Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 9, September 2013, pg.24 – 28

RESEARCH ARTICLE

Cloud Security for Computing Secure Cloud Bursting, Brokerage and Aggregation Using Cryptography

Neeraj Shrivastava[1]
neeraj0209@gmail.com

Rahul Yadav[2]
rahul.yadav024@gmail.com

IES, IPS Academy Indore, MP, INDIA

ABSTRACT:

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood [1]. Many schemes are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and retrieve-ability of data, etc. In my work, I encrypt data by using 64 bit block cipher Method for Computing Secure Cloud (*DaaS*) bursting and Aggregation. It provides better security to other security schemes because it uses OTP (One Time Password) to access the facilities of cloud computing each time.

Keyword: OTP, Aggregation, Bursting, encryption, DaaS

1. INTRODUCTION

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. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models [6].

Essential Characteristics:

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

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Resource pooling: The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

2. CLOUD COMPUTING MODELS

Service Models:

Software as a Service (SaaS): The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

*Infrastructure as a Service (IaaS): T*he capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Network as a service (NaaS): a category of cloud services where the capability provided to the cloud service user is to use network/transport connectivity services and/or inter-cloud network connectivity services. NaaS involves the optimization of resource allocations by considering network and computing resources as a unified whole. Traditional NaaS services include flexible and extended VPN, and bandwidth on demand.

Data as a Service (DaaS): a category of cloud services where a service provider that enables data files (including text, images, sounds, and videos) are made available to customers over a network, typically the Internet regardless of their geographic location. Data services can eliminate redundancy and streamline costs by housing critical data in one location, enabling the data to be accessed and/or updated by multiple users while ensuring a single point for updates.

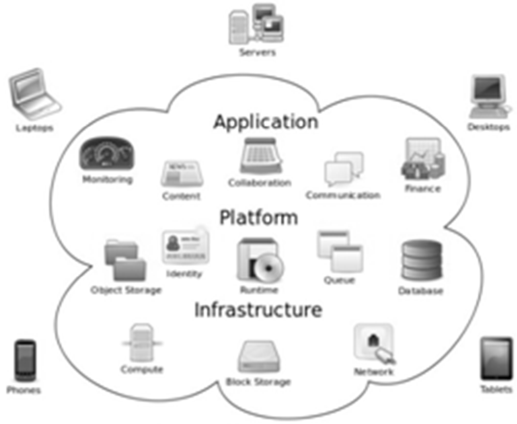


Figure 1: Cloud Computing

Deployment Models:

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

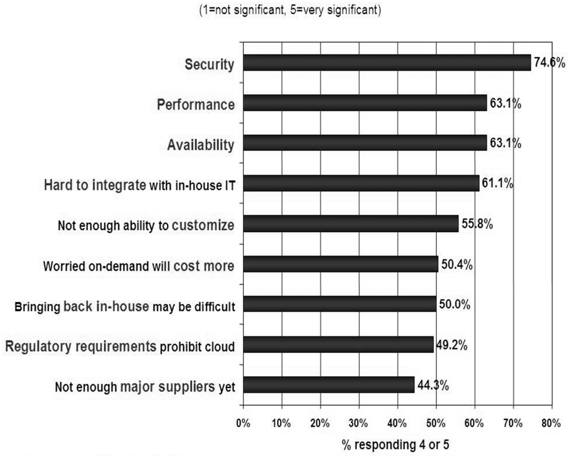
Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

3. SECURITY ISSUES

Many survey say that the prime issue of cloud computing is security: in every model of cloud we need different type of security



Source: IDC Enterprise Panel, n=244

Figure 2: Rate challenges/issues of cloud computing

Organizations use cloud computing as a service infrastructure; critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the "cloud" is difficult, if not impossible, as they provide different services like Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Each service has their own security issues[1].

Data security: Security refers to confidentiality, integrity and availability, which pose a major issue for cloud vendors. 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

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.

Privileged user: access Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the physical, logical and personnel controls IT shops exert over in-house programs.

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. Cloud computing providers who refuse to undergo this scrutiny are signaling that customers can only use them for the most trivial functions [2].

Data location: When users use the cloud, they probably won't know exactly where their data will be hosted. In fact, they might not even know what country it will be stored in. Service providers need to be asked 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 [9].

4. PROPOSED WORK

In this paper we proposed an approach for Cloud Security for Computing Secure Cloud Bursting and Aggregation Using Cryptography for multi cloud environment through Class and Object. In this approach we mainly concentrate on some phases:

I. Cloud1(C++ Cloud)
II. Cloud2(Java Cloud)
III. Cloud3(C# Cloud)
IV. Shared Cloud with Encrypted Data
V One Time Password

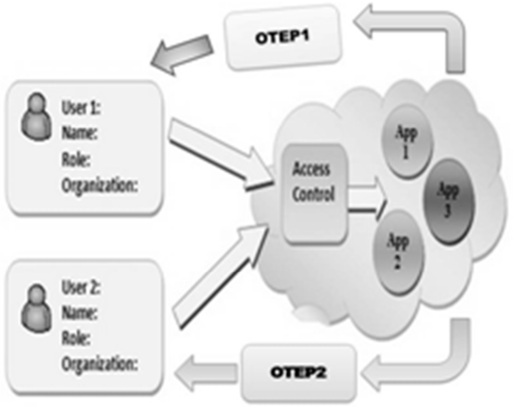


Figure3: Cloud Access Environment

Phase I: In First phase our method the environment for cloud1 where we perform aggregation and bursting on C++ files. We calculate several object oriented properties like class and object and according to those values we perform aggregation and bursting.

Phase II: In Second phase our method opens the environment for cloud2 where we perform aggregation and bursting on Java files. We calculate several object oriented properties like class and object and according to those values we perform aggregation and bursting.

Phase III: In Third phase our method opens the environment for cloud3 where we perform aggregation and bursting on C# files. We calculate several object oriented properties like class and object and according to those values we perform aggregation and bursting.

Phase IV: In the fourth phase we encrypt data and establish a connection between user and cloud environment through user id and password which is provided by the cloud environment.

Phase V: In the last phase, when user wants to use any facility in cloud. Cloud generates a One Time Password to use the cloud facility. User decrypts the data by using some encryption/decryption key which is also provided by the cloud environment and then he/she uses the cloud facilities.

5. CONCLUSION

Cloud computing paradigm is still relatively young in terms of maturity and adoption. The expectation is that it will undergo several changes in the future, in terms of resources, issues, risks, and ultimately best practices and standards.

In this paper we proposed an algorithm that is Cloud Security for Computing Secure Cloud Bursting and Aggregation Using encryption and One Time password method. we consider three clouds for bursting and aggregation operation. We also used secure sharing mechanism so that the cloud resources are shared among different cloud environment and consider some of the security concern for the cloud computing for authorized data sharing between clouds. In this approach we mainly concentrate on four phases.

1) Interconnectivity
2) Security
3) Resource Sharing
4) Mapping

In future we can apply this concept in Real environment check for the real time simulations on different Platform.

6. REFERENCES

[1] B.R. Kandukuri, R. Paturi V, and A. Rakshit, “Cloud Security Issues,”2009 IEEE International Conference on Services Computing, Sep. 21-25, 2009, Bangalore, India, pp. 517-520.

[2] G. Hughes, D. Al-Jumeily & A. Hussain,” Supporting Cloud Computing Management through an Object Mapping Declarative Language” , 2010 Developments in E-systems Engineering.

[3] Yunqi Ye, Liangliang Xiao, I-Ling Yen, Farokh Bastani, “Secure, Dependable, and High Performance Cloud Storage”, 2010 29th IEEE International Symposium on Reliable

[4] Campbell, Jeronimo, “Applied Virtualization Technology,” Hillsboro, Intel Press (ISBN 0-9764832-3-8), 2006, pp. 69-73.

[5] Tout, Sverdlik, and Lawver, “Cloud Computing and its Security in Higher Education,” In Proceedings of the Proc ISECON 2009.

[6] Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing,” NIST Special Publication 800-145, Gaithersburg, MD, September 2011, pp. 1-7.

[7] Cloud Security Alliance, “Top Threats to Cloud Computing v1.0,” Prepared by the Cloud Security Alliance, March 2010, pp. 1-14.

[8] Jouni Mäenpää, “Cloud Computing with the Azure Platform,” TKK T-110.5190 Seminar on Internet Working, April 27, 2009.

[9] Feng-Tse Lin, Teng-San Shih, “Cloud Computing: The Emerging Computing Technology,” ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, September 2010, pp. 33-38.

[10] Amazon Web Service, Amazon Elastic Compute Cloud, User Guide, API Version, August 31, 2010.

[11] John Krautheim, “Private Virtual Infrastructure for Cloud Computing,” HotCloud'09 USENIX Association Berkeley, CA, USA, 2009.

[12] Campbell, Jeronimo, “Applied Virtualization Technology,” Hillsboro, Intel Press (ISBN 0-9764832-3-8), 2006, pp. 69-73.

[13] Tout, Sverdlik, and Lawver, “Cloud Computing and its Security in Higher Education,” In Proceedings of the Proc ISECON 2009, v26 (Washington DC): §2314 (refereed), November 6, 2009, pp. 1-5.

[14] Vaquero, Merino and Lindner, “A Break in the Clouds: Towards a Cloud Definition,” ACM

SIGCOMM Computer Communication Review, v.39 n.1, January, 2009, pp. 50-55.

[15] Kandukuri, Paturi, and Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing Bangalore, India, Sep. 21-25, 2009, pp. 517-520.

[16] Vishnu S Pendyala, Joanne Holliday, “Performing Intelligent Mobile Searches in the Cloud Using Semantic Technologies,” 2010 IEEE International Conference on Granular Computing, Aug. 14-16, 2010, pp. 381-386.

[17] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg and Ivona Brandic, “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility,” Future Generation Computer System, 2009, pp. 599-616.

[18] Sun Microsystems, “Introduction to Cloud Computing Architecture,” White paper, 1st Edition, June 2009, pp. 1-40.

[19] Ian Foster, “Cloud, Grid, What's in a Name?” Type pad blog, August 07, 2008.

[20] Information Society and Media, “An EGEE Comparative Study: Grids and Clouds - Evolution or Revolution,” Technical Report Enabling Grids for E-sciencE, v1.1, Jun 11, 2008, pp. 1-33.

[21] Derrick Harris, “Grid vs. Cloud vs. What Really Matters,” HPC in the Cloud on Demand Enterprise Blogs, August 22, 2008.

[22] Yi Hu, Bin Gong, Fengyu Wang, “Cloud Model-Based Security-aware and Fault-Tolerant Job Scheduling for Computing Grid,” 2010 Fifth Annual China Grid Conference, July 16-18, 2010, IEEE, pp. 25-30.

[23] Hai Zhong, Kun Tao, Xuejie Zhang, “An Approach to Optimized Resource Scheduling Algorithm for Open-source Cloud Systems,” 2010 Fifth Annual China Grid Conference (China Grid), July 16-18, 2010, IEEE, pp. 124-129.