Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secure Cloud Computing Model Based on Multi Cloud Service Providers

Mooga Masthan
M.Tech 2nd year, Dept of CSE,
ASCET, GUDUR, India

Dora Babu Sudarsa
Associate Professor, Dept of CSE,
ASCET, GUDUR, India

Abstract— ***In cloud computing, cloud service provider provides its internal storages for storing client's data and installing firewall, ips/ids to protect against attacks. Storing data in encrypted fonnat is a common method of data privacy protection. If a cloud service provider is responsible for all services (authentication, encryption/ decryption, storage and auditing) then high level administrators may obtain user id, password, encrypted data and decryption keys which cause a risk for the unauthorized disclosure of the user data. This model proposes a secure cloud computing model based on separating the storage service from authentication, encryption/ decryption and auditing services. In addition, the party operates on storage must store encrypted data and the party operates on authentication, encryption/ decryption and auditing services must delete all data upon computation complete i.e. One cloud service provider is responsible for storage and the other one is responsible for authentication, encryption/ decryption and auditing services. At last the cloud service providers should sign multi-party service level agreement to establish cooperation model for providing common services to clients.***

Keywords— Computing, Cloud Computing Security , Service Level Agreement (SLA), Infrastructure as a Service (SaaS)

I. INTRODUCTION

The boom in cloud computing [I] over the past few years has led to a situation that is common to many innovations and new technologies such as service oriented utility computing [2], grid computing [3] with large amount of computing resources. In the term 'cloud computing' the word 'cloud' is a metaphor for the Internet. By using cloud computing, you can gain access any time through any device via the Internet to data and files which you have uploaded, or to software applications which you need to use for personal or professional use. In cloud computing, cloud providers provide their own storage for storing their client's information and protected by firewall which prevent intruders to access the data. The cloud providers have specific policies and practices to protect their client's data. Moreover, the practices for preventing high level administrators from unauthorized access to client's information which causes unauthorized disclose of the client's data. In cloud computing, the services offered by cloud service provider (CSP) can be adjusted according to the needs of client. For example, storage, transmission speed, no. of applications use, data encryption, data privacy etc. These services are started in service contract. The service contract includes service items, service scope, scope of privacy and protection, client responsiveness etc ... By signing Service Level Agreements (SLA) [4], the client has understood and agreed to those services provided by CSP. A common method to protect client data is that separating storage service from authentication, encryption/ decryption, audit services. If authentication, encryption/decryption, auditing and storage services performed by same service provider then system administrators can use the password or encryption/decryption keys to access user data which causes risk to client's sensitive information. This study proposes a secure model for cloud computing based on the concept of two cloud service providers. In this model, the storage service is provided to one CSP and authentication, encryption/ decryption and auditing services provided to another CSP. In addition, data storage system will have no access to password table, encryption/decryption keys table which is carried by another CSP. The CSP working on encryption/decryption, auditing will delete all the temporary data after necessary transmission. Under this model, the data storage CSP is authorized to store and retrieve client's encrypted data but don't access to encryption/decryption keys and the other one, stores password hash in password table. So, that admin of this CSP can't get the password. In addition, storing encryption/Decryption keys securely so, that storage CSP can't access to key table.

Making storage service independent from other services provides a unique model of cloud computing which are operated by different cloud providers and Providers should sign conventional SLA to establish a secure model for providing common services to clients.

II. LITERATURE REVIEW

A. Cloud Computing Business Model :

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.

The architecture of cloud services can be divided into three levels: infrastructure, platform and application software [5]. In the business model using software as a service, users are provided access to application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run. Software as a Service (SaaS) is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. SaaS providers generally price applications using a subscription fee.

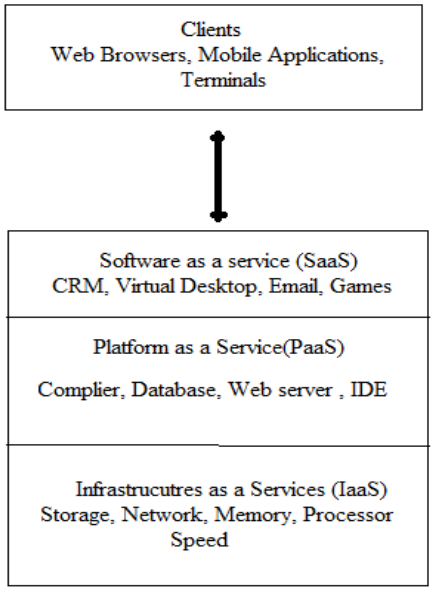

Fig. 1. Cloud Computing layer architecture

Fig. I presents a layer structure with platform as a service as the value-added infrastructure service. The application is built on the infrastructure and computing platform and requires a user interface. Proponents claim that the SaaS allows a business the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider. This enables the business to reallocate IT operations costs away from hardware/software spending and personnel expenses, towards meeting other IT goals. In addition, with applications hosted centrally, updates can be released without the need for users to install new software. End users access, cloud-based applications through a web browser or a light-weight desktop [6] or mobile application while the business software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud computing relies on sharing of resources to achieve coherence and economics scale similar to a utility (like the electricity grid [3]) over a network.

B. User data privacy concerns in a cloud computing:

In a cloud computing environment, the equipment used for business operations 'Can be leased from a single service provider along with the application, and the related business data can be stored on equipment provided by the same service provider. Storing the company's data on the service provider's equipment raises the possibility that information may be improperly disclosed to others. Some researchers have suggested that user data stored on a service provider's equipment must be encrypted. However, if the decryption key and the encrypted data are held by the same service provider, the high-level administrators within the service provider would have access to both the decryption key and encrypted data, thus presenting a risk for the unauthorized disclosure of the user data.

C. Existing methods for protecting client's data:

In existing cloud computing, client's data is encrypted before storage. Client authentication procedure is prior to storage or retrieval. All the communication channels are encrypted for secure data transmission. Common data encryption methods include symmetric and asymmetric cryptography algorithms. In case of symmetric cryptography a secret key is used for encryption and decryption. In the other hand Asymmetric key cryptography uses two different keys, "public key" for encryption and "private keys for decryption. Some of the symmetric key algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (3-DES), Advance Encryption Standard (AES) [7] etc.. Asymmetric key algorithms are RSA cryptography [8] and Elliptic Curve Cryptography (ECC) [9].

Password authentication is a general authentication procedure used by every cloud service provider (CSP). During registration, client gives own user id and password and these will store directly in password file of database. This file is encrypted and protected from other system files of the cloud systems.

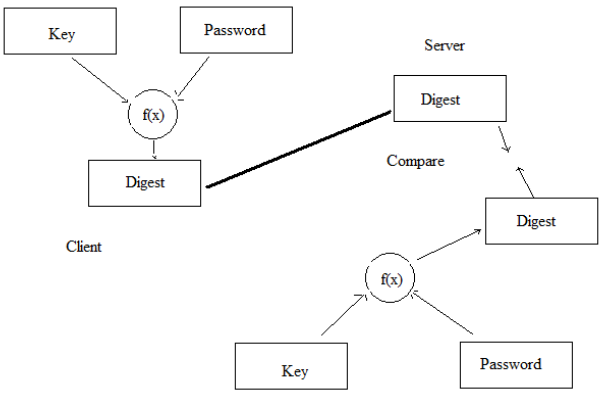

Fig 2: Password authentication mechanism

Fig. 2 presents how authentication mechanism is worked in case of password authentications. During login, client gives own user id and password. These are encrypted to form digest and this digest sends to server side. At server side, stored password is encrypted and compared with the digest from client side. If both are same then client gets the authorization. However, if administrator with high privileges can decrypt the file which may cause unauthorized access to user data. Now a day, one of the strong authentication mechanisms is two factor authentications with one time pad password [-10]. Fig. 3 presents how a two factor authentication with one time pad mechanism is worked through mobile SMS.

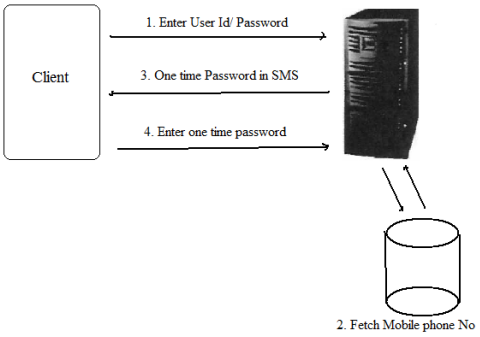

Fig. 3. Operation of one time pad password authentication through SMS

During Login client will enter User Id/ Password. After verification, if client is one of the authorized clients, a one time password is generated by server and that password is stored in database. According to client phone no. the password is send to client phone'. During next login the client has to use the SMS password for authentication. Throughout this operation, all the passwords are stored in database; it may be for few time or more. So, this mechanism is not a secure one. Another limitation of this mechanism, if clients are more this may cause DOS. In cloud computing, all the. transmission takes place through secure channels. The Secure Sockets Layer (SSL) [11] is a common method of building secure channels. Different encryption/ decryption algorithms are used to encrypt the data transmitted between clients and server.

III. PROPOSED MODEL

A. Core Concepts

This study proposes a secure Model for Cloud Computing based on two cloud service providers. The concept is based on securing user data i.e. separating storage service from authentication, encryption/decryption, auditing services. As shown in Fig. 4. In this model authentication, encryption and decryption, audit services provided by one CSP and storage service is provide by another CSP. Storage service provider having no control over other CSP and it stores data in encrypted format. Other CSP must delete the temporary data after necessary computation to prevent unauthorized access by its admin.

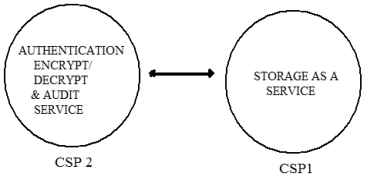

Fig 4: Storage as an independent service

To illustrate the concept of our proposed business model, Fig. S presents an example in which the client uses storage and other services. According to the user's needs, services could be swapped for other function-specific services. Here authentication, encryption/decryption and audit services handled by CSP 2 and storage service is handled by CSP1. There is no dependency between two service providers.

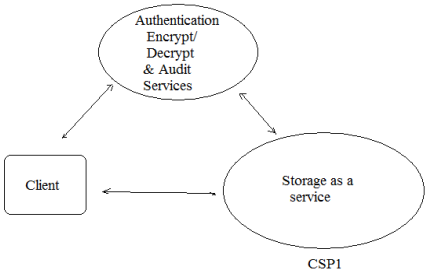

Fig. 5. Model of cloud computing with separate storage and authentication, encryption/decryption, auditing services

Prior to an emphasis on the independence of authentication, encryption/decryption, audit services from storage, CRM, ERP and other cloud services would simultaneously provide their client with storage services. The cooperation between two service providers will be established through SLA.

B. Operation of Authentication as a Service

Throughout two factor authentication, all the passwords are generated and stored in database, its may be for few time or more. So, this mechanism is not a secure one which is already discussed. Another limitation of this mechanism, if clients are generating passwords at login time may cause Denial of Service Attack (DOS) [12]. To avoid these types of limitation, this study proposes a model for separate authentication as a service and giving responsibility to other CSP to avoid all the work done by same CSP. This will possible through collaboration between two service providers. Fig 6 presents the model of separate authentication i.e. authentication service is provided by separate CSP.

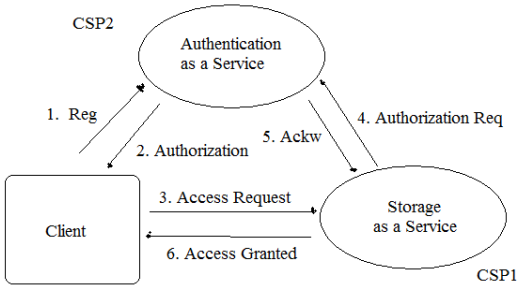

Fig 6. Authentication as a service diagram

When a client wants to access the cloud services, he/she must go through authentication process. In case of a new client, first he will register to get the cloud services as shown in step I. This step uses e-commerce application services for registration/login processes. All the authenticated data are stored in CSP2 for client authentication. Next time, client must go through the login process to get into the cloud. Authentication server will check whether client is the authorized one or not. If so, then it provides authorization to that client as shown in step 2. Suppose client wants to access data what is stored previously, then access request is generated from client to CSPl server as shown in step 3. CSPl will check whether he/she is the valid one through step 4 and 5 as shown in the above fig ... If client is the authorized one, client request is granted by CSPI and necessary data will transfer as shown in step 6. One of the limitations of two factor authentication mechanism which described in literature review is admin, can be avoided by modifying it to two factor authentication with symmetric key encryption which is proposed by some of the scientists. Fig. 7 Shows working model of two factor authentication mechanisms with symmetric key encryption. These factors/keys are from something the user knows (e.g. Password, pin, pattern), something the user has (e.g. ATM card, smart card) and something the user is (e.g. biometric characteristic such as a fingerprints).

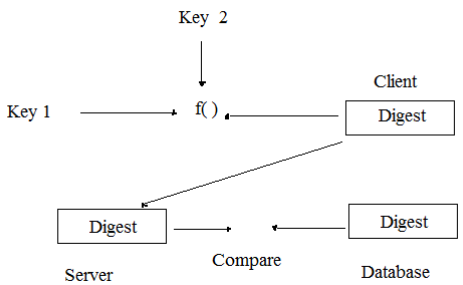

Fig. 7. Two factor authentication mechanism with symmetric key encryption

In steed of storing password, it stores the digest in database. During authentication process, digest generated from two keys from client side is compared with digest stored in database. AES algorithm with high key factors may used, for security proposes.

C. Operation of Encryption / Decryption as a Service

This concept is based on separating the storage and encryption/ decryption of user data as shown in fig 7 and 8. In this business model, Encryption /Decryption and storage as a Service are not provided by a single operator. Storage' as a Service (SaaS) provider may not store unencrypted user data and, once the provider of Encryption/Decryption as a service has finished encrypting the user data, the system must delete all encrypted and decrypted user data.

Fig. 8 presents, data retrieval diagram of proposed business model. When client wants to access a file which is encrypted and stored in storage provided by CSP1 the file is transferred to CSP2 for decryption. At last, the unencrypted file is transferred to client.

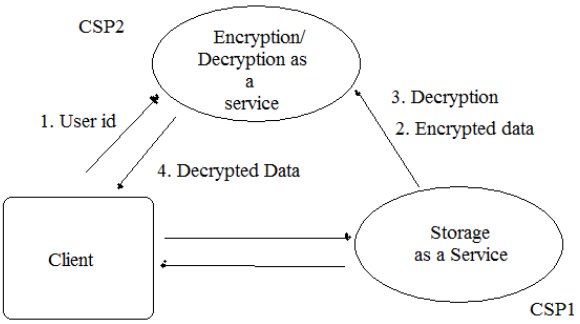

Fig 8. Data retrieval diagram

After successful login, suppose client sends data request to fetch a file from storage, its User Id will automatically send to CSP2 which is shown in step!. According to request CSP1 sends encrypted data/file to CSP2 for decryption which is belongs to step 2. In step 3 CSP2 fetch client's private key from key table and decrypt the file. After decryption the decrypted file is send to client and all temporary data will be deleted to protect client's encrypted data which is the last step of data decryption. Next, we describe the Data storage program, as shown in Fig. 9. When clients want to upload/ store a data in cloud the data is transferred to CSP2 for encryption. After encryption operation,' the encrypted data is transferred to CSPl for store. If all the operation completed successfully then success message is transferred to client.

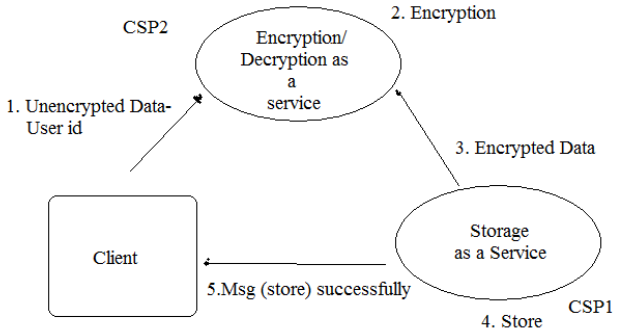

Fig 9: Data storage diagram

Similarly, after successful login, if a client sends a file for storing purposes then the file with its User Id will be sending to CSP2 shown in step!. According to User Id, it will fetch encryption /public key. Using this key it will encrypt all clients' data which are belonging to step2. In step 3 and 4, the encrypted data is transferred to CSP1 for storage. If storage is successful, then a storage successful message is generated and transferred to clients in step5. After encryption all the temporary data will be deleted. In both cases, temporary data is deleted after encryption /decryption operation. RSA algorithm is used for encryption /decryption. Both private and public keys are stored and handled by CSP2. In both cases all the channels of communication will be encrypted to prevent any types of sniffing attacks which can be possible by implementing SSL protocols.

D. Operation of Auditing as a Service

The client can access the data, use the data and store the data. In a Corporate world there are large number of client who accessing their data and modifying a data. In Cloud. application software and services are move to the centralized large data centre and management of this data and services may not be trustworthy. To manage this data we use third party auditor (TP A).It will check the reliability of data but it increases the data integrity risk of data owner. Since TP A not only read the data but also it can modify the data. Therefore a mechanism is provided who solved the problem.

Fig. 10 shows the model of auditing using third party (CSP2) as auditor. In this proposed model• TP A can check the data for integrity and reliability after certain period of time.

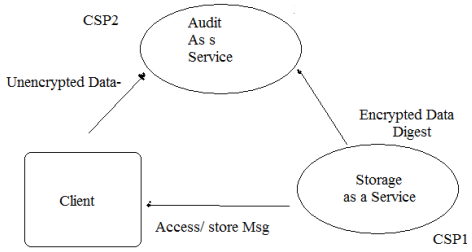

Fig 10: Data security Using third party(CSP2) as auditor

In this model CSP2 as auditor, audit client's data after certain instant of time. Integrity of a file is verified from its digests stored in CSPI. CSP2 periodically fetches these digests and verify whether data is correct. If there is some change in pattern, then it will inform to client that file is corrupted.

Audit as a service (CSP2) generates three types of digests for maintaining data integrity, reliability etc.

$$(F', Ó, I/U/D) \rightarrow Md$$

$$(Filename, Ó, I/U/D) \rightarrow M$$

$$(F', Md) \rightarrow Td$$

CSP2 digest Md. This Md will be merge with F' to form Td. This data is send along with M to CSP1. During integrity checking CSP1 sends Td to CSP2. CSP2 disintegrate the data from Td to form F' and Md. Then it checks F' with F' came from Md. If something wrong in file then it will ask the client and data owner to replace that file with new one.

Here F' indicates encrypted file, Ó for digital signature [8] of client, I for insertion U for Update and D for delete.

a. Insertion After verification of client the CSP1 will ask the client for new location of file. Client's file is send to CSP2. CSP2 generates Td, M and sends Td along with M to CSP1 for storage proposes.

b. Deletion Client sends a request to CSP 1 to delete the record. Client sends the file name to CSP2. CSP2 sends digest like M (Filename, (2), D) to CSP1 for delete. CSP1 delete the particular file from storage by matching filename.

c. Update Client gets the file for modification from CSPI. After modification it sends file to CSP2. It generates F', Md , Td and sends Td with (Filename, Ó, U) to CSP1 for modifying the particular file. CSPI will replace the previous one with the new one by matching the file name.

Encryption/ decryption of file operation are taken place by encryption/decryption as a service which is provided by CSP2. After computation and transmission of digests, all the data will be deleted by CSP2 to maintain data privacy.

E. Service Level Agreement

The above model has multiple service operators coordinating to provide a CRM cloud service. The data handling flow and cooperation among operators will affect the effectiveness with which clients use the service. A service-level agreement (SLA) is a part of service contracts where a service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service or performance). As an example, internet service providers will commonly include service level agreements within the terms of their contracts with customers to define the level(s) of service being sold in plain language terms. Any SLA between the client and the service provider must consider the rights and obligations of the collaborating operators, and operators should sign contracts between themselves to establish the division of responsibilities and cooperation model for providing common services to clients. The proposed example includes a template for a multi-party SLA for the user, authentication, encryption/decryption and audit service operator (CSP2), storage service operator (CSPI). The content is based on rights and obligations for ensuring data privacy and protection as shown in fig. 11.

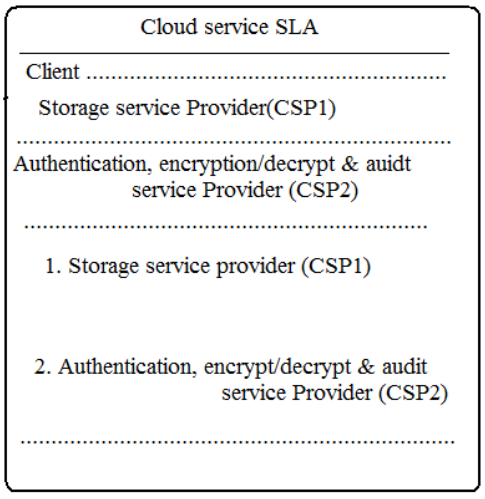

Fig. 11. Cloud services SLA template based on policy and privacy.

IV. Conclusion

In cloud computing, three services are provided by cloud. These are software as a service (SaaS), Platform as a service (PaaS) and infrastructure as a service (IaaS). A client can access the services by using laptop, PC, smart phone/PDA etc . .In cloud computing all clients' data is encrypted prior to storage and stored in CSP server. However, if the decryption key and encrypted data are held by the same service provider, it raises the possibility that high-level administrators within the service provider would have access to both the decryption key and encrypted data, presenting a risk for the unauthorized disclosure of the user data. This study proposes "A• secure cloud computing model based on two cloud service providers". After establishing of this model, clients of cloud services will use the services of two cloud service providers.

So, contract between two service providers is required to establish a cooperation model for providing common services to clients. In future, this model will be enhanced by adding biometric authentication with password authentication. The theme of this study is division of authority to reduce operational risk, thus avoiding for the unauthorized disclosure of the client's data.

References

[1]. M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.

[2]. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com /developerswork/websphere/zones/hip ods/library.html, October 2007, pp. 4-4

[3] G. Frankova, Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.

[4]. "Service Level Agreement and Master Service Agreement", http://www.softlayer.com/sla.html, accessed on April 05, 2009.

[5]. S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "Security for the cloud infrastrcture: trusted virtual data center (TVDc)." [Online]. Available: www.kiskeya.net /ramon/work/pubs/ibmjrd09.pdf

[6]. http://www.cloudsecurity.org, accessed on April 10, 2009.

[7]. "Sampling issues we are addressing", http://cloudsecurityalliance.org/issues.html#15, accessed on April 09, 2009.

[8]. MikeKavis,"Real time transactions in the cloudhttp://www.kavistechnology.com/ blog/?p=789, accessed on April 12, 2009.

[9]. "Secure group addresses cloud computing risks", http://www.secpoint.com/security-group-addresses-cloudcomputingrisks.html, April 25, 2009.

[10]. "Service Level Agreement Definition and contents", http://www.servicelevel-agreement.net, accessed on March 10, 2009.

[11] "Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1," Dec 2009. Available at: www.cloudsecurityalliance.org.

[12]. "Wesam Dawoud, Ibrahim Takouna, Christoph Meinel Infrastructure as a Service Security,

