International Journal for Rapid Research in Engineering Technology & Applied Science
ISSN (Online): 2455-4723
Vol 3 Issue 3 March 2017

"Secure Cloud Bursting, Brokerage, Aggregation using AES Encryption and One Time Authentication Password"

1Pooja Keshare, 2 Kapil Sahu
*1 Research Scholar, Sanghvi Institute of Management & Science, Indore, M.P, India
2 Professors, Sanghvi Institute of Management & Science, Indore, M.P, India
*Department of Computer Science & Engineering
*sahukapil@gmail.com***

***Abstract* - Cloud bursting is an application deployment model during which an application runs in the private cloud or data center and bursts into public cloud when the actual demand for computing capacity spikes. The advantage of this type of hybrid cloud deployment is make fish an organization only pays with regard to extra compute resources when they are needed. Some organization create own private cloud are interested in leveraging cloud bursting. Conventionally some architecture has run application workload fully in private cloud till workload is not over the threshold value. After cross the threshold value application burst into public cloud for additional compute resources. In this paper, we proposed bridge between multiple clouds and deal with cost and security issue relating to communication between public and private clouds. We extend Security for Computing Cloud Bursting and Aggregation Applying AES encryption, One Time password. We also used secure sharing mechanism so your cloud resources are distributed among different cloud environment and consider some of the security concern for your cloud computing for authorized data sharing between clouds.**

Keywords: **Cloud Computing, Bursting, Broker, Encryption, OTP, Security**

1. Introduction

1.1 Cloud computing

Cloud computing has emerged as one of the most promising and challenging technologies of our time. Some of the properties that characterize the cloud computing service delivery model are scalability/elasticity, on-demand service provisioning, shared resource pooling, multi-tenancy hosting, utility pay-as-you-use pricing and abstraction of lower layers [1].Cloud computing refers to the delivery of computing resources over the Internet. Rather than storing data on your own hard drive or updating applications for your needs, we use a service over the Internet, we can store, manage and process data rather than local server or personal computer.Doing so may give rise to certain privacy implications [2]. We can access information and computer resources from anywhere if network connection is available. Cloud computing provides a shared pool of computing resources, that is data storage space, networks, processing power, and user applications.

Cloud services allow individuals and businesses to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. [2]

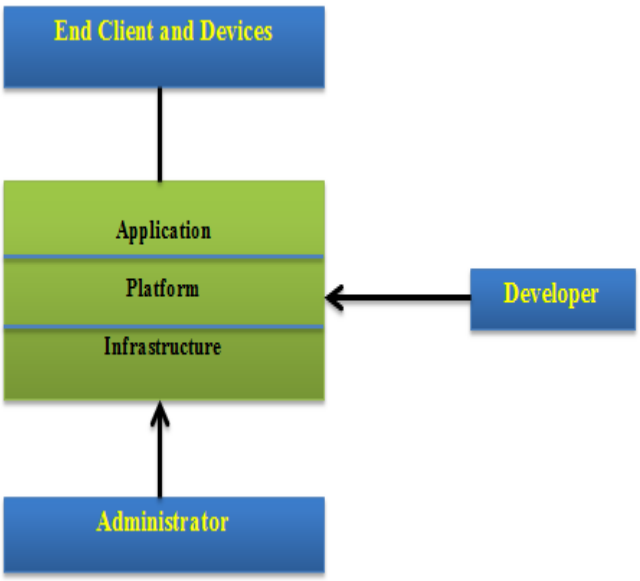

Figure 1 Cloud Computing Overview

Cloud computing refer to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and we need not to install a piece of software on our local PC and this is how the cloud computing overcomes platform dependency issues. [2]

1.2 Cloud Services

A cloud service is any resource that is provided over the Internet. The most common cloud service resources are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [3].

1.2.1 Software as a Service (SaaS):- Software as a Service (SaaS) 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.

1.2.2 Platform as a Servies (PaaS):- Platform as a service (PaaS) is a cloud computing model that delivers applications over the Internet. In a PaaS model, a cloud provider delivers hardware and software tools -- usually those needed for application development -- to its users as a service. A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.

1.2.3 Infrastructure as a Service (IaaS):- Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. IaaS is one of three main categories of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS).

1.3 Cloud Brokerage:

Cloud service brokerage provides the intermediary between cloud providers and cloud consumer that choosing the services from different-different provider and offerings that to consumer which best suits their needs. They may also assist in the deployment and integration of apps across multiple clouds or provide a choice and possible cost saving function which includes multiple competing services from a catalog [4].

1.3.1 Broker Functions/Capabilities

Cloud Service Intermediation: An intermediation broker provides value added services on top of existing cloud platforms, such as identity or access management capabilities [5].

Aggregation: An aggregation broker provides the "glue" to bring together multiple services and ensure the interoperability and security of data between systems.

Cloud Service Arbitrage: A cloud service arbitrage provides flexibility and "opportunistic choices" by offering multiple similar services to select from.

1.4 Costing & Charging Model:

First of all we need to make sure you understand some basics so in simple terms [6]:
Cost **–** How much your finance department pay to produce a pathology result.
Price **–** How much your customers will be charged for the result.
Profit or Loss **–** The difference between Cost and Price

Costing can be defined as the process of determining how much it costs to produce and sell a product or service. Costing is very important as the cost of a product can decide its profit or loss. There are two costs involved in determining the cost of a product / service, i.e. direct cost and indirect cost [7].

- **Direct Cost:** The cost of those items that become part of the end-product are known as direct costs such as; raw material, labour, packing material, etc.
- **Indirect Cost:** All expenses incurred in running a business and that which cannot be directly identified with the end product are indirect costs.

1.5 Security Issues

1.5.1 Data Security: Security refers to confidentiality, integrity and availability, which pose a major issue for cloud provider. Confidentiality refers to who stores the encryption keys data from company A, stored in an encrypted format at company B must be kept secure from employees of B, thus the client company should own the encryption keys. Integrity refers that no common policies exist for approved data exchanges.
1.5.2 Data Recovery: Even if we don't know where your data is, a cloud provider should tell us what will happen to our data and service in case of a disaster.
1.5.3 Privileged User: When sensitive data processed, then we face inherent level of risk, because outsourced services bypass the physical, logical and personnel controls IT shops exert over in-house programs.
1.5.4 Regulatory Compliance: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications.
1.5.5 Data Location: When users use the cloud, they probably won't know exactly where their data will be hosted. In fact, even customers not know what country it will be stored in. Service providers need to be asked to customer if they will commit to storing and processing data in specific jurisdictions,

and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers [8].

- In the cloud, data and services are not restricted within a single organization's perimeter. This dynamism and fluidity of data introduces more risk and complicates the problem of access control. Therefore, compared with the traditional models, in cloud computing model ensuring confidentiality and integrity of the end-users' data is far more challenging.
- Users with confidential data are fear of insecurity, even the service providers are not confidently sure of the data security despite the encryption used.
- Where data security measures are implemented by cloud providers, users are not sufficiently assured sole ownership of control of their useful, confidential or classified sensitive data.

2. Background

2.1 Cryptography Cloud

Cryptography is methods of transforming an intelligible message into one that is unintelligible form, and then retransforming that message back to its original form. "In the cloud, we don't have the physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key."Cloud computing provides clients with a virtual computing infrastructure on top of which they can store data and run applications. While the benefits of cloud computing are clear, it introduces new security challenges since cloud operators are expected to manipulate client data without necessarily being fully trusted. We are designing cryptographic primitives and protocols tailored to the setting of cloud computing, attempting to strike a balance between security, efficiency and functionality [9].

The current generation of cloud computing infrastructures does not provide any security against untrusted cloud operators making them unsuitable for storing sensitive information such as medical records, financial records or high impact business data [9].

2.2 Cryptography & Security

Cloud computing offers a new way of services by re-arranging various resources and providing them to users based on their demands. It also plays an important role in the next generation services. Storing data in the cloud greatly reduces storage burden of users and brings them access convenience, thus it has become one of the most important cloud services. However, cloud data security, privacy and trust become a crucial issue that impacts the success of cloud computing. Cloud data storage increases the risk of data leakage and unauthorized access. Cloud data management cannot be fully trusted by data owners. Cloud data process and computation could disclose the privacy of data owners or to unauthorized parities. For overcoming the above problems, cryptography has been widely applied to ensure data security, privacy and trust in cloud computing, but existing solutions are still imperfect. Computation efficiency, key management, verifiable data computing is key challenges. Cryptography in cloud computing promises many novel solutions but at the same time, many challenges are yet to be overcome [10].

Topics of interest include, but are not limited to [10]:

- Cryptography for cloud data trust management
- Cryptography for cloud data access control
- Cryptography for privacy preserving data analytics and mining
- Cryptography for auditing on cloud data management
- Cryptography for verifiable computing
- Cryptography for cloud data authentication and authorization
- Cryptography for secure cloud data storage and reduplication
- Cryptography for secure and privacy enhanced cloud data search and query
- Cryptography for data security and privacy

2.3 Type of Cryptography [11]

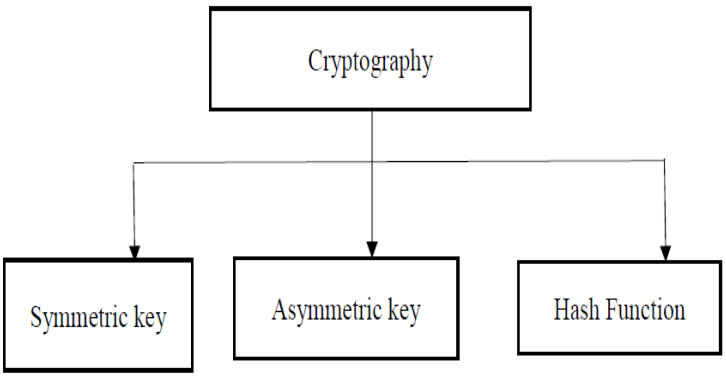

Figure 2Types of Cryptography

2.3.1 Symmetric Key Cryptography

- Same Key is used by both parties

- Simpler and Faster

2.3.2 Asymmetric Key Cryptography: two different keys are used users get the Key from:

Certificate Authority:

Authentication in asymmetric cryptography is more secured but the process is relatively more complex as the certificate has to be obtained from certification authority.

Hash Function

- Uses mathematical transformation to irreversibly encrypt information
- It is a one-way encryption
- Uses no key for encryption and decryption

3. Literature Survey

Publication & Year	Paper Title	Advantages	Limitations
2013	Towards Secure Cloud Bursting, Brokerage and Aggregation	1. Secure cloud data from unauthorized access.	
2013	Cloud Security for Computing Secure Cloud Bursting, Brokerage and Aggregation Using Cryptography	1.Cloud Security for Computing Secure Cloud Bursting and Aggregation Using encryption and One Time password method. 2.Used secure sharing mechanism shared among different cloud environment.	
2015	Towards A Cryptographically-Secure Cloud Security Solution	1. Protecting the cloud data from unauthorized access. 2. Effectively hide meaningful user data from all external parties - even from the service provider.	
2013	An Approach towards Security in Private Cloud Using OTP	1. Use of Dynamic one time password with two factor authentication as a strong authentication technique.	

4. Proposed System

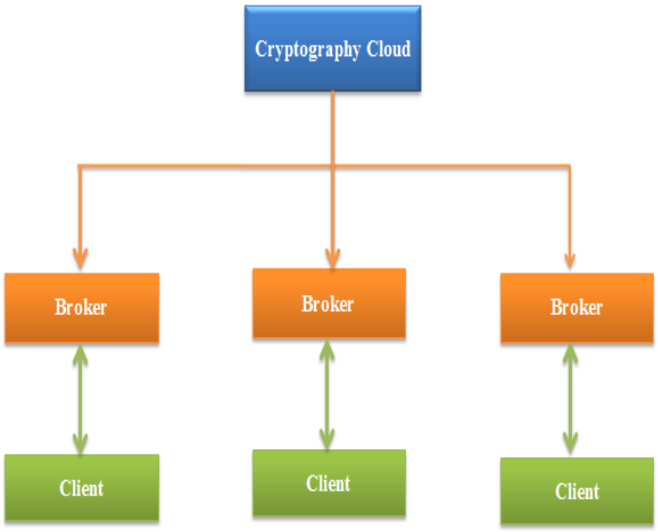

Figure Cryptography Cloud

Many types of cloud computing service providers are required to provide management services. The cloud provider has to make sure that it has a well-designed management infrastructure so that all of its services operate efficiently and safely.

The provider wants to sure that each customer's data is well protected and supported from intruder, attacker,and malicious programs. When the provider has done a good job, you may be unaware of it. For distribution of service there are two ways –

1. Directly to the client
2. by the broker

A Cloud Service Broker aggregates and integrates services and managed services from different –different providers based on client requirement. The broker's role may simply be to save the customer time by researching services from different vendors and providing the information about how to use cloud computing to support business goals [13].

We need a trust to manage a client trust between broker and service provider. That's why we compute a trust on opinion basis.

Figure 4 Virtualization of Cloud

Stakeholder Role

Fig. 4 shows the conceptual model of VCB and its relationship with stakeholders. It consists of four parts, each associated with a distinct role: tenant, provider, administrator, and customizer. Each role is defined by its business relationship with VCB. The stakeholders associated with these roles are explained in detail as follows:

1) Tenant: a VCB user who finds and uses cloud services. The tenant can be a person, organization, community, or anyone who wants to use a cloud service.

2) Provider: a person or corporation that provides one or more services for tenants. Providers make services and register their specifications with VCB.

3) Administrator: a person who manages and helps adapt VCB. When an administrator receives a management and error report from VCB, he/she may take a variety of actions including policy modification.

4) Customizer: a person or corporation who compounds several services. If a tenant is not satisfied with the suggested services from the VCB, the tenant can request to make combined or upgraded service. This requirement is delivered to the customizer via VCB. The customizer then creates a new service that meets the tenant's requirements. This sequence is called cloud service aggregation.

Following step we performed in out proposed System:

We extend Security for Computing Cloud Bursting and Aggregation Applying AES encryption, One Time password and Token exchange method. We also used secure sharing mechanism so your cloud resources are distributed among different cloud environment and consider some of the security concern for your cloud computing for authorized data sharing between confuses which would help cloud users maintain control of their meaningful, confidential and sensitive data (at rest or in transit within the cloud networks) rather than outsource to external vendors as usual.

The system if implemented or algorithm adopted, would improve the existing state of data privacy, and security of cloud data and application environment as it would effectively hide meaningful user data from all external parties to a virtual network- even from the service provider.

5. Conclusion

Cloud computing provide a benefits for organizations and individuals. There are secure cloud algorithm which service providers, organizations or consumers could implement as a cryptographically- secure SaaS or PaaS cloud when outsourcing meaningful data, applications, and infrastructure to a virtualized cloud environment. The security of the cloud infrastructure entails protecting the cloud data from any unauthorized access or intrusion by malicious users. Therefore, the research aim of designing a cryptographically secure cloud apps solution which would effectively hide meaningful user data from all external parties to a virtual network- even from the service provider have been achieved. The system if deployed or algorithm adopted promises to improve the existing state of data privacy, and security of cloud data and application environment.

REFERENCE

[1] Srijith K. Nair, "Towards Secure Cloud Bursting, Brokerage and Aggregation",BT Innovate and Design European Conference on Web Services, 2013.
[2] Introduction to Cloud computing, available online http://www.aftab-mp.com/new-technologies/introduction-cloud-computing".
[3] Cloud services, Available Online at: http://searchcloudprovider.techtarget.com/definition/cloud-services.
[4] Solutions: Cloud Service Brokeragehttps://www.computenext.com/cloud-service-brokerage/.
[5] Cloud Services Brokerage Company List and FAQ http://talkincloud.com/cloud-services-broker/cloud-services-brokerage-company-list-and-faq
[6] "Standard Costing Model", available Online at: http://www.atebit.co.uk/id20.html
[7] Costing and Pricing of Products.
[8] Pradeep Kumar Tripathi, Surendra Mishra and Pankaj Kawadkar, "Cloud Aggregation and Bursting for Object based Sharable Environment", International Journal of Advanced Computer Research, Volume 1, PP. 86-90, 2011.
[9] Cloud Security & Cryptography, available Online: http://research.microsoft.com/enus/projects/cryptocloud/.
[10] Special Issue on Cryptography and Data Security in Cloud computing available online: http://www.journals.elsevier.com/information-sciences/call-for-papers/special-issue-on-cryptography-and-data-security-in-cloud-com.
[11] Types of Cryptography,http://haktuts.com/What-are-the-types-of-Cryptography/.
[12] Judith Hurwitz, Robin Bloor and Marcia Kaufman, "How to Work with a Service Provider in Cloud Computing**",** The Essentials of Services in Cloud Computing, available Online, http://www.dummies.com/how-to/content/how-to-work-with-a-service-provider-in-cloud-compu.html.
[13] Building a cloud service brokerage business http://www.gravitant.com/roles/cloud-brokerage-for-solution-providers/.