Secure Cloud Computing Using Encryption and Decryption Method

Dr. Yashpal singh	Ms. Pritee Gupta	Ms. Mrinalini shringirishi
Reader & Head, IT Deptt.	Assistant Professor, CSE Deptt.	Scholar M.tech Computer Science
B.I.E.T Jhansi (U.P.)	Gr. Noida (U.P.)	College of Science & Engineering, Jhansi (U.P.)
Yash_biet@yhoo.co.in	23march.pritee@gmail.com	shringirishimrinal35@gmail.com

Abstract

Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their services and human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more using one server for 1,000.

Enterprises usually store data in internal storage and install firewalls to protect against intruders to access the data. They also standardize data access procedures to prevent insiders to disclose the information without permission. In cloud computing, the data will be stored in storage provided by service providers. Service providers must have a viable way to protect their clients' data, especially to prevent the data from disclosure by unauthorized insiders. Storing the data in encrypted form is a common method of information privacy protection. If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the system administrators may simultaneously obtain encrypted data and decryption keys.

This allows them to access information without authorization and thus poses a risk to information privacy. This study proposes a business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service.

Furthermore, the party responsible for the data storage system must not store data in plaintext, and the party responsible for data encryption and encryption must delete all data upon the computation on encryption or decryption is complete.

A CRM (Customer Relationship Management) service is described in this paper as an example to illustrate the proposed business model.

Keywords

Cloud computing, data privacy protection, Encryption or decpryption service, data Security.

Introduction of Cloud Computing

Cloud computing is the Internet based development and is used in computer technology. It has become an IT buzzword for the past a few years. Cloud computing has been often used with synonymous terms such as software as a services (SaaS), grid computing, cluster computing, autonomic computing, and utility computing . SaaS is only a special form of services that cloud computing provides. Grid computing and cluster computing are two types of underlying computer technologies for the development of cloud computing. It is often difficult to define the cloud computing.[1]. Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet. It provides a mandatory application programming environment. Fig. 2. It can deploy, allocate or reallocate computing resource dynamically and monitor the usage of resources at all times Cloud computing collects all the computing resources and manages them automatically through software. In the process of data analysis, it integrates the history data and present data to make the collected information more accurate and provide more intelligent service for users and enterprises. The users need not care how to buy servers, software solutions and so on. Users can buy the computing resource through internet according to their own needs[2]. Cloud computing does not depend on special data center, but we can look it as the inevitable product of grid computing and efficiency computing. Cloud computing is easy to extend, and has a simple management style. Cloud is not only simply collecting the computer resource, but also provides a management mechanism and can provide services for millions of users simultaneously. Organizations can provide hardware for clouds internally (internal clouds), or a third party can provide it externally (hosted clouds). A cloud might be restricted to a single organization or group (private clouds), available to the general public over the Internet (public clouds), or shared by multiple groups or organizations (hybrid clouds) in fig 1.

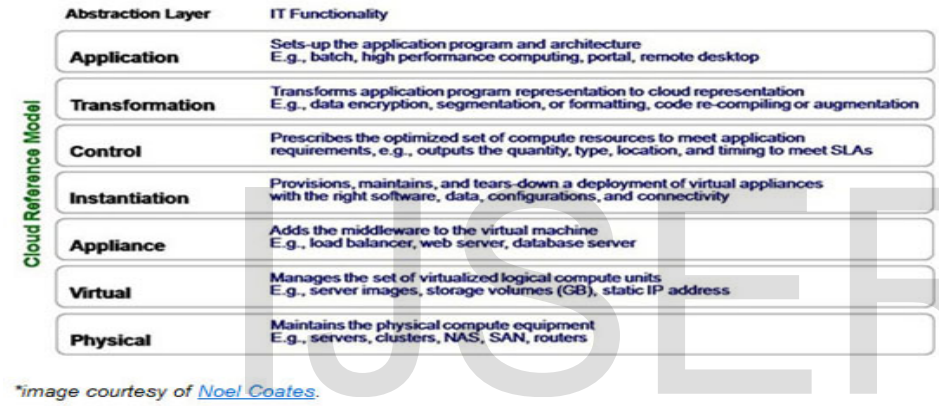

Fig.1. Cloud reference Model.

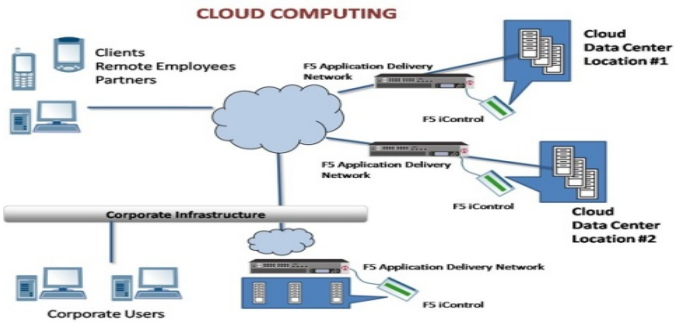

Fig .2. Cloud Computing

Advantage of Cloud Computing:

1 Ultra large-scale: The scale of cloud is large. The cloud of Google has owned more than one million servers. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers. There are hundreds of servers in an enterprise.

2. Virtualization: Cloud computing makes user to get service anywhere, through any kind of terminal. You can complete all you want through net service using a notebook PC or a mobile phone. Users can attain or share it safely through an easy way, anytime, anywhere. Users can complete a task that can't be completed in a single computer.

3 High reliability: Cloud uses data multigrain script fault tolerant, the computation node isomorphism exchangeable and so on to ensure the high reliability of the service .Using cloud computing is more reliable than local computer.

4 Versatility: Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

5. High extendibility: The scale of cloud can extend dynamically to meet the increasingly requirement.

6. On demand service: Cloud is a large resource pool that you can buy according to your need; cloud is just like running water, electric, and gas that can be charged by the amount that you used.

7. Extremely inexpensive: The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully enjoy the low cost advantage. Various application and advantage of cloud computing are listed below.

:

1 Cloud computing do not need high quality equipment for user, and it is easy to use.

2 Cloud computing provides dependable and secure data storage center. You don't worry the problems such as data loss or virus.

3 Cloud computing can realize data sharing between different equipments.

4 Cloud provides nearly infinite possibility for users to use internet.

Applications of cloud computing:

1. Most Common Cloud Many providers of different Example: Sales force, Gmail, Yahoo mail, Quicken online.

2. This is also support in part if gifts from google, Microsoft, sun Microsystem ,Amazon Web Services ciscosystem cloudera, eBay,Facebook, fujitsu, Intel, Network appliances, sap, VMware yahoo and by using in cloud computing**.**

Requirement of software and Hardware:

We predict cloud computing will grow, so developers should take it into account Regardless of whether a cloud provider sells services at a low level of abstraction like EC2 or a higher level like AppEngine, We believe computing, storage, and networking must all focus on horizontal scalability of virtualized resources rather than on single node performance. Moreover:

1. Application software needs to both scale down rapidly as well as scale up, Which is a new requirement. Such software also needs a pay-for –use licensing model to match needs of cloud computing.
2. Infrastructure software must be aware that it is no longer running on bare metal but on VMS. Moreover, metering and billing need to be built in from the start.
3. Hardware system should be designed at the scale of container(at least a dozen racks),Which will be the minimum purchase size. cost of operation will match performance and cost of purchase in importance, rewarding energy proportionality by putting idle portions of the memory, disks, and network into low-power mode. Processors soul work well with VMS and flash memory should be added to the memory hierarchy, and LAN switches and WAN routers must improve in bandwidth and cost.

II Literature Review:

A. Origin and definition of cloud computing

The Internet began to grow rapidly in the 1990s and the increasingly sophisticated network infrastructure and increased bandwidth developed in recent years has dramatically enhanced the stability of various application services available to users through the Internet, thus marking the beginning of cloud computing network services. Cloud computing services use the Internet as a transmission medium and transform information technology resources into services for end-users, including software services, computing platform services, development platform services, and basic infrastructure leasing as shown fig. As a Concept , Cloud computing primary significance lies in allowing the end user to access computing resources through the Internet as shown fig 3.

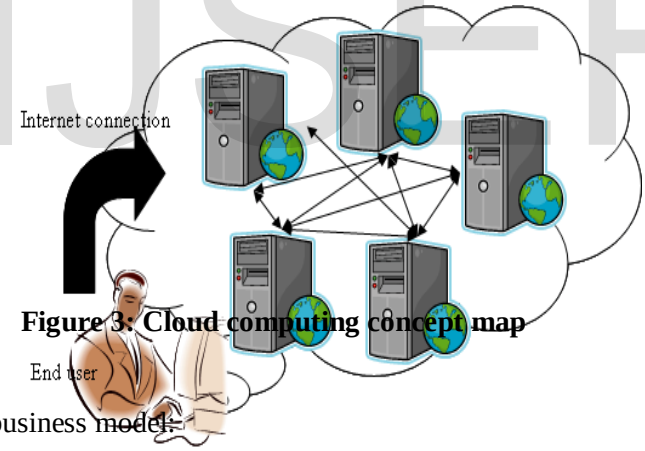

Figure 3: Cloud computing concept map

B. Cloud computing business model:-

The hardware and architecture required for providing cloud computing environment services is similar to most computer hardware and software systems. The hardware in a modern personal computer (i.e , C.P.U, HDD , Optical drive,etc.)
Performs basic function such as performing calculations and storing data. The operating system (e.g., window XP) is the platform for operations of the basic infrastructure,and text processing such as MSW word and Excel are application services which run on the platform.

Bulinding a cloud computing application as a services require infrastructure, platform and application software which can be obtained from a single provider or from different service providers.
Fig 4. Present a hierarchical structure, with Platform as services as the value-added infrastructure service. The Application is built on the infrastructure and computing platform, and requires a specific user interface.

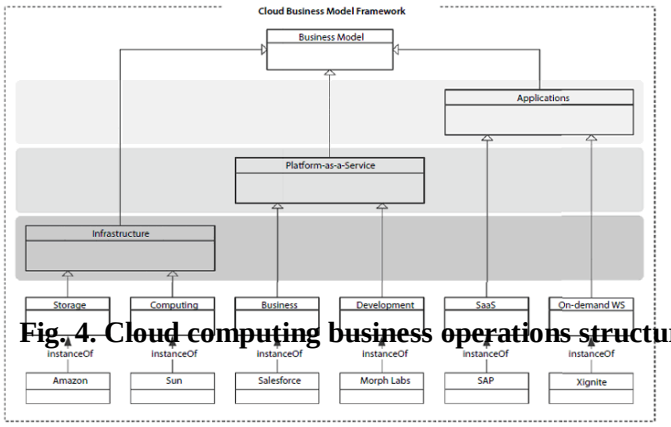

Fig. 4. Cloud computing business operations structure

Existing Method:

Common data encryption methods include symmetric and asymmetric cryptography algorithms. Symmetric cryptography is used in the U.S. Federal Information Processing Standard's (FIPS) 46-3 Triple Data Encryption Algorithm (TDEA, also known as Triple-DES or 3DES) or 197 Advanced Encryption Standard (AES) and others. This type of encryption and decryption process uses a secret key. Asymmetric cryptography, on the other hand, uses two different keys, a "public key" for encryption, and a "private key" for decryption. Examples include RSA cryptography and Elliptic Curve Cryptography [12]. Generally speaking, symmetric cryptography is more efficient, and is suitable for encrypting large volumes of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography.

Proposed Method:

For cloud computing to spread, users must have a high level of trust in the methods by which service providers protect their data. This study proposes a Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, emphasizing that authorization for the storage and encryption/decryption of user data must be vested with two different service providers. Furthermore, the privileges of the Encryption/Decryption as Service provider includes management of the key required for the encryption/decryption of user data, but not the storage of decrypted or encrypted user data. In this new business model, user data in the Storage Service System is all saved encrypted.Without the decryption key, there is no way for the service provider to access the user data. Within the Encryption/Decryption Service System there is no stored user data, thus eliminating the possibility that user data might be improperly disclosed as shown fig. 5.

Block Diagram:

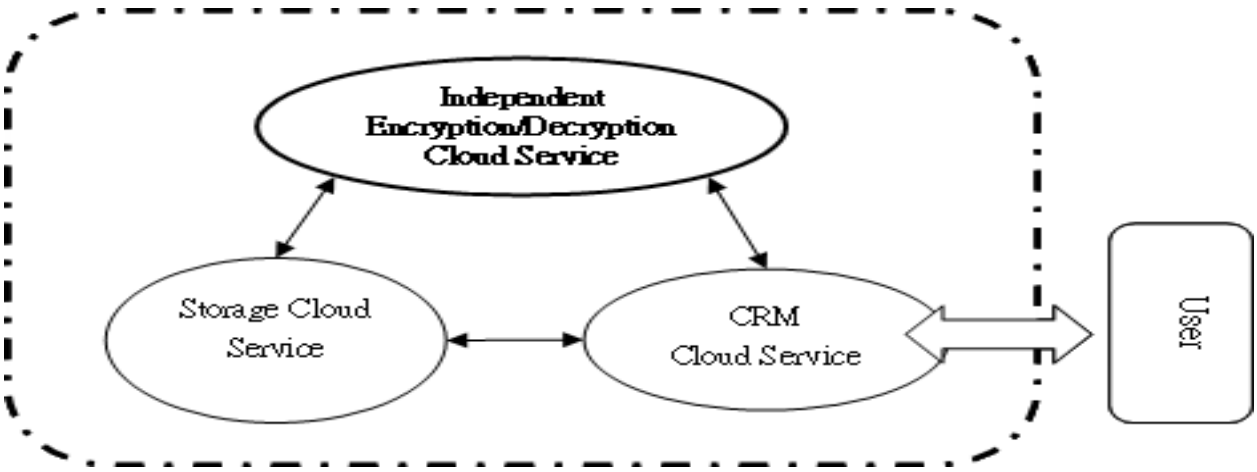

Fig.5 Encryption or Decryption Model of Cloud computing.

In this Block diagram three cloud service system: CRM Service system, Encryption / Decryption Service System, and Storage Service System.

Data storage Request (user): The client sending a data storage request to the CRM Service system which then imitates the data storage program, requesting data encryption from the Encryption/ Decryption service System as shown in fig. model, Fig. 5 presents an example in which the uses separate cloud services for CRM, storage and encryption/decryption. According to the user's needs, CRM Cloud Services could be swapped for other function-specific application services (e.g., ERP Cloud Services, Account Software Cloud Services, Investment Portfolio Selection and Financial Operations Cloud Services). Prior to the emergence of an emphasis on the independence of encryption/decryption services, CRM, ERP and other cloud services would simultaneously provide their users with storage services. This study emphasizes thatEncryption/Decryption Cloud Services must be provided independently by a separate provider.

References:

[1] http://en.wikipedia.org/wiki/Cloud_computing
[2] http://www.cloudcomputingchina.cn/Article/ujjan/200909/306.html
[3] http://searchcloudcomputing.techtarget.com/s
Definition/0, sid201_gci1287881,00.html
[4]http://www.boingboing.net/2009/09/02/cloudcomputing-skep.html
[5] http://dl.acm.org/citation.cfm?id=1721672
[6] A. weiss, "Computing in the clouds ", net Worker, vol. 11, no 4, pp.16-25, December 2007.
[7] C.S Yeo ,S. Venugopal,X. Chu,and R.Buyya,"Autonomic service", Future Generation Computer Systems, Vol. 26 issue 8, pp.1368-1380 october 2010.
[8] R. Bunya, C. S. Yeo, S. Venugopal, J. Broberg,and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.
[9] Salesforce.com, Inc., "Force.com platform, "Retrieved Dec. 2009, fromhttp://www.salesforce.com/tw/
[10] V. Miller, "Uses of elliptic curves in cryptography," Advances in Cryptology -CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986. L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.

[11] Shuai Zhang, Shufen Zhang, Xuebin Chen and Xiuzhen Huo, (2010) "Cloud Computing Research and Development Trend", Second International Conference on Future Networks, pp 93-97.