*Journal of Advanced Computer Science and Technology*, 2 (1) (2013) 38-43
©Science Publishing Corporation
www.sciencepubco.com/index.php/JACST

# Securing and managing the data with efficient architecture in cloud computing environment

**L. Kartheesan[1] , S. K. Srivatsa[2]**

[1]*Research Scholar SCSVMV University Kanchipuram, Tamil Nadu, India*
[2]*Professor (Rtd), Anna University, Chennai, Tamil Nadu, India*
**Corresponding author E-mail: karthee.cse@gmail.com*

**Abstract**

Cloud computing technology and services has become an important issue in the recent years. Cloud Computing needs lot of attention, time and innovative concepts for the technology to mature over a period of time. Many organizations show interest in adopting cloud computing technology and services because of its socio economic and time factor.
Cloud computing is nothing but virtual centralization of different computers where the software and memory space is provided by the vendor and the data is managed by them. This leaves the client/customer unaware of where the process is running or where the data is stored. Security of the data is highly dependent on the vendor who has to provide an assurance to the customer on security issues by making service level agreements. This paper focus on security issues, requirements for providing a secured data in cloud computing environment by giving a standard service oriented cloud computing Architecture and management tools that can be used by the organizations for authentication, confidentiality and integrity. Thus providing secured data access and transfer.

***Keywords***: *Cloud Computing, Data Security, Cloud Infrastructure, Data Management.*

## 1 Introduction

Cloud computing is a computing model in which virtualized resources are provided as a services through the Internet. It incorporates various recent technologies that have the common theme of reliance on the internet for satisfying the computing needs of the user. Cloud Computing services usually provide a common business applications online that can be accessed through web browser on user side. Customer engaged on cloud does not own the physical infrastructure that host the software service. Instead they rent usage from third party providers. They consume resource as service, paying for only the resource they use or on subscription basis sharing of resource among multiple customers can reduce cost and also eliminate the need to install and run the application on the customer's computer thus alleviating the burden of software maintenance and support all operations with ease.
Cloud Computing Technology and services is now witnessing a lot of attention now. Cloud has started evolving everywhere since it cuts the capital and operational cost. [1] Cloud computing involves delivering hosted services through the Internet. Cloud computing is made up of elements: client, the data center and distributed server as shown in fig. -1 These elements have a purpose and play a specific role in delivering a functional cloud based applications.

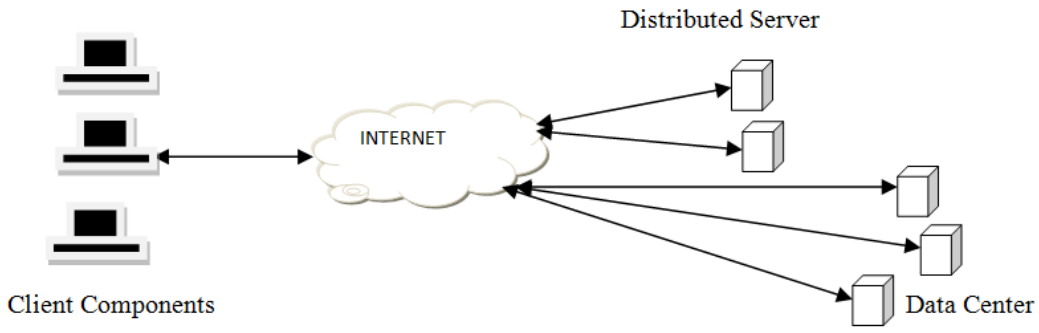


Fig. 1: Cloud computing infrastructure

Cloud computing is a complex infrastructure of software, hardware processing and storage that is available as service. It offers immediate access to large number of the world's most sophisticated super computers and their corresponding processing power interconnected at various locations around the world. Cloud computing moves the application software and database to the large data centers where the management of data and services may not be trustworthy [2] this has given opportunity for many new challenges.
Organizations use cloud computing as a service infrastructure, critically like to examine the security and confidentiality issues for their business applications [6] the clouds have different architecture based on the services they provide. The data processing is done somewhere on the servers so the client have to trust the providers on the availability as well as data security. This paper discuss about providing security to the data which may be located in the data centers and moved for processing where the client is unaware of we focus on providing security for data by forming a better policy and providing a good architecture for specific applications.

## 1.2 Cloud services

Cloud involves in delivering hosted services through the internet. As this internet is a public platform for transmission of data, security is always a threat. These services are broadly classified as

### 1.2.1 Software-as-a-Service

Its origin in the Application Service Provider (ASP) model has emerged in the late 1990s as an alternative to the traditional on-premise enterprise software implementation approach. While the idea of software service is not new, recent studies indicate a significant increase in the adoption of SASS[7]. The adoption of SaaS was initially driven by the need to reduce the cost of software ownership, but there are indications that the benefits of SaaS go well beyond Cost-effective software delivery, enabling organizations to transform their business processes [9].some of the successful SaaS applications are Salesforce.com CRM applications[10]

### 1.2.2 Infrastructure-as-a Service

Cloud computing involve in making computing, data storage and software services available via Internet , transforming the internet into a vast computing platform and running a software on it. One of the most prevalent is Amazon Elastic Compute Cloud (EC2). Another player in the field is Go Grid which is the service provider of windows and Linux cloud-based server hosting.

### 1.2.3 Platform-as- service

It is a way to build applications and have them hosted by the cloud provider. It allows you to deploy application without having to spend the money to buy the servers. Google app Engine offers services that include authentication, authorization, data persistence and task scheduling. The inclusion of App Engine and Google web Toolkit within the plug-in makes it possible for developers to create advanced user interface as well as backend services using the java programming Language.

# 2 Related work

The cloud has a different architecture based on the services they provide. The data is stored on a centralized location called data center having large size of date storage [6]. The data processed is somewhere on the server There are several ways the cloud Infrastructure can be deployed. The Infrastructure depends on the application and how the provider has chosen to build the cloud solution. The client has to trust the provider on the availability as well as data security. Large volume of data is stored in the computer. Managing these data and need of resource Security is the main concern when it comes to cloud computing. When cloud computing is adopted the enterprise has a challenging task of data privacy and security it is needed for the organization to incorporate new techniques like Service Oriented Architecture (SOA) Metering Tools and Technologies [5]. In service oriented architecture environment end-user request an IT service at the desired functional, quality and capacity level and receive it either at the time requested or at a specified later time. Service discovery, brokering and reliability are important and services are usually designed to inter-operate as are the composites made of this service [8]

### 2.1 Security issues.

To get the full benefit of Cloud Computing Security threats has to be dealt carefully some of the security concerns are [3]

- With the cloud model physical security is lost because of sharing computing resources with other companies. No knowledge of where the resource in running
- Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides t move from one to the other
- Ensuring the integrity of data really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not exist.
- The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure audibility of records.

### 2.2 Security standards.

To secure the data, Data management framework this covers the collection, Storage maintenance and dissemination of data and a policy to be created for data management policy and standards. An important measure of security often overlooked by companies is how much downtime a cloud service provider experiences. Ask to see service providers' reliability reports to determine whether these meet the requirements of the business. Exception monitoring systems is another important area. An important consideration for cloud service customers, especially those responsible for highly sensitive data, is to find out about the hosting company used by the provider and if possible seek an independent audit of their security status. The policy and standards should focus on

- A clear framework which define accountability, responsibility, security and user privileges
- High quality data to be managed that results in cost saving and improve business agility
- Appropriate usage of data is important and that the policy and architecture should focus on it.

## 3 Proposed work

To design the architecture for specific application, first we need to clearly identify the requirements for this we need to clearly identify the requirements. Generally clouds have single security architecture but have many customers with different demands. So question ere to be prepared and answers to be sought. Based on the answer the architecture can be designed.

- Where the resource is going to run and list of companies sharing the resources
- Had companies created the policy and law for resource sharing
- Does the storage is transferable from one vendor to another
- Ensure the integrity of the data through security managers and regulators
- Data stored is accessed by the person given access rights by the organizations
- Does a privacy law in various countries allow transferring the some type of personal information to other region or countries?
- Can business application capability is extended to cloud that can directly interface with business

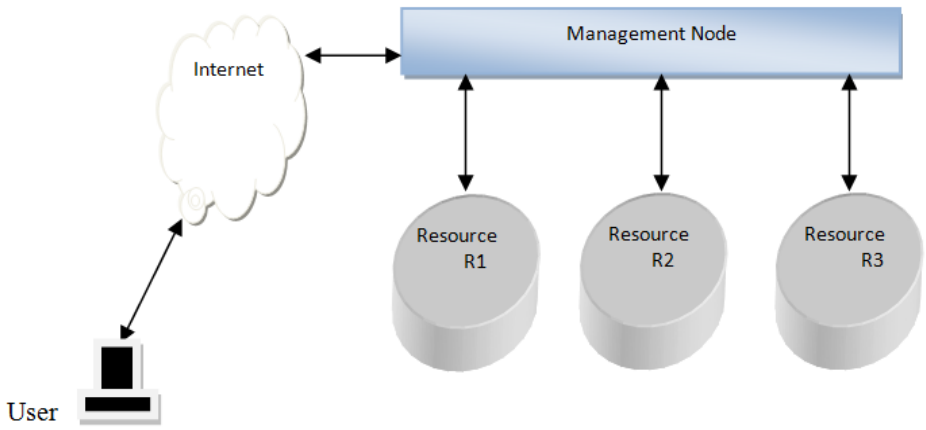


Fig. 2: Proposed Architecture for secure cloud

Securing the data can be done by data into three types: Restricted Data is the most confidential information and therefore requires a high level of protection. These types of data are identified through the policy and the questioner and stored in Reasource1. Sensitive data is the information that requires moderate to high level of security and these types of data are stored in resource 2. General Data are the information which is published or can be made available for public access or to the concern organization is stored in the Resource 3

We use a double authentication for accessing the account. When the user want to log into their account user id password and resource id has to be provided to the management node Data received by the management node is in encrypted form is processed by this node and checked and verified and allows the user to access the type of resource the user requested for.

This can be done by a management node that has complete control of the resources that may be delivered as shown in fig.-2. End user should feel comfortable with a cloud solution that holds their software, data and processes. There exists assurance that services are highly reliable, available and protected.

## 3.1 Providing data confidentiality and authentication

The security scheme consists of RSA Algorithm key exchange mechanism to provide security. The data M is encrypted using the data specific key and the data specific is encrypted with Rkey. Then the sender appends the destination ID and transmits the message to its authenticated management node. The plain text message is obtained if the ID of the resource matches, and it is considered as the intended recipient. The decryption is performed with Rkey of the sender.

Each user in the network has its own symmetric Nkey

Each Resource has its own symmetric key Rkey

To perform encryption and decryption each user must know others Rkey

At source, Nkey is encrypted with Public key(PU) of Resource(R) N and transmitted to the destination. Management node decrypts Nkey with Private (PR) of Resource(R) N

Thus we provide confidentiality to the data and authentication to the user for accessing the data

### 3.1.1 Focused algorithm

User A create a Dkey

The data M is encrypted with Dkey, [EDkey(M)]

Data is encrypted with public key of the Resource n E PU Rn [EDkey(M)]

User encrypted with client Private key A's PRkeyA [EPU Rn [EDkey(M)]]

The Resource ID is appended to the cipher text [PRkeyA [EPU Rn [EDkey(M)]] dest ID]

If the dest ID matches with cipher text decryption is performed D[PRkeyA [EPU Rn [EDkey(M)]] dest ID]

Else

Management node makes alert message and allow only public resource R3 to user.

# 4 Functional specification

From an engineering perspective, cloud computing is architecture characterized by a large number of identical computing devices that can scale on demand and that communicate via an IP network. As long as the provider can deliver these services, how they do it is really immaterial. From the consumer's perspective, the architecture the vendor uses to deliver their services is only significant in terms of the cost reductions that the vendor realized through commodity hardware and software purchases and those they choose to pass along to the consumer. Here we look at the function of the how the data can be securely transferred to the cloud and accessed wherever required.

## 4.1 Client response

Whenever the user want to use the services provided by the service provider, the user enter the user id and password and when he wants to send a new data to be stored in the cloud storage he first answer the questioner the service provider and identify how important his data is and decide where his data is to be stored he gets the public key of the resource through the management node and encrypt using the RSA algorithm the data and send it to the management node. The user enters the key and the data access is provided to the user after authentication is made clear.

### 4.2 Management node

When the management node receives the message it checks for the user and authenticate the user. Thus the authentication is done twice first by checking the user Identification and password then by the RSA algorithm process as shown in the Block diagram Fig-3. If the authentication process check the cryptographic key with the private of resource 1 if yes then it allow the user to access the restricted data form resource1 else the key is passed on to the next resource if it matches the user is allowed to access the sensitive data.

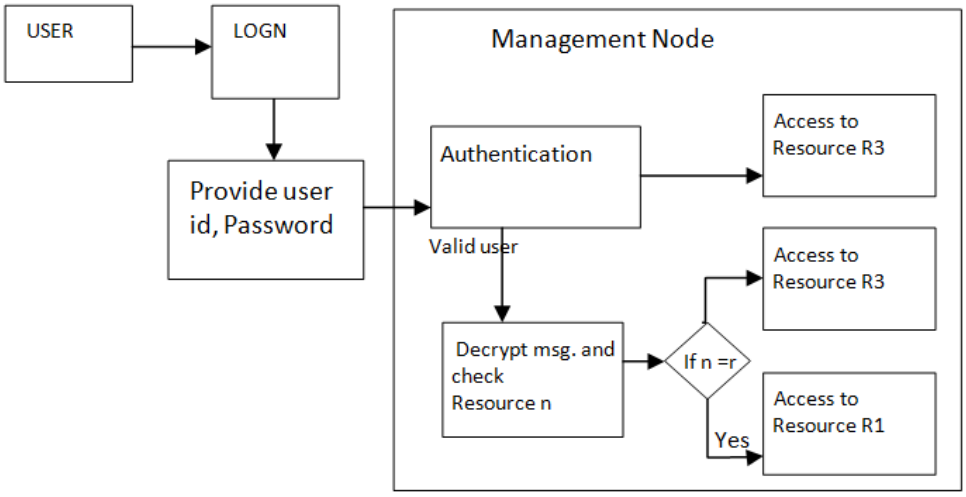


Fig. 3: Block diagram of the proposed System

If the user not the authorized person to access the right data, he will not be able to get through the strong authentication process and the user will be allowed to access the general public data.

## 5 Analysis of proposed scheme

We analyze the security properties of the proposed system and they are as follows

a) Data confidentiality: we use one of the strongest cryptography algorithms such as RSA Algorithm for encryption and decryption of data there by having only the owner is able to access data which provide data confidentiality.

b) Authentication: Authentication is performed with the help of password set by the user during registration. The key with is generated with the help of RSA Algorithm also ensures that the user is authenticated again apart from the user id and password for accessing the data stored in the resource.

c) Integrity: the significant challenge is data integrity. There can be attacker from inside the cloud environment, we can have check over the data integrity because of the segregation of data at different resource and managing integrity is made easier.

## 6 Conclusion

It is very important to consider the security aspects when designing and using cloud services. In this paper, security in cloud is elaborated that covers the security issues, challenges, standards and management models the architectural approach primarily focus on modeling and managing IT resources and do not address situations where infrastructure and applications are sourced externally. The architecture may converge into a single architectural framework in the near future that may help in integration of external and internal services, optimization, management and governance of complex service environment.

# References

[1] CHANG-Lung Tsai Allen Y. Chang Chun –Jung Chen "Information Security Issue of Enterprises Adopting the Application of Cloud Computing" IEEE 2010 645-649
[2] Jian Wnag Yan Zhao Shuo Jiang "Providing Privacy Preserving in Cloud Computing" IEEE 2010 978-1-4244-7562
[3] Kresimir Ppopovic Zeljko Hocenkski "Cloud Computing Security Issues and Challenges " MIPRO 2010 may 24-28
[4] Cloud security Alliance, Security Guidance for critical Areas of Focus in Cloud Computing V2.1 http:// Cloudsecurityalliance.org/ Dec 2009
[5] International data Corporation, Worldwide Security and Vulnerability Management 2009 http://velnerabilitymanagement.com/IDC_MA_2009.pdf
[6] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit "Cloud Security Issues" 2009 IEEE International Conference on Services Computing.
[7] George Feuerlict, Shyam Govardhan "SOA: Trends and Directions" System Integration 2009
[8] Mladen A. Vouk "Cloud Computing- Issues, Research and Implementations" Journal of Computing and Information Technology –CIT 16, 2008 235-246
[9] http// cloud security.org
[10] Tim mather "Cloud security and Privacy" 2009
[11] Jithedra Pal thethi "Realizing the value Proposition of cloud computing" April 2009
[12] The Open group service oriented architecture http:// www. Opengroup.org/ Project/soa