverages existing techniques to build trusted cloud computing platforms. This focuses on solving confidentiality problems for clients data and for computation outsourced to the cloud. With TCCP, the sysadmin is unable to inspect or tamper with the content of running VMs.

- *Retaining data control back to customer:* Considering the customers fear of losing the data control in cloud environments, it is propose to retain data control for the cloud customers by simply storing encrypted VMs on the cloud servers. Encrypted VM images guarantee rigorous access control since only the authorized users known as key-holders are permitted access. Due to the encryption, the data cannot be mounted and modified within the cloud without an access key, assuring the confidentiality and integrity. This approach offers security guarantees before a VM is launched; however, there are ways to attack the VM during running time and to jeopardize the data and computation.

5.1.2 Cloud integrity

Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

Threats to cloud integrity

- *Data loss/manipulation:* In cloud storage, applications deliver storage as a service. Servers keep large amounts of data that have the capability of being accessed on rare occasions. The cloud servers are distrusted in terms of both security and reliability , which means that data may be lost or modified maliciously or accidentally. Administration errors may cause data loss (e.g., backup and restore, data migration, and changing memberships in P2P systems). Additionally, adversaries may initiate attacks by taking advantage of data owners loss of control over their own data.

- *Dishonest computation in remote servers:* With outsourced computation, it is difficult to judge whether the computation is executed with high integrity. Since the computation details are not transparent enough to cloud customers, cloud servers may behave unfaithfully and return incorrect computing results; they may not follow the semi-honest model. For example, for computations that require large amount of computing resources, there are incentives for the cloud to be lazy . On the other hand, even the semi-honest model is followed, problems may arise when a cloud server uses outdated, vulnerable code, has misconfigured policies or service, or has been previously attacked with a rootkit, triggered by malicious code or data.

Defence strategies

- *Provable data possession (PDP):* The main challenge of integrity checking is that tremendous amounts of data are remotely stored on untrustworthy cloud servers; as a result, methods that require hashing for the entire file become prohibitive. In addition, it is not feasible to download the file from the server and perform an integrity check due to the fact that it is computationally expensive as well as bandwidth consuming. Each of the former notions is not acceptable in cloud environments.

- *Third party auditor (TPA):* Instead of letting customers verify data integrity, it is also possible to offload task of integrity checking to a third party which can be trusted by both cloud provider and customers. It is propose to adopt a TPA to check the integrity of outsourced data in cloud environments. TPA ensures the following: 1) cloud data can be efficiently audited without a local data copy, and cloud clients suffer no on-line overhead for auditing; 2) no new vulnerabilities will be introduced to jeopardize data privacy. The key technique is a publicbased homomorphic authenticator, which has been utilized in existing literatures . When combining a homomorphic authenticator with random masking, TPA becomes unable to access the data content while it is performing auditing.

- *Combating dishonest computing:* Conventional strategies to check external computation integrity fall into four categories:

  Re-computation requires the local machine to re-do the computation, and then compare the results. Re-computation guarantees 100detection, and does not require trusting the cloud vendor. However, the cost is usually unbearable due to the fact that each of the verifications require at least the equal time as the original computation. To this end, customers could possibly have no incentive to verify computation integrity in this manner. A variation of re-computation is sampling, which offers probabilistic guarantees of mistake detection, depending on the degree of sampling. Sampling trades accuracy for efficiency.

  Replication assigns one computation task to multiple machines, and then compares the results. Majority voting may be employed to determine correctness. Replication assumes semi-trust to cloud vender because both computation and verification are conducted remotely. Intelligent adversaries that control certain amounts of machines may bypass replication checking by returning the same incorrect results.

  Auditing usually works together with logging. During the execution of a computation, a logging component records all critical events into a log file, which is subsequently sent to one or multiple auditors for review. Auditing is a typical approach to do forensics investigation. One drawback of auditing is that if the attacker understands the computation better than the auditor, it is possible for the attacker to manipulate data bits without being detected.

  Trusted computing enforces the computer to behave consistently in expected ways with hardware and software support. The key technique of integrity checking is known as remote attestation, which works by having the hardware generate a certificate stating that what software is running. The certificate can then be sent to the verifier to show that the software is unaltered. One assumption of trusted computing is that some component like the hardware and the hypervisor is not physically altered.

5.1.3 Cloud availability

Availability is crucial since the core function of cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system. In this section, we have studied two kinds of threats that impair cloud availability. Threats to Cloud Availability:

Threats to cloud availability

- *Flooding attack via bandwidth starvation:* In a flooding attack, which can cause *Deny of Service* (DoS), a huge amount of nonsensical requests are sent to a particular service to hinder it from working properly. In cloud computing, there are two basic types of flooding attacks:
  Direct DOS the attacking target is determined, and the availability of the targeting cloud service will be fully lost.
  Indirect DOS the meaning is twofold: 1) all services hosted in the same physical machine with the target victim will be affected; 2) the attack is initiated without a specific target.

- *Fraudulent Resource Consumption (FRC) attack:* A representative *Economic Denial of Sustainability* (EDoS) attack is FRC, which is a subtle attack that may be carried out over a long period (usually lasts for weeks) in order to take effect. In cloud computing, the goal of a FRC attack is to deprive the victim (i.e., regular cloud customers) of their long-term economic availability of hosting web contents that are publicly accessible. In other words, attackers, who act as legal cloud service clients, continuously send requests to website hosting in cloud servers to consume bandwidth, which bills to the cloud customer owning the website; seems to the web server, those traffic does not reach the level of service denial, and it is difficult to distinguish FRC traffic from other legitimate traffic. A FRC attack succeeds when it causes financial burden on the victim.

Defence strategies

- *Defending the new DOS attack:* This new type of DOS attack differs from the traditional DOS or DDOS attacks in that traditional DOS sends traffic to the targeting application/host directly while the new DOS attack does not;

therefore, some techniques and counter-measures for handling traditional DOSs are no longer applicable. A DOS avoidance strategy called service migration has been developed to deal with the new flooding attack. A monitoring agent located outside the cloud is set up to detect whether there may be bandwidth starvation by constantly probing the cloud applications. When bandwidth degradation is detected, the monitoring agent will perform application migration, which may stop the service temporarily, with it resuming later. The migration will move the current application to another subnet of which the attacker is unaware.

- *FRC attack detection:* The key of FRC detection is to distinguish FRC traffic from normal activity traffic. Idziorek et al. propose to exploit the consistency and selfsimilarity of aggregate web activity . To achieve this goal, three detection metrics are used: i) Zipf s law are adopted to measure relative frequency and self-similarity of web page popularity; ii) Spearmans footrule is used to find the proximity between two ranked lists, which determines the similarity score; iii) overlap between the reference list and the comparator list measures the similarity between the training data and the test data. Combining the three metrics yields a reliable way of FRC detection.

5.1.4 Cloud accountability

Accountability implies that the capability of identifying a party, with undeniable evidence, is responsible for specific events. When dealing with cloud computing, there are multiple parties that may be involved; a cloud provider and its customers are the two basic ones, and the public clients who use applications (e.g., a web application) outsourced by cloud customers may be another party. A fine-grained identity, however, may be employed to identify a specific machine or even the faulty/ malicious program that is responsible.

Threats to Cloud accountability

- *SLA violation:* the loss of data control is problematic when something goes awry. For instance, the following problems may possibly arise: 1) The machines in the cloud can be mis-configured or defective and can consequently corrupt the customers data or cause his computation to return incorrect results; 2) The cloud provider can accidentally allocate insufficient resources for the customer, an act which can degrade the performance of the customers services and then violate the SLA; 3) An attacker can embed a bug into the customers software in order to steal valuable data or to take over the customers machines for spamming or DoS attacks; 4) The customer may not have access to his data either because the cloud loses it or simply because the data is unavailable at an inconvenient time.

- *Dishonest MapReduce:* MapReduce is a parallel computing paradigm that is widely employed by major cloud providers (Google, Yahoo!, Facebook, etc.). MapReduce splits a large data set into multiple blocks, each of which are subsequently input into a single worker machine for processing. However, working machines may be mis-configured or malicious, as a result, the processing results returned by the cloud may be inaccurate.

- *Hidden identity of adversaries:* Due to privacy concerns, cloud providers should not disclose cloud customer's identity information. Anonymous access is employed to deal with this issue; although anonymity increases privacy, it also introduces security problems. Full anonymity requires that a customers information must be completely hidden from absolutely anyone or anything else. In this case, malicious users can jeopardize the data integrity without being detected since it becomes easier to hide their identities.

- *Inaccurate billing of resource consumption:* The pay-as-you-go model enables customers to decide how to outsource their business based on their necessities as well as the financial situations. However, it is quite difficult for customers to verify the expenses of the resource consumption due to the black box and dynamic nature of cloud computing. From the cloud vendors perspective, in order to achieve maximum profitability, the cloud providers choose to multiplex applications belonging to different customers to keep high utilization. The multiplexing may cause providers to incorrectly attribute resource consumption to customers or implicitly bear additional costs, therefore reducing their costeffectiveness. For example, I/O time and internal network bandwidth are not metered, even though each incurs non-trivial cost. Additionally, metering sharing effects, such as shared memory usage, is difficult.

Defence strategies

- *Accountability on Service Level Agreement(SLA):* To deal with this dispute of an SLA violation, a primitive AUDIT (A, S, t1, t2) is proposed in to allow the customers to check whether the cloud provider has fulfilled the SLA (denoted by A) for service S between time internal t1 and t2. AUDIT will return OK if no fault is detected; otherwise AUDIT will provide verifiable evidence to expose the responsible party.

- *Accountable virtual machine (AVM):* The intent of AVM is to enable users to audit the software execution on remote machines. AVM is able to 1) detect faults, 2) identify faulty node, 3) provides verifiable evidence of a particular fault and point to the responsible party. AVM is applicable to cloud computing in which customers outsource their data and software on distrusted cloud servers. AVM allows cloud users to verify the correctness of their code in the cloud system. The approach is to wrap any running software in a virtual machine, which keeps a tamper-evident log to record the entire execution of the software.

- *Collaborative monitoring:* A solution that is similar to AVM was developed by maintaining an external state machine whose job is to validate the correctness of the data and the execution of business logic in a multi-tenancy environment. The authors in define the service endpoint as the interface through which the cloud services are delivered to its end users. It is assumed that the data may only be accessed through endpoints that are specified according to the SLA between the cloud provider and the users. The basic idea is to wrap each endpoint with an adapter that is able to capture the input/output of the endpoint and record all the operations performed through the endpoint. The log is subsequently sent to the external state machine for authentication purposes.

- *Accountable MapReduce(AMR):* This problem has been addressed with SecureMR, which adopts full task duplication to double check the processing result. SecureMR requires that twice two different machines, which will double the total processing time, execute a task. Additionally, SecureMR suffers false positive when an identical faulty program processes the duplicated tasks.

- *Secure provenance:* Secure provenance is introduced with an aim to ensure that verifiable evidence might be provided to trace the real data owner and the records of data modification. Secure provenance is essential to improve data forensic and accountability in cloud systems. It is proposed a secure provenance scheme based on bilinear paring techniques, first bringing provenance problems into cloud computing. Considering a file stored in cloud, when there is dispute on that file, the cloud can provide all provenance information with the ability to plot all versions of the file and the users that modified it. With this information, a specific user identity can be tracked.

- *Verifiable Resource Accounting:* It enables cloud customers to be assured that i) their applications indeed consumed the resources they were charged for and ii) the consumption was justified based on an agreed policy. The scheme in considers three roles: the customer C, the provider P, and the verifier V. First, C asks P to run task T; then, P generates a report R describing what resources P thinks that C consumes. C then sends the report R and some additional data to V who checks whether R is a valid consumption report. By implementing a trusted hardware layer with other existing technologies such as offloading monitoring, sampling, and snapshot, it can be ensured that a) the provider does not overcharge/undercharge customers and b) the provider correctly assigns the consumption of a resource to the principal responsible for using that resource.

5.1.5 Cloud privacy-preservability

Privacy is yet another critical concern with regards to cloud computing due to the fact that customers data and business logic reside among distrusted cloud servers, which are owned and maintained by the cloud provider. Therefore, there are potential risks that the confidential data (e.g., financial data, health record) or personal information (e.g., personal profile) is disclosed to public or business competitors. Privacy has been an issue of the highest priority. Throughout this text, we regard privacy- preservability as the core attribute of privacy. A few security attributes directly or indirectly influence privacy preservability, including confidentiality, integrity, accountability, etc. Evidently, in order to keep private data from being disclosed, confidentiality becomes indispensable, and integrity ensures that data/computation is not corrupted, which somehow preserves privacy. Accountability, on the contrary, may undermine

TABLE 5.1: Approches of privacy enforcement

Approach	Description
Information centric security	Data objects have access-control policies with them.
Trusted computing	The system will consistently behave in expected ways with hardware or software enforcement.
Cryptographic protocols	Cryptographic techniques and tools are employed to preserve privacy.

privacy due to the fact that the methods of achieving the two attributes usually conflict [5].

Threats to cloud privacy

In some sense, privacy-preservability is a stricter form of confidentiality, due to the notion that they both prevent information leakage. Therefore, if cloud confidentiality is ever violated, privacy-preservability will also be violated. Similar to other security services, the meaning of cloud privacy is two fold: data privacy and computation privacy.

Defence strategies

The privacy-preserving classified into three categories, which are shown in Table 5.1. It is proposed that *Fully Homomorphic Encryption* (FHE) to preserve privacy in cloud computing . FHE enables computation on encrypted data, which is stored in the distrusted servers of the cloud provider. Data may be processed without decryption. The cloud servers have little to no knowledge concerning the input data, the processing function, the result, and any intermediate result values. Therefore, the outsourced computation occurs under the covers in a fully privacy-preserving way. FHE has become a powerful tool to enforce privacy preserving in cloud computing. However, all known FHE schemes are too inefficient for use in practice. While researchers are trying to reduce the complexity of FHE, it is worthwhile to consider alleviating the power of FHE to regain efficiency. Somewhat homomorphic encryption, which only supports a number of homomorphic operations, which may be much faster and more compact than FHE [5].

6. CONCLUSIONS

Every new technology has its pros and cons, similar is the case with cloud computing. Although cloud computing provides easy data storage and access. But there are several issues related to storing and managing data, that is not controlled by owner of the data. This paper discussed security issues for cloud. These issues include cloud integrity, cloud confidentiality, cloud availability, cloud privacy. There are several threats to cloud confidentiality including cross-VM attack and Malicious sysadmin. On the other hand integrity of cloud is compromised due to data loss and dishonest computation in remote servers. Denial of Service attack(Dos) is the most common attack which is also possible in cloud computing network. This attack attempts to prevent the data available to its intended users. The last issue is cloud privacy and it is similar to cloud confidentiality. if cloud confidentiality is at risk, cloud privacy will also be at risk.

REFERENCES

[1] C. Wang, Q, Wan, K. Ren nd Wenjing Lou, "Privacy-Preserving Public Auditing for Data StorageSecurity in Cloud Computing", *Infocom, Proceedings IEEE*, 2010, pp.1-9.

[2] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", in *International Conference on Computer Science and Electronics Engineering(ICCSEE)*, 2012, vol.1, pp.647-651.

[3] H. Takabi, J. B. D. Joshi and G. J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments" , *Security and Privacy, IEEE*, vol.8 , no.6, pp.24-31, Nov/Dec 2010.

[4] K. Ren, C. Wang and Q. Wang, "Security Challenges for the Public Cloud", *Internet Computing, IEEE* , vol.16, no.1, pp.69-73, Jan/Feb 2012.

[5] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing ",*IEEE Commun. Surveys and Tutorials*, vol. 15, no.2, pp.843 - 859, Second quarter 2013.

[6] Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, (Released December 17, 2009). (http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf. Accessed Jan. 13, 2011.)