A Secure Model and Algorithms for Cloud Computing Based on Multicloud Service Providers

Ashutosh Satapathy
Department of IT,
College of Engineering and Technology
Bhubaneswar, Odisha, India

J. Chandrakanta Badajena
Department of IT,
College of Engineering and Technology
Bhubaneswar, Odisha, India

Chinmayee Rout
Department of CSE
Ajay Binay Institute of Technology
Cuttack, Odisha, India

Abstract— **In modern computing environment, using cloud computing mechanism, cloud service provider provides its internal storages for storing client's data and installing firewall, ips/ids to protect against attacks. To achieve data privacy protection one common method used is storage of data in encrypted format. 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— Cloud Computing; Service Level Agreements; Authentication Service; Encryption and Decryption; Audit Service; Data Privacy

I. INTRODUCTION

The rapid progress in cloud computing [1] 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, grid computing with large amount of computing resources. In the term 'cloud computing' the word 'cloud' is a metaphor for the Internet. By using cloud computing, we can access data and files any time through any device via the Internet which we have uploaded, or software applications which we 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 access to the client's data and may hamper the confidentiality, integrity and availability of it.

The services offered by cloud service provider (CSP), in cloud computing environment, can be adjusted according to the needs of client. For example, storage, transmission speed, number 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) [2], the client has understood and agreed to those services provided by CSP.

The client data can be protected using a separate storage service apart 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.

literature review

A. Cloud Business Model

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a

network mostly in internet. The name comes from the use of a cloud shaped symbol as an abstraction for the complex infrastructure present in system diagrams. Remote services with a user's data, software and computation are secure in cloud computing.

The architecture of cloud services can be divided into three levels: infrastructure, platform and application software [3]. 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. 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.

Cloud-based applications can be accessed by the end user's through a web browser or a light-weight desktop [4] or mobile application while the business software and user's data are stored on servers at a remote location and 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.

B. Data Privacy in the Cloud

In the 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 and may create vulnerability to private data.

C. Existing Methods for Protection

In existing cloud computing mechanisms, client's data is encrypted before storage. Client authentication procedure occurs prior to storage or retrieval. All the communication channels are encrypted for secure data transmission.

Common data encryption methods include symmetric (private or secret key encryption) and asymmetric (public key encryption) cryptography algorithms. In case of symmetric cryptography a secret key is used for both encryption and decryption. In the other hand Asymmetric key cryptography uses two different keys, "public key" for encryption and "private key" for decryption. Some of the symmetric key algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (3-DES), and Advance Encryption Standard (AES) [5] etc.. Asymmetric key algorithms are RSA cryptography [6] and Elliptic Curve Cryptography (ECC) [7].

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.

Now-a-days, one of the strong authentication mechanisms is two factor authentications with one time pad password [8]. 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 Denial-of-Services (DOS).

In cloud computing, all the transmission takes place through secure channels. The Secure Sockets Layer (SSL) [9] is a common method of building secure channels. Different encryption/ decryption algorithms are used to encrypt the data transmitted between clients and server.

II. PROPOSED MODEL

A. Core Concept

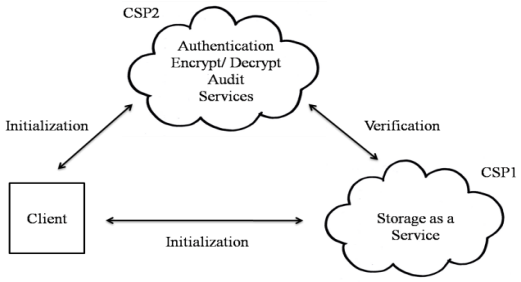

Figure 1: Model of Cloud Computing with Separate Storage and Authentication, Encryption/Decryption, Auditing Services

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. According to the user's needs, services could be swapped for other function-specific services. Here authentication, encryption/decryption and audit services handled by CSP2 and storage service is handled by CSP1. There is no dependency between these two service providers.

B. Authentication as a service

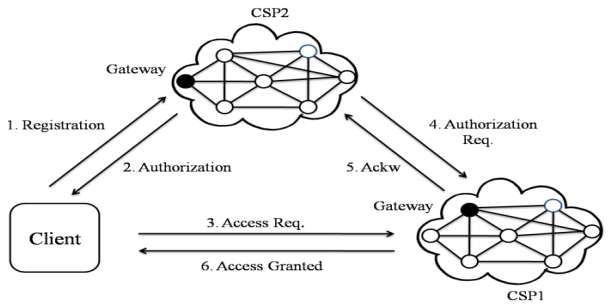

Figure 2: Authentication as a Service

When a client wants to access the cloud services, he/she must go through authentication process. In case of a new client, first he/she must register to get into the cloud services as shown in step1. 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 step2. Suppose client wants to access data stored previously, then access request is generated from client to CSP1 server as shown in step3. CSP1 will check the authorization of user through step4 and sends an acknowledgement to CSP2 at step5 as shown in the figure above. If client is the authorized one, client request is granted by CSP1 and necessary data will transfer as shown in step 6.

Authorized users can access cloud using their mobile devices (e.g., Notebook PC, PDA). Before issuing any queries to or access data from CSP1, the user has to register with the CSP2 of the network. Upon successful registration, the user can submit query to the cloud at any time. The basic idea of the protocol is that a user will receive a personalized smart card from the gateway at the time of the registration process and then, with the help of user's password and smart card the user can login to the CSP2 and access data from the network. The protocol is divided into two phases: Registration phase and Authentication phase.

ID_i	Identity of client
PW_i	Password of client
DID_i	Dynamic login identity of client
CSP2	Cloud service provider 2
K	Symmetric key of CSP2
H()	Hash functions
S_1 XOR S_2	String S_1 is XOR with string S_2

Table 1: Notation used in the Protocol

a) Registration Phase

This phase is invoked when a user, U_i, wants to register with the cloud. U_i submits his/her identity (ID_i) and password (PW_i) to the gateway in a secure manner. Upon receiving the registration request, the gateway of CSP2 computes $N_i = H(ID_i||PW_i)$ *XOR* $H(K)$, where K is a symmetric key known to only gateway, and || is bit-wise concatenation operator. Then the gateway personalizes a smart card with the parameters $H()$, ID_i, N_i, $H(PW_i)$ and x_a, where $H()$ is a cryptographically secure hash function. Here, x_a is a secret parameter generated securely by the gateway and stored in CSP2 The gateway now sends the personalized smart card to U_i in a secure manner. We note that x_a is not known to the user, as it is generated and stored in user's smart card securely by the gateway.

b) Authenhtication Phase

The authentication phase is invoked when U_i wants to perform some query to or access data from the network. The phase is further divided into Login and Verification phases. The authentication phase is invoked when U_i wants to perform some query to or access data from the network. The phase is further divided into Login and Verification phases.

1) Login Phase:

U_i inserts her/his smart card to a terminal, and keys ID_i and PW_i. The smart card validates ID_i and PW_i with the stored ones in it. If the entered ID_i and PW_i are correct, the smart card performs the following operations:

Step 1: Compute $DID_i = H(ID_i || PW_i)$ *XOR* $H(x_a||T)$, where T is the current timestamp of Ui's system.
Step 2: Compute $C_i = H(N_i||x_a||T)$.
Then send $< DID_i, C_i, T >$ to the gateway.

2) Verification Phase:

Upon receiving the login request $< DID_i, C_i, T >$ at time T^*, the gateway authenticates U_i by the following steps:

Step 1: Validate T. If $(T^* - T) \leq \Delta T$ then the gateway proceeds to next step, else abort, where ΔT denotes the expected time interval for the transmission delay.
Step 2: Compute $H(ID_i||PW_i)^* = DID_i$ *XOR* $H(x_a||T)$ and $C_i^* = H((H(ID_i||PW_i)^*$ *XOR* $H(K))||\ x_a\ ||T)$.
Step 3: If $C_i^* = C_i$, the GW-node accepts the login request; else rejects it.
Step 4: gateway now sends a message $< DID_i, A_i, T' >$ to CSP2, say, Sn, over a public channel to respond the query/data what U_i is looking for, where $A_i = H(DID_i||S_n\ ||x_a||T\ ')$, and $T\ '$ is the current timestamp of gateway system. Here, Ai is used to ensure CSP2 that the message $< DID_i, A_i, T' >$ has come from the legitimate gateway, as A_i is generated with secret parameter xa which is known to both CSP2 and gateway.
Step 5: Sn first validates T' in similar line of Step-V1. Then S_n computes $H(DID_i||\ S_n\ ||x_a||T\ ')$ and checks whether it is equal to A_i. If these two checks pass correctly then S_n responds to U_i's query.

C. Encryption/Decryption as a Service.

UID	Current User ID
SID	Current Session ID
Req	Query for retrieval of user file
E[File]	Encrypted file
K_p	Private key
D[,]	Decryption function
Msg	Notification generated by CSP1
K_s	Public key
E[,]	Encryption function

Table 2: Notation used in the encryption/decryption as a service

In this 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.

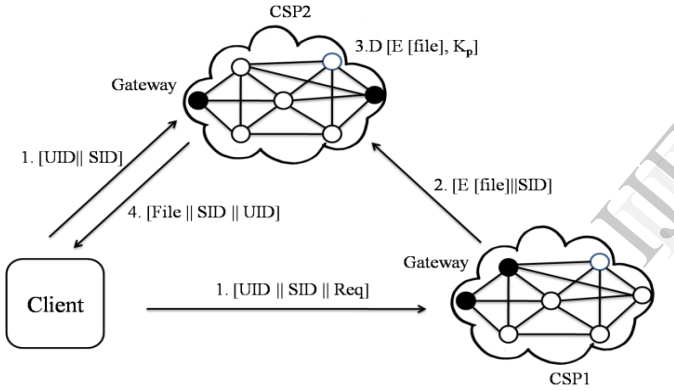

Figure 3: Data Retrieval Diagram

After successful login, suppose client sends data request to fetch a file from storage, its User Id and session Id will automatically send to CSP2 which is shown in step1. 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.

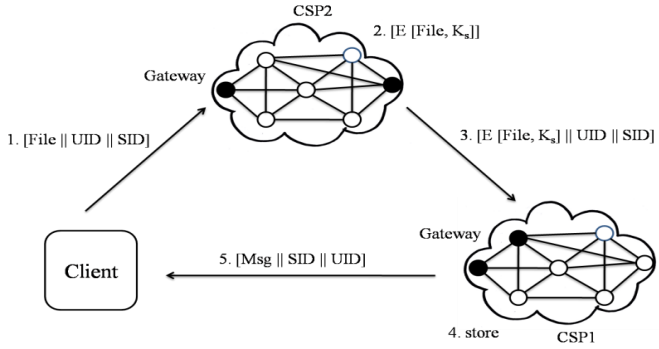

Figure 4: Data Storage Diagram

Next, we describe the Data storage program, as shown in Fig.4. 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 CSP1 for store. If all the operation completed successfully then success message is transferred to client.

Similarly, after successful login, if a client sends a file for storing purposes then the file with its User Id and Session Id will be sending to CSP2 shown in step1. 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 with large key size 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.

RSA Algorithm for key Generation:

Step1: Select two prime numbers p, q

Step 2: Compute $n=p \times q$

$v= (p-1) \times (q-1)$

Step 3: Select small odd integer k such that

$\gcd (k, v)=1$

Step 4: Compute d such that

$(d \times k)\%v =1$

RSA algorithm for encryption/decryption

Encryption compute $E (M) = (M^k) \% n$

Decryption compute $D (M) = (E(M)^d)\%n$

In this paper we propose four security levels. Each level has own database and consists of many sets, these levels identifiers by property of e values and the key length see table 3.

Security Level	Key Length
Low	512 bits
Medium	1024 bits
Medium-High	2048 bits
Security-High	4096 bits

Table 3: Security levels

D. 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 (TPA).It will check the reliability of data but it increases the data integrity risk of data owner. Since TPA not only read the data but also it can modify the data. Therefore a mechanism is provided who solved the problem. Fig. 5 shows the model of auditing using third party (CSP2) as auditor. In this proposed model TPA can check the data for integrity and reliability after certain period of time.

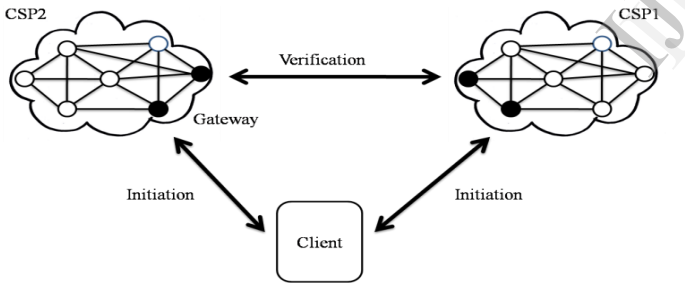

Figure 5 : Data Security Using Third Party (CSP2) as Auditor

In this model CSP2 as auditor, audit client's data after certain instant of time. Integrity of a file is verified from its digests store in CSP1. CSP 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.

Digest generation:

Step1: CSP2 generates 3 types of digests

M_d = (F', Ø , I/U/D)

M = (Filename, Ø, I/U/D)

T_d = (F', M_d)

Step 2: T_d is send along with M to CSP1.

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

Integrity checking:

Step1: T_d is send to CSP2.

Step2: disintegration of the data from Td to form F' and M_d .

Step3: checks F' with F' came from M_d .

Step4: If mismatch occurs then "replace with new one" msg generated.

Insertion:

Step1: CSP1 will ask the client for new location of file.

Step2: CSP2 generates T_d, M.

Step3: T_d is send along with M to CSP1.

Deletion:

Step1: File name is sends to CSP2.

Step2: CSP2 sends digest M (Filename, Ø, D) to CSP1.

Step3: Deletion occurs.

Update:

Step1: Get the file from CSP1 for modification.

Step2: File is send to CSP2.

Step3: Send T_d with M (Filename, Ø, U) to CSP1.

Step4: Modification occurs.

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.

III. EXPERIMENT AND RESULTS

With using RSA-Key Generations Algorithm and different keys lengths, the decryption processes is faster for smaller key length.

The timings were made on a 2.0GHz Pentium by using the below factors:

- Block size is 2048 bits.
- Different bandwidths:
  I. 1000 Mbps.
  II. 100 Mbps.
  III. 4 Mbps.

The Figure below shows the compare between RSA decryption processes by using RSA-Key Generations method.

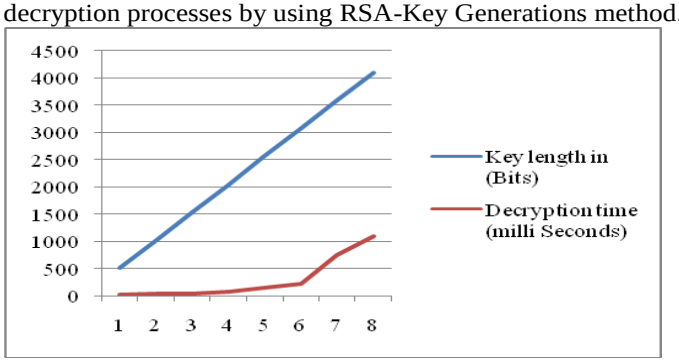

Figure 6: Compare between decryption processes using RSA-key generations

V. CONCLUSION

In cloud computing, three services are provided by cloud viz. 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. 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 administrator 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 this model, clients of cloud services can 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 incorporated with biometric authentication with password authentication to provide a strong and better security. The theme of this study is division of authority to reduce operational risk confidential data, thus avoiding for the unauthorized disclosure of the client's data.

REFERENCES

[1] A. Weiss, "Computing in the clouds", networker, vol. 11, no.4, pp. 16- 25, December 2007.
[2] Z. Shu, "An architecture design of life cycle based SLA management", IEEE International conference on Advance Communication Technology (ICACT), vol. 2, pp. 1351-1355, Feb 2010.
[3] M. Zhou, "Services in the cloud computing era: survey", IEEE 4th International conference on Universal communication Symposium (IUCS), pp. 40-46, October 2010.
[4] Lai, "A service based Lightweight Desktop Virtualization system", IEEE International conference on Service Sciences (ICSS), pp. 277-282, May 2010.
[5] O.P. Verma, "Performance analysis of data Encryption Algorithm", IEEE 3rd International Conference on Electronics Computer Technology (ICECT), vol.5, pp. 399-403, April 2011.
[6] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, no.2, pp.120-126, 1978.
[7] Miller, "Uses of elliptic curves in cryptography", Advances in cryptology-CRYPTO '85, Lecture Notes in Computer science, pp. 417- 426, 1986.
[8] Svogor, "Two factor authentication using EEG augmented Passwords", IEEE International Conference on Information technology interfaces (ITI), pp. 373-378, June 2012.
[9] A.C. Weaver, "Secure socket layer", IEEE Journal & Magazine on computer, vol. 39, Issue 4, pp.88-90, April 2006.
[10] K. Pelechrinis, "Denial of service attacks in wireless network: The case of jammers", IEEE Journal & Magazine on Communications Surveys & Tutorials, vol. 13, issue 2, pp. 245-257, Second quarter 2011.