International Journal of Scientific Research in Computer Science and Engineering

Research Paper

Volume-1, Issue-1, Jan - Feb-2013

Available online at www.isroset.org

ISSN 2320-7639

Security Enhancement in Cloud Computing (CC)

Shivlal Mewada* and Umesh Kumar Singh[#] and Pradeep Sharma[##]
*[#]*Institute of Computer Science, Vikram University, Ujjain – INDIA*
[##]*Dept. of Computer Science, Govt. Holkar Science College, Indore, India*

Abstract— **Cloud computing (CC) is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. CC is becoming one of the most important areas in the Information Technology world. Several issues and challenges are being raised from the adoption of this computational paradigm including security, privacy and authentication and association. In this paper aims to introduce new security ideas in cloud computing. In this paper, we describe the specifics of cloud computing, we address the principal security issues for cloud computing and we discuss primary cloud operations that need to be secured and we discuss the data security based model for cloud computing. We identify the new challenges and opportunities posed by this new cloud computing environment and explore approaches to secure its communication.**

Key words— *Cloud Computing; Security Model; Privacy; Authentication*

I. Introduction

Distributed computing is suffering from high scalability because it affects the performance of the resources. The volume of data quadruples in every 22 month while available processor speed doubles during same time period which does not allow centralized storage of data [1]. So we need some highly decentralized storage systems called "cloud" developed by major Internet based companies hence cloud computing supports distributed computing so that performance can be maintained by resource utilization in highly scalable environment.

The industry is moving towards the cloud computing, it will completely change the way we use the computer and the Internet. Cloud computing concerns with feasible ways to storing information and running applications. Instead of running application and data on an individual desktop computer, everything is kept in the cloud, a large pool of computers and servers accessed by the Internet [2, 3].Cloud computing allows us to access all the documents and applications from anywhere in the world, i.e. it frees users from the limitations of the desktop and makes it easier for group members in different locations to communicate with each other.

Cloud computing is the computing analogous to the electricity revolution of a century ago. Before the advent of electrical utilities, stand alone generators were the medium of generation of electricity required for every farm and business. After the creation of electrical grid, farms and businesses switch off their generators and bought electricity from the utilities, because the price was much lower and the system was more reliable than the production of their own capabilities [2]. Same type of revolution is making cloud computing so much popular that's why the industries are looking it as a future scope but major concern is security, putting everything in the cloud makes highly unsecured environment The desktop-based concept of computing that we are using today is not as much capable as we could expect the universal access, 24X7 reliability, and ubiquitous collaboration promised by cloud computing.

II. Characteristics of Cloud Computing

No definition of the term 'Cloud Computing' has yet succeeded in becoming universally acceptable. Definitions are often used in publications and presentations that are extremely similar to each other while nonetheless differing. One definition that is frequently drawn upon by experts is that of the USA's National Institute of Standards and Technology (NIST) [4], which is also used by ENISA [5]:

"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 released with minimal management effort or service provider interaction."

Cloud computing exhibit five essential characteristics defined by NIST (National Institute of Standards and Technology) [6].

- *On-demand self-service:* A consumer can unilaterally provision computing capabilities.
- *Broad network access:* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
- *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.
- *Rapid elasticity:* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.
- *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.

III. Cloud Computing Models

The architecture of Cloud computing can be categorized according to the three types of delivery models, namely Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS).

1. Infrastructure as a Service (IaaS): With IaaS, IT resources such as processing power, data storage and networks are available as a service. A cloud customer buys these virtualized

Corresponding Author: P Sharma, psharma29762@gmail.com

and, to a large degree, standardised services and adds their own services on top for internal or external use. For example, a cloud customer can rent server time, working memory and data storage and have an operating system run on top with applications of their own choice.

2. Platform as a Service (PaaS): A PaaS provider provides a complete infrastructure and, on the platform, provides the customer with standardized interfaces to be used by the customer's services. For example, the platform can provide multi-tenancy, scalability, access controls, database accesses, etc. as a service. The customer has no access to the underlying layers (operating system, hardware), but can run their own applications on the platform, for which the CSP will usually provide its own tools.

3. Software as a Service (SaaS): Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multi tenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet [7]. Combining the three types of clouds with the delivery models we get a holistic cloud illustration as seen in Figure 3, surrounded by connectivity devices coupled with information security themes. Virtualized physical resources, virtualized infrastructure, as well as virtualized middleware platforms and business applications are being provided and consumed as services in the Cloud [8].

Cloud vendors and clients' need to maintain Cloud computing security at all interfaces. The next section of the paper introduces challenges faced in the Cloud computing domain.

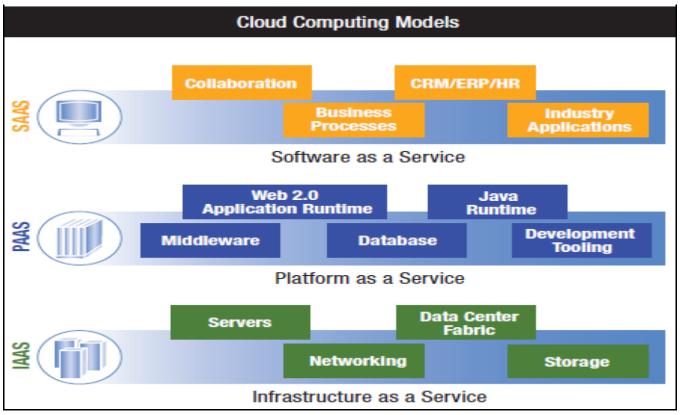


Figure1: Cloud computing service delivery models

IV. Types of Cloud

There are four fundamental deployment models for cloud computing and the differences relate to who accesses the services [9], how it is made available, who controls the infrastructure and where the infrastructure is located. These different characteristics have an impact on the opportunities and risks associated with each deployment model.

A) Public Cloud: The primary benefit of a public cloud deployment is cost efficiency for the user in terms of capital expenditure and management overheads. Disadvantages include risks associated with data security, privacy, performance, latency, location and ownership of data [9]. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third-party and may exist-on-premise or off-premise.

B) Private Cloud: Private cloud deployment based either on internal or third party resources offers greater control over your business information and therefore addresses many of the abovementioned risks. The trade-offs however are higher costs for procuring or renting sites and managing infrastructure that enables cloud [10]. Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third-party and may exist-on-premise or off-premise.

C) Community cloud: Community cloud involves a private cloud that is shared by several organizations with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. An example community cloud is the sharing of a private cloud by several agencies of the same government.

D) Hybrid Cloud: A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [11]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Clouds provide more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems.

V. Security Threats in CC

Top security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are [12]:

1. Abuse and Nefarious Use of Cloud Computing. Abuse and nefarious use of cloud computing is the to p threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers' ca infiltrates 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. 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.

8. Attacks by other customer. If the barriers between customers break down, one customer can access another customer's data or interfere with their applications.

9. Availability and reliability issues. The cloud is only usable through the Internet so Internet reliability and availability is essential.

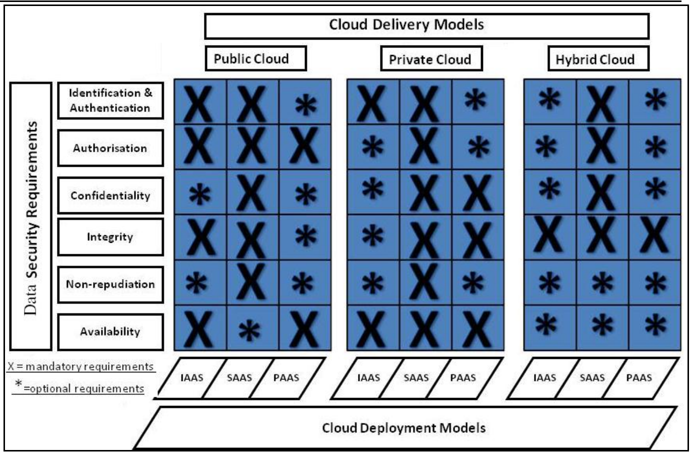
10. Legal and Regulatory issues. The virtual, international nature of cloud computing raises many legal and regulatory issues regarding the data exported outside the jurisdiction.

11. 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.

12. 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.

VI. SECURITY REQUIREMENTS

In the International Standards Organization 7498-2 standard [13], produced by The ISO, Information Security should cover a number of suggested themes. Cloud computing security should also be guided in this regard in order to become an effective and secure technology solution.



Data Security Requirements	Public Cloud			Private Cloud			Hybrid Cloud		
	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS
Identification & Authentication	X	X	*	X	X	*	*	X	*
Authorisation	X	X	X	*	X	*	*	X	*
Confidentiality	*	X	*	*	X	X	*	X	*
Integrity	X	X	*	*	X	X	X	X	X
Non-repudiation	*	X	*	*	X	*	*	*	*
Availability	X	*	X	X	X	X	*	*	*

Figure: 2 Cloud Computing Security Requirement

Figure 2, illustrating the information security requirements coupled with the Cloud computing deployment model and delivery models has been adapted from Eloff et al [14]. In Figure 2, the different cloud delivery models and deployment models are matched up against the information security requirements with an "X" denoting mandatory requirements and an asterisk (*) denoting optional requirements. However future task is needed in investigating of the optimal balance required in securing Cloud computing. Figure 2 should be viewed in context as a guideline in assessing the security level. Each of the security requirements will be highlighted below in context of Cloud computing.

1) Identification: In Cloud computing, depending on the type of cloud as well as the delivery model, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly. This process is targeting at verifying and validating individual cloud users by employing usernames and passwords protections to their cloud profiles.

2) Authentication: : In Cloud computing, depending on the type of cloud as well as the delivery model, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly. This process is targeting at verifying and validating individual cloud users by employing usernames and passwords protections to their cloud profiles.

3) Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

4) Authorisation: Authorisation is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing. Authorisation is maintained by the system administrator in a Private cloud.

5) Confidentiality: In Cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. It is a must when employing a Public cloud due to public clouds accessibility nature. Asserting confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications.

6) Integrity: The integrity requirement lies in applying the due diligence within the cloud domain mainly when accessing data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the cloud's data should without a doubt be robustly imposed across all Cloud computing deliver models

7) Non-repudiation: Non-repudiation in Cloud computing can be obtained by applying the traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).

8) Availability: Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability in cloud services and resources between the cloud provider and client.

Therefore by exploring the information security requirements at each of the various cloud deployment and delivery models set out by the ISO, vendors and organizations can become confident in promoting a highly protected safe and sound cloud framework.

VII. Security Enhancement In Cloud Computing

A. 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 [15].

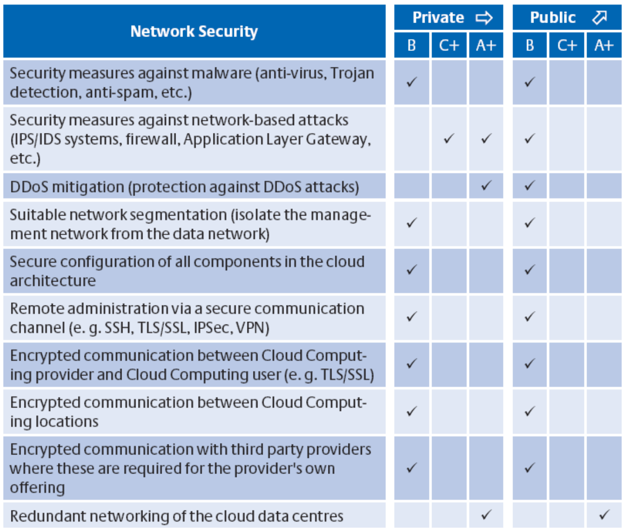
1. Minimize personal information sent to and stored in the cloud.
2. Protect personal information in the cloud.
3. Maximize user control.
4. Allow user choice.
5. Specify and limit the purpose of data usage.
6. Provide feedback.

B. Identity and Access Management. 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 [16].

C. Security governance: A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. This committee must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions.

D. Network security: In the past, Cloud Computing platforms have often been misused either by placing malware there which is then used to send spam, or their processing power has been exploited to crack passwords using brute force attacks or to hide command and control servers (C&C servers) used to control botnets. To prevent these and similar attacks as well as the misuse of resources, each CSP should take effective security measures to defend against network-based attacks.

As well as the usual IT security measures such as anti-virus protection, Trojan detection, spam protection, firewalls, Application Layer Gateway and IDS/IPS systems, particular care should be taken to encrypt all communication between the CSP and the customer and between the provider's sites. If a third party provider is required to deliver the services, the communication with them also needs to be encrypted.



Network Security	Private ⇨			Public ⬀		
	B	C+	A+	B	C+	A+
Security measures against malware (anti-virus, Trojan detection, anti-spam, etc.)	✓			✓		
Security measures against network-based attacks (IPS/IDS systems, firewall, Application Layer Gateway, etc.)		✓	✓	✓		
DDoS mitigation (protection against DDoS attacks)			✓	✓		
Suitable network segmentation (isolate the management network from the data network)	✓			✓		
Secure configuration of all components in the cloud architecture	✓			✓		
Remote administration via a secure communication channel (e. g. SSH, TLS/SSL, IPSec, VPN)	✓			✓		
Encrypted communication between Cloud Computing provider and Cloud Computing user (e. g. TLS/SSL)	✓			✓		
Encrypted communication between Cloud Computing locations	✓			✓		
Encrypted communication with third party providers where these are required for the provider's own offering	✓			✓		
Redundant networking of the cloud data centres			✓			✓

Because of the concentration of resources in centralized data centres, an attack which is a particular threat to public Cloud Computing platforms is the Distributed Denial of Service (DDoS) attack. According to a report by Arbor Networks, a provider of security solutions, DDoS attacks (such as the DNS Amplification/Reflection Attack) can now achieve enormous bit rates (over 100 Gbps) [17]. A standard backbone is designed for a far lower data rate. As a result, many CSPs can hardly defend against DDoS attacks using high data rates. This can have serious consequences for both the victim themselves and other connected customers. Against this background, each public CSP should undertake suitable measures to defend against DDoS attacks. Owing to the fact that many CSPs can scarcely protect themselves against DDoS attacks using high data rates, the option exists to buy these mitigation services from larger Internet service providers (ISPs) and regulate their use in agreements. Measures should also be implemented to detect internal DDoS attacks by cloud customers on other cloud customers.

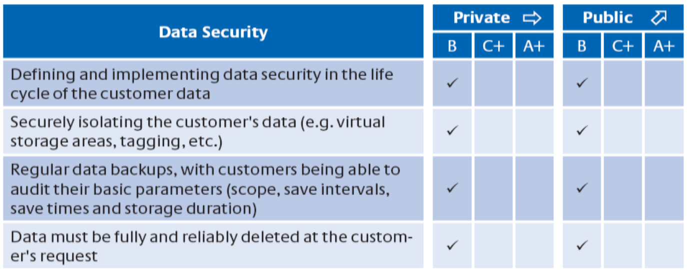
The incorrect configuring of a system is frequently the reason for successful attacks. As Cloud Computing platforms consist of many different components.

E. Virtual machine security: In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

E. Data security: The data life cycle comprises its generation, data storage, data usage, data distribution and data destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms. A number of storage technologies, e.g. NAS, SAN, Object Storage, etc., are used to store data. Common to all these storage technologies is the fact that many customers share a common data storage. In this type of constellation, a secure separation of customer data is essential and should, therefore, be guaranteed. With SaaS, for example, customer data is usually stored in a common table. The distinction between customers is then achieved using a so-called tenant ID. If the web application (shared application) is insecurely programmed, a customer could possibly use an SQL injection to gain unauthorized access to another customer's data, and delete or manipulate it. To prevent this, appropriate security measures must be implemented.

As with traditional IT, in Cloud Computing data losses are a threat that must be taken seriously. To avoid data losses, each CSP should do regular data backups based on a data security plan. Technical defects, incorrect parameterization, obsolescent media, inadequate data media administration and non-compliance with regulations stipulated in a data security plan can result in an inability to reinstall backups and reconstruct the data inventory. So there is a need to sporadically check whether the data backups created to restore lost data can be re-used. Depending on the length of time between backing up the data and restoring the data due to data loss or some other incident, the most recent data modifications may be lost. So a CSP should immediately notify its customers if data backups need to be restored, and in particular indicate the status of the backup. The backing up of data (scope, save intervals, save times, storage duration, etc.) should be transparent and auditable for the customers. It may also be useful to the customer if cloud providers provide them with the option of backing up data themselves.

Because of the underlying multi-tenant architecture, customer data can often only be deleted permanently – i.e. fully and reliably – at the request of a service consumer, for example when a contractual relationship ends, after a certain period of time. The SLAs should make this period clear. When the specified time-scale has elapsed, all the customer data must then be fully and reliably deleted from each storage media. To delete data selectively, care must be taken to delete not only the current version but all previous versions, including temporary files and file fragments. Therefore all CSPs should have an effective procedure for securely deleting or destroying data and data media. Customers should ensure that their agreement specifies at which time and in which manner the CSP must completely delete or destroy their data or data media.



Data Security	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Defining and implementing data security in the life cycle of the customer data	✓			✓		
Securely isolating the customer's data (e.g. virtual storage areas, tagging, etc.)	✓			✓		
Regular data backups, with customers being able to audit their basic parameters (scope, save intervals, save times and storage duration)	✓			✓		
Data must be fully and reliably deleted at the customer's request	✓			✓		

F. Data Security Model [18]: Data model of cloud computing can be described in math as follows:

Df = C(NameNode); …………………(1)

Kf = f * Df; ……………..(2)

C (.): the visit of nodes;

D f : the distributed matrix of file f ;

K f : the state of data distribution in data nodes;

f :file, file *f* can be described as:

f ={F(1),F(2),…..F(n)}; means *f* is the set of n file blocks。 F(i) ∩ F(j)=Ø ,i ≠ j;I,j ∈ 1,2,3,...*n* ;

D_f is a Zero-One matrix, it is L*L, L is the number of datanode.

To enhance the data security of cloud computing, we provide a Cloud Computing Data Security Mode called C2DSM.It can be described as follows:

$D'_f = C\,A$ (namenode) ………………… (3)

D_f =M. D'_f ………………………………….(4)

$K_f = E(f)\,D_f$……………………………… (5)

C_A (.): authentic visit to namenode:

D'f : private protect model of file distributed matrix;

M: resolve private matrix;

E(f): encrypted file *f* block by block, get the encrypted file vector; This model can be show by Figure 3.

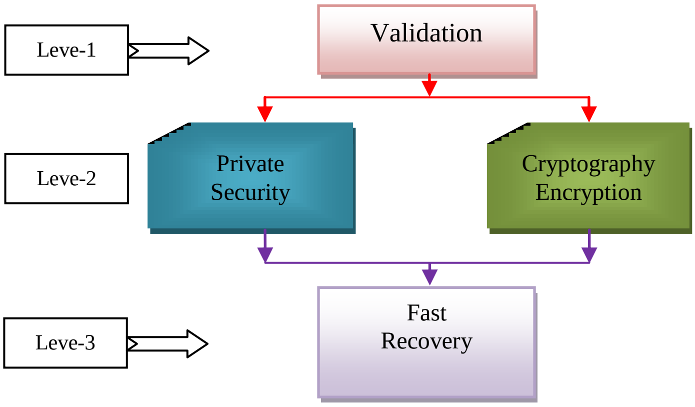


Figure:3 Data Security Model

The model used three-level defense system structure, in which each floor performs its own duty to ensure that the data security of cloud layers. The first layer: responsible for user authentication, the user of digital certificates issued by the appropriate, manage user permissions; the second layer: responsible for user's data encryption, and protect the privacy of users through a certain way;

The third layer: The user data for fast recovery, system protection is the last layer of user data.

With three-level structure, user authentication is used to ensure that data is not tampered. The user authenticated can manage the data by operations: Add, modify, delete and so on. If the user authentication system is deceived by illegal means, and malign user enters the system, file encryption and privacy protection can provide this level of defense. In this layer user data is encrypted, even if the key was the illegally accessed, through privacy protection, malign user will still be not unable to obtain effective access to information, which is very important to protect business users' trade secrets in cloud computing environment. Finally, the rapid restoration of files layer, through fast recovery algorithm, makes user data be able to get the maximum recovery even in case of damage.

From the model there will be follow theorems:

Theory one: If *f D* is not a full order, then the user lost his data.

Verify:

D_f if the file distribution matrix, so with the formula (5), K_f is the L length vector.

If D_f is not full order, D_f can be convert to

D^*_f , D^*_f is (L-i)*(L-i) matrix, i ≥ 1;

K_f become L-I length vector, that make confliction to the definition of the model.

Theory two: if $\sum_{i=i}^{n} K_f\ (i) < n,$ then the data of the user is damaged. K_f *(i) m*eans the value of position i of file vector *f K*

Verify:

$\sum_{i=i}^{n} K_f\ (i)$ means the number of store data in datanode, with definition *f* ={F(1),F(2),…..F(n)},if F(i) not existence, i=1, 2….n, then the file store failure.

If $\sum_{i=i}^{n} K_f\ (i)$ <n, then there will be i=1,2….n, let $K_f(i)$ =0,F(i) not existence in *f* ,the file is damaged. Theory three: if there existed matrix J,J ≠ M, but $D_f = J.\ D'_f$, the private of user leak.

Verify:

M is the user's private matrix. With the matrix M we can get D_f .if *J* existed then illegal user may get

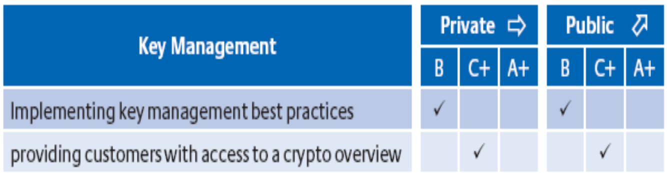
D_f by *J*. There is existence of private leakence.

G. Encryption and key management: To be able to store, process and transport sensitive data securely, suitable cryptographic methods and products should be used. The management of cryptographic keys in Cloud Computing environments is complex, and there are currently no appropriate tools for key management. For this reason, most providers do not encrypt data categorized as 'at rest'. With "IaaS storage" offerings, however, the customer has the option of encrypting their data themselves prior to storage. In this way, they retain complete control over the cryptographic keys and also obviously need to deal with key management. If the provider encrypts the data, suitable security measures should be implemented at each phase in a cryptographic key's life cycle to ensure that keys are generated, stored, shared, used and destroyed on the basis of confidentiality, integrity and authenticity. As highly complex factors need to be considered when using cryptographic methods, each CSP should draw up a cryptography strategy. If customers are to know which tasks the CSP is taking on with respect to cryptography, and which issues they themselves need to consider, it is a good idea if providers provide customers with an overview of the cryptographic mechanisms and methods used.

The following key management best practices should be implemented:

- Keys should be generated in a secure environment and using suitable key generators.
- Where possible, cryptographic keys should be used for one purpose only.
- In general, keys should never be stored in the system in a clear form, but always encrypted. Furthermore, the storage should always be redundantly backed up and restorable, to avoid losing a key.
- The keys must be distributed securely (on the basis of confidentiality, integrity and authenticity).
- The cloud's administrators should have no access to customers' keys.
- Keys should be changed regularly. The keys used should be regularly checked to ensure they are current.
- Access to key management functions should require a separate authentication.
- The keys should be archived securely.
- Keys that are no longer required (e.g. keys whose validity duration has elapsed) should be deleted or destroyed in a secure manner.

Adequate cryptography skills are required for reliable key management. For this reason, CSP personnel who are responsible for key management must be identified and trained.



Key Management	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Implementing key management best practices	✓			✓		
providing customers with access to a crypto overview		✓			✓	

VIII. Conclusion

Although Cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However one must be very careful to understand the limitations and security risks posed in utilizing these technologies. Cloud computing is no exception.

In this paper we discuss the cloud computing environment with cloud service models as soon as we discuss threats and security challenges. In this paper we totally discuss about the security enhancement in cloud computing. Finally we conclude a cloud computing model for data security.

Reference

[1] Ricardo vilaca, Rui oliveira, "*Clouder : A Flexible Large Scale Decentralized Object Store. Architecture Overview",* Proceeding of WDDDM, 2009.

[2] Michael Miller, *"Cloud Computing-Web Based Application that change the way you collaborate online"*, Publishing of QUE, 2nd print 2009.

[3] Shivlal Mewada, Umesh Kumar Singh and Pradeep Kumar Sharma, *"Security Based Model for Cloud Computing"*, IRACST-International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1, 2011.

[4] Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST, Draft Special Publication 800-144, January 2011 http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800 144_cloudcomputing.pdf

[5] ENISA, Cloud Computing: Benefits, Risks and Recommendations for information Security, November 2009 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment/at_download/fullReport

[6] 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)

[7] S. Subashini, and V. Kavitha. (2010) "Asurvey on security issues in service delivery models of cloud computing." J Network Computer Application doi:10.1016/j.jnca.2010.07.006. Jul., 2010.

[8] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009.

[9] R. Woolley and D. Fletcher "The Hybrid Cloud: Bringing Cloud-Based IT Services to State Government October 4, 2009" Department of Technology Services.

[10] T. kraska "Building Database Applications in the Cloud" Swiss federal institute of technology Zurich 2010

[11] Global Netoptex Incorporated , 2009, Demystifying the cloud. Important opportunities, crucial choices, http://www.gni.com , pp 4-14, viewed 13 December 2009.

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

[13] ISO. ISO 7498-2:1989. Information processing systems- Open Systems Interconnection. ISO 7498-2

[14] Dlamini M T, Eloff M M and Eloff J H P, 'Internet of People, Things and Services – The Convergence of Security, Trust and Privacy', 2009.

[15] 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.

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

[17] Worldwide Infrastructure Security Report, Arbor networks, 2010 http://www.arbornetworks.com/dmdocuments/ISR2010_EN.pdf

[18] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, "Data Security Model for Cloud Computing" Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22, 2009 (ACADEMY PUBLISHER AP-PROC-CS-09CN004)