# Survey on Cloud Computing Security

Shilpashree Srinivasamurthy
*Department of Computer Science*
*Indiana University – Purdue University Fort Wayne*
*Fort Wayne, IN 46805*
*srins01@students.ipfw.edu*

David Q. Liu
*Department of Computer Science*
*Indiana University – Purdue University Fort Wayne*
*Fort Wayne, IN 46805*
*liud@ipfw.edu*

## Abstract

*Cloud computing may be defined as management and provision of resources, software, applications and information as services over the cloud (internet) on demand. Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. With its ability to provide users dynamically scalable, shared resources over the Internet and avoid large upfront fixed costs, cloud computing has recently emerged as a promising hosting platform that performs an intelligent usage of a collection of services, applications, information and infrastructure comprised of pools of computer, network, information and storage resources. However along with these advantages, storing a large amount of data including critical information on the cloud motivates highly skilled hackers thus creating a need for the security to be considered as one of the top issues while considering Cloud Computing. In this paper we explain the cloud computing along with its open secure architecture advantages in brief and emphasize on various security threats in cloud computing also the existing methods to control them along with their pros and cons.*

## 1. Introduction

Cloud computing is the collection of virtualized and scalable resources, capable of hosting application and providing required services to the users with the "pay only for use" strategy where the users pay only for the number of service units they consume. A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way. [2]

### 1.1. Characteristics of cloud computing

Cloud computing exhibit five essential characteristics defined by NIST (National Institute of Standards and Technology) [1].

**1. On-demand self-service**. A consumer can unilaterally provision computing capabilities.

**2. Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

**3. Resource pooling.** The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

**4. Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

**5. Measured service**. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

## 2. Open Security Architecture of cloud computing

Cloud computing can be defined as the provision of computing services via the Internet such as [7] Applications (software-as-a-service, or SaaS), Platforms, Infrastructure (IaaS), Process orchestration and integration

Figure 1 shows the open secure architecture of cloud computing [4]. The Open Security Architecture cloud computing pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis.

The various controls in this architecture are [7]

- SA-1/4/5 System and Services Acquisition: ensure that acquisition of services is managed correctly.
- CP-1 (contingency planning): ensure a clear understanding of how to respond in the event of interruptions to service delivery.

- Risk Assessments controls: helps to understand the risks associated with services in a business context.

The pattern also provides a view into activities that are shared by security architects, security managers, and business managers. They should:

- Agree on the control baseline applicable to this cloud sourcing activity/service.
- Confirm how this translates into the control framework of the cloud provider.
- Decide on additional risk mitigating controls.

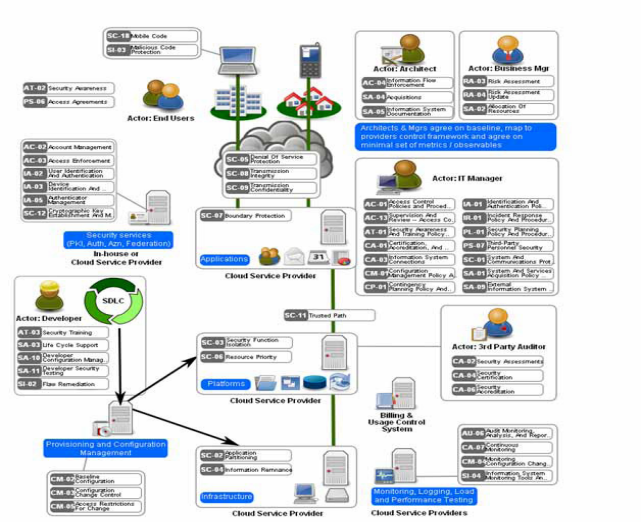


**Figure 1. Cloud Computing Model - Open Secure Architecture [OSA09].**

There are a number of key control areas that should be considered carefully before moving the computing operations to cloud services: Contractual agreements, Certification and third-party audits, Compliance requirements, Availability, reliability, and resilience, Backup and recovery, Service levels and performance, Decommissioning. If the process is comprised of a number of cloud services, then supporting services such as security, load monitoring & testing and provisioning and configuration management are required.

## 3. Feasibility of Cloud Computing

### 3. 1. Advantages of Cloud Computing [4]:

The following are some of the major advantages of cloud computing:

- **Virtualization.** Virtualization is defined as decoupling and separation of the business service from the infrastructure needed to run it.
- **Flexibility to choose vendor.**
- **Elasticity.** Elastic nature of the infrastructure allows to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis.
- **Cost Reduction.** Reduced costs due to operational efficiencies, and more rapid deployment of new business services.

### 3.2. Obstacles and opportunities of cloud computing

The following table shows the top ten obstacles and opportunities of cloud computing.

**Table1. Obstacles and opportunities of cloud computing [3].**

| No | Obstacle | Opportunities |
|---|---|---|
| 1 | Availability/Business Continuity | Use Multiple Cloud Providers |
| 2 | Data Lock-In | Standardize APIs; Compatible SW to enable Surge or Hybrid Cloud Computing |
| 3 | Data Confidentiality and Auditability | Deploy Encryption, VLANs, Firewalls |
| 4 | Data Transfer Bottlenecks | FedExing Disks; Higher BW Switches |
| 5 | Performance Unpredictability | Improved VM Support; Flash Memory; Gang Schedule VMs |
| 6 | Scalable Storage | Invent Scalable Store |
| 7 | Bugs in Large Distributed Systems | Invent Debugger that relies on Distributed VMs |
| 8 | Scaling Quickly | Invent Auto-Scalar that relies on ML; Snapshots for Conservation |
| 9 | Reputation Fate Sharing | Offer reputation-guarding services like those for email |
| 10 | Software Licensing | Pay-for-use licenses |

Despite of these obstacles as well as opportunities and advantages, cloud computing raises several security issues and hence security is still the primary concern of many customers who want to leverage public cloud services.

## 4. Cloud Computing Security Threats

### 4.1. Top Seven Security Threats

Top seven security threats to cloud computing discovered by “Cloud Security Alliance” (CSA) are [6]:

**1. Abuse and Nefarious Use of Cloud Computing.** Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

Suggested remedies by the CSA to lessen this threat:

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

**2. Insecure Application Programming Interfaces.** As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

Suggested remedies by CSA to lessen this threat:

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

**3. Malicious Insiders.** The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

Suggested remedies by CSA to lessen this threat:

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

**4. Shared Technology Vulnerabilities.** Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.

Suggested remedies by CSA to lessen this threat:

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

**5. Data Loss/Leakage.** Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe

Suggested remedies by CSA to lessen this threat:

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyze data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers to wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

**6. Account, Service & Traffic Hijacking.** Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of-service attacks.

Suggested remedies by CSA to lessen this threat:

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

**7. Unknown Risk Profile.** Security should always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts - all things that should always be kept in mind.

Suggested remedies by CSA to lessen this threat:

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.,* patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

### 4.2. Other Security Threats [14, 18]

1. **Failures in Providers Security.** Cloud providers control the hardware and the hypervisors on which data is stored and applications are run and hence their security is very important while designing cloud.
2. **Attacks by other customer.** If the barriers between customers break down, one customer can access another customer's data or interfere with their applications.
3. **Availability and reliability issues**. The cloud is only usable through the Internet so Internet reliability and availability is essential.
4. **Legal and Regulatory issues**. The virtual, international nature of cloud computing raises many legal and regulatory issues regarding the data exported outside the jurisdiction.
5. **Perimeter security model broken.** Many organizations use a perimeter security model with strong security at the perimeter of the enterprise network. The cloud is certainly outside the perimeter of enterprise control but it will now store critical data and applications.
6. **Integrating Provider and Customer Security Systems**. Cloud providers must integrate with existing systems or the bad old days of manual provisioning and uncoordinated response will return.

## 5. Security in Cloud Computing [7]

- **Infrastructure Security.** The security challenges at various levels namely network level, host level and application level are not specifically caused by cloud computing instead are exacerbated by its use. The issues of infrastructure security and cloud computing can be addressed by clearly defining trust boundaries by understanding which party provides which part of security [7].

- **Data Security and Storage.** Data security is a significant task, with a lot of complexity. Methods of data protection, such as redaction, truncations, obfuscation, and others, should be viewed with great concern. Not only are there no accepted standards for these alternative methods, but also there are no programs to validate the implementations of whatever could possibly be developed. Homomorphic encryption can be used for data security encryption. But with this approach key management is a problem [7].

- **Identity and Access Management (IAM).** The key critical success factor to managing identities at cloud providers is to have a robust federated identity management architecture and strategy internal to the organization. Using cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with cloud providers [8].

- **Security Management.** From a security management perspective, a key issue is the lack of enterprise-grade access management features. The scope of security management of cloud services will vary with the service delivery model, provider capabilities, and maturity. Customers will have to make trade-offs with respect to the flexibility and control offered by the SPI services. The more flexible the service, the more control you can exercise on the service, and with that come additional security management responsibilities. In a virtualized environment where infrastructure is shared across multiple tenants, your data is commingled with that of other customers at every phase of the life cycle—during transit, processing, and storage. Hence, it is important to understand the location of the service, service-level guarantees such as inter-node communication, and storage access (read and write) latency [7].

- **Privacy.** Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design. The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. The following tips are recommended for cloud system designers, architects, developers and Testers [9].
  1. Minimize personal information sent to and stored in the cloud.
  2. Protect personal information in the cloud.
  3. Maximize user control.
  4. Allow user choice.
  5. Specify and limit the purpose of data usage.
  6. Provide feedback.

  (Please refer [21] for more details on privacy).

- **Audit and Compliance.** A programmatic approach to monitoring and compliance will help prepare CSPs (Cloud Service Provider) and their users to address emerging requirements and the evolution of cloud business models. To drive efficiency, risk management, and compliance, CSPs need to implement a strong internal control monitoring function coupled with a robust external audit process. To gain comfort over their in-cloud activities, CSP users need to define their control requirements, understand their CSP's internal control monitoring processes, analyze relevant external audit reports, and properly execute their responsibilities as CSP users [7].

- **Security-as-a [cloud] Service.** Security-as-a-service is likely to see significant future growth for two reasons. First, a continuing shift in information security work from in-house to outsourced will continue. Second, several other information security needs are present for organizations currently, but they will accelerate in need and complexity with the growing adoption of cloud computing. The two proactive controls are important to the growth of cloud computing: identity management that is inter-cloud and scalable to the cloud size, and (encryption) key management. The two reactive controls are needed for audit and compliance purposes as well: scalable and effective SIEM, and data leakage prevention (DLP). Providing solutions to each of these controls will be difficult and requires significant complexity that must be hugely scalable and yet easy to use [7].

## 6. EXISTING SOLUTIONS FOR SECURITY THREATS

### 6.1. Mirage Image Management System [10]

The security and integrity of VM images are the foundation for the overall security of the cloud since many of them are designed to be shared by different and often unrelated users. This system addresses the issues related to secure management of the virtual-machine images that encapsulate each application of the cloud.

Figure 2 shows the overall architecture of Mirage Image Management System.

Mirage Image Management System consists of 4 major components:

1. **Access Control**. This framework regulates the sharing of VM images. Each image in the repository has a unique owner, who can share images with trusted parties by granting access permissions.
2. **Image Transformation by Running Filters.** Filters remove unwanted information from images at publishes and retrieval time. Filters at publish time can remove or hide sensitive information from the publisher's original image. Filters at retrieval time filters may be specified by the publisher or the retriever.
3. **Provenance Tracking.** This mechanism that tracks the derivation history of an image.
4. **Image maintenance**. Repository maintenance services, such as periodic virus scanning, that detect and fix vulnerabilities discovered after images are published.

**Advantages.** Filters mitigate the risk in a systematic and efficient way. The system stores all the revisions which allows the user to go back to the previous version if the current version if she desires. The default access permission for an image is private so that only owner and system administrator can access the image and hence untrusted parties cannot access the image.

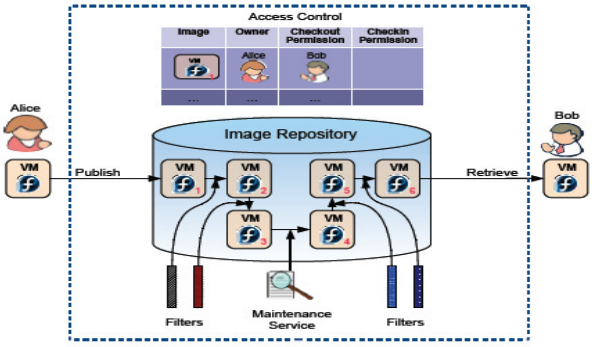


**Figure 2. Architecture of Mirage Image Management System.**

**Limitations.** Huge performance overheads, both in space and time. Filters cannot be 100% accurate and hence the system does not eliminate risk entirely. Virus scanning does not guarantee to find all malware in an image. "The ability to monitor or control customer content" might increase the liability of the repository provider
(For detailed explanation about Mirage Image Management System please refer [21]).

### 6.2. Client Based Privacy Manager [11]

Client based privacy manager helps to reduce the risk of data leakage and loss of privacy of the sensitive data processed in the cloud, and provides additional privacy-related benefits.

Figure 3 shows the overall architecture of the privacy manager. The main features of the privacy manager are:

- **Obfuscation.** This feature can automatically obfuscate some or all of the fields in a data structure before it is sent off to the cloud for processing, and translate the output from the cloud back into de-obfuscated form. The obfuscation and de-obfuscation is done using a key which is chosen by the user and not revealed to cloud service providers.
- **Preference Setting.** This is a method for allowing users to set their preferences about the handling of personal data that is stored in an unobfuscated form within the cloud. This feature allows the user greater control over the usage of his data.
- **Data Access.** The Privacy Manager contains a module that allows users to access personal information in the cloud, in order to see what is being held about them,

and to check its accuracy. This is an auditing mechanism which will detect privacy violations once they have happened.

- **Feedback.** The Feedback module manages and displays feedback to the user regarding usage of his personal information, including notification of data usage in the cloud. This module could monitor personal data that is transferred from the platform.
- **Personae.** This feature allows the user to choose between multiple personae when interacting with cloud services. (Please refer [21] for detailed description of Privacy Manager).

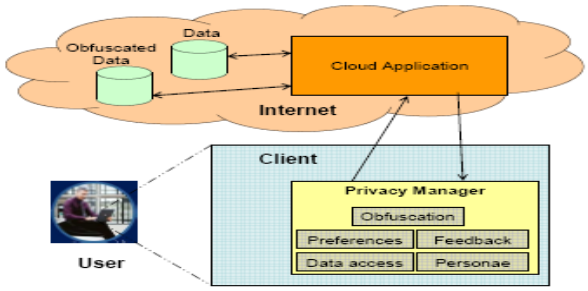


**Figure 3. Overview of Privacy Manager.**

**Advantages.** This solution solves many practical problems such as Sales Force Automation Problem, Customized End-User Services Problem and Share Portfolio Calculation problem. (Please refer [21] for detailed explanation of these solutions)

**Disadvantages.** If the service provider does not provide full cooperation the features of the Privacy Manager other than obfuscation will not be effective, since they require the honest cooperation of the service provider. The ability to use obfuscation without any cooperation from the service provider depends not only on the user having sufficient computing resources to carry out the obfuscation and deobfuscation, but also on the application having been implemented in such a way that it will work with obfuscation.

### 6.3. Transparent Cloud Protection System (TCPS) [12]

TCPS is a protection system for clouds aimed at transparently monitoring the integrity of cloud components. TCPS is intended to protect the integrity of guest Virtual Machines (VM) and of the distributed computing middleware by allowing the host to monitor guest VMs and infrastructure components.

Figure 4 shows the architecture of TCPS. TCPS is a middleware whose core is located between the Kernel and the virtualization layer. (Please refer [21] for detailed explanation of TCPS architecture). By either actively or passively monitoring key kernel or cloud components TCPS can detect any possible modification to kernel data and code, thus guaranteeing that kernel and cloud middleware integrity has not been compromised and consequently no attacker has made its way into the system.

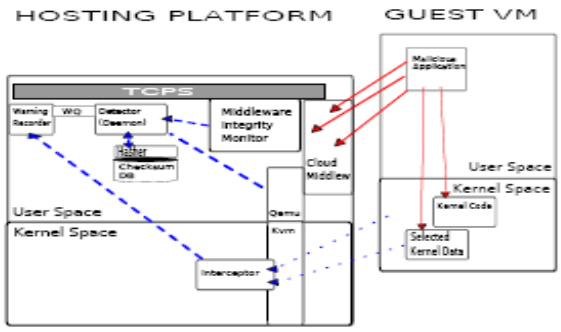


**Figure 4. TCPS Architecture.**

All TCPS modules reside on the Host and Qemu is leveraged to access the guest. Suspicious guest activity can be noticed by the Interceptor and they are recorded by the Warning Recorder into the Warning Queue where the potential alteration will be evaluated by the Detector component. TCPS can locally react to security breaches or notify the distributed computing security components of such an occurrence. In order to avoid false positives as much as possible, an administrator can notify TCPS of the new components' checksum.

**Advantages.** This system is effective in detecting most kind of attacks. This system is able to avoid false-positives (Guest maintenance tolerance). The system minimizes the visibility from the VMs (Transparency). The system and the sibling guests are protected from attacks of a compromised guest. The system can be deployed on majority of the available middleware.The system can detect an intrusion attempt over a guest and, if required by the security policy, takes appropriate actions against the attempt or against the compromised guest and/or notify remote middleware security-management components.

### 6.4. Secure and Efficient Access to Outsourced Data [13]

Providing secure and efficient access to outsourced data is an important component of cloud computing and forms the foundation for information management and other operations.

**Problem.** Figure 5 shows the typical owner-write-user-read scenario. Only the owner can make updates to the outsourced data, while the users can read the information according to access rights. Since the data owner stores a large amount of information on the untrusted service provider, the owner has to encrypt the outsourced data

before putting on the server. The outsourced data will be accessed by different end users all over the network and hence computationally expensive operations on the data blocks (smallest unit of data) should be avoided and the amount of data stored in the end users must be reduced. Right keys should be provided to the end users to control their access.

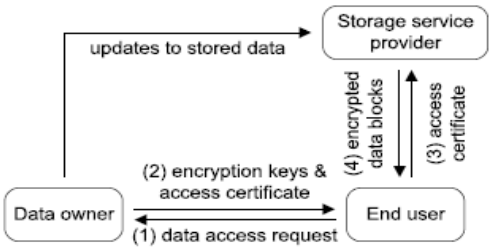


**Figure 5. Illustration of application scenario**

**Solution.** Fine-grained access control should be provided for the outsourced data by encrypting every data block with a different symmetric key. (Please refer [21] for key derivation method).

**Data Access Procedure.**

1. End user U will send a data access request to the data owner O.
   U -> O: {U, O, $E_{Kou}$ , (U, O, request index, data block indexes, MAC code)}
2. Data owner O authenticates the sender, verify the request and determine the smallest key set
   O-> U: { U, O, $E_{Kou}$, (O, U, request index, ACM index, seed for P(), $K^{l}$, cert for S, MAC code)}
   The cert in the packet is a certificate for the service provider and it has the following format:
   {$E_{Kos}$, (U, request index, ACM index, seed, indexes of data blocks, MAC code)}
3. End user U sends {U, S, request index, cert} to the service provider S.
4. Service Provider S verifies the cert, check the user and ACM index, and retrieve data blocks, and conduct over encryption as follows. Using seed as the initial state of P(), the function will generate a long sequence of pseudo random bits. S will use this bit sequence as one-time pad and conduct the xor operation to the encrypted blocks. The computation results will then be sent to U.
5. End user U receives the data blocks, use seed and $K^{l}$ to derive keys, and then recover the data.

**Dynamics in Use Access Rights.**

- **Grant Access Right.** The owner will change the access control matrix and increase the value of ACM index. The service provider and end user do not need to change to adapt to this update.
- **Revoke Access Right:** If the service provider conducts over encryption, the owner updates the access control matrix, increases the value of ACM index and sends this new ACM index to the service provider until it receives acknowledgement. If the services provider refuses to conduct over encryption, then adopt lazy revocation to prevent revoked users from getting access to updated data blocks.

**Dynamics in Outsourced Data.**

- **Block Deletion.** A special control block is used to replace the deleted block. The owner will label its access control matrix to show that the block no longer exists
- **Block Update.** The control block is encrypted with $k_{p,i}$ and write it to the i-th block of the outsourced data. The control block will contain the following information: (1) a pointer to the data block in which $D^{l}_{i}$ is currently stored; (2) information used by the data owner to derive the encryption key of $D^{l}_{i}$ ; (3) information used by the data owner to verify the integrity of the control block. The owner will also use the new secret to encrypt $D_{0i}$ and write it to the corresponding place in S.
- **Block Insertion and Appending.** The data owner will locate an unused block index, derive the encryption key in the hierarchy using $k_{0,1}$, encrypt the data block, and store it on the service provider. The new data blocks are inserted based on their access patterns.

**Advantages.** Data access procedure reduces the overhead of the data owner and prevents the revoked users from getting access to the outsourced data. This approach is robust against collusive attacks if the hash function is safe. Over-encryption conducted by the service provider defends against eavesdroppers even when they have the data block encryption keys. This approach has less communication and overhead for data retrieval when they have infrequent update operations. This approach handles user revocation without impacting service provider.

**Disadvantages.** This approach is applicable only for owner-write-users-read applications and hence not generic. There is a lengthened data retrieval delay caused by the access to updated data blocks. (For detailed explanation of this approach please refer Survey on Cloud Computing Security – Technical Report)

## 7. Conclusion

More than ten papers were surveyed regarding the cloud computing, advantages of cloud computing, risks in cloud computing and various approaches to solve those risks each with their pros and cons. Each algorithm is

aimed at solving a particular risk. However cloud computing is still struggling in its infancy, with positive and negative comments made on its possible implementation for a large-sized enterprise. IT technicians are spearheading the challenge and pursuing research to improve on its drawbacks. Several groups have recently been formed, such as the Cloud Security Alliance or the Open Cloud Consortium, with the goal of exploring the possibilities offered by cloud computing and to establish a common language among different providers. Cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it [17].

## 8. References


[1] The NIST Definition of Cloud Computing, version 15, by Peter Mell and Tim Grance, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov)

[2] Wang, Lizhe; von Laszewski, Gregor; Kunze, Marcel; Tao, Jie. Cloud computing: A Perspective study, *Proceedings of the Grid Computing Environments (GCE) workshop. Held at the Austin Civic Center: Austin, Texas*: 16 November 2008.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. *Communications of the ACM , Volume 53 Issue 4*, pages 50-58. April 2010.

[4] Open Security Architecture http://www.opensecurityarchitecture.org/

[5] Steve Bennett, Mans Bhuller, Robert Covington. Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing. August 2009. DOI= http://www.oracle.com/technology/architect/entarch/pdf/architectural_strategies_for_cloud_computing.pdf

[6] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI = http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[7] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009

[8] Discovering Identity: Cloud Computing: Identity and Access Management DOI = http://blogs.sun.com/identity/entry/cloud_computing_identity_and_access

[9] Siani Pearson. Taking Account of Privacy when Designing Cloud Computing Services. *CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing,* pages 44-52. May 2009

[10] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning. Managing security of virtual machine images in a cloud environment. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security* pages 91-96. November 2009.

[11] Miranda Mowbray, Siani Pearson. A Client-Based Privacy Manager for Cloud Computing**.** *COMSWARE '09: Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middleware* . June 2009

[12] Flavio Lombardi, Roberto Di Pietro. Transparent Security for Cloud. *SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing,* pages 414-415. March 2010.

[13] Weichao Wang, Zhiwei Li, Rodney Owens, Bharat Bhargava. Secure and Efficient Access to Outsourced Data. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security,* pages 55-65. November 2009

[14] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, Jesus Molina. Controlling Data in the Cloud Outsourcing Computation without Outsourcing Control. *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security,* pages 85-90. November 2009.

[15] Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong. Securing Elastic Applications on Mobile Devices for Cloud Computing**.** *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, pages- 127-134. November 2009.

[16] Top 7 threats to cloud computing DOI = www.net-security.org/secworld.php?id=8943

[17] Traian Andrei, Raj Jain. Cloud Computing Challenges and Related Security Issues. A Survey Paper. DOI = http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud.pdf

[18] Steve Hanna. A security analysis of Cloud Computing. Cloud Computing Journal. DOI = http://cloudcomputing.sys-con.com/node/1203943

[19] Amazon, Amazon Elastic Compute Cloud (ec2), DOI = http://aws.amazon.com/ec2/.

[20] Amazon CloudFront. DOI = http://aws.amazon.com/cloudfront/

[21] Shilpashree Srinivasamurthy, David Q. Liu, Survey on Cloud Computing Security – Technical Report. *Department of Computer Science, Indiana University Purdue University Fort Wayne* July 2010.