Ms. Palvi Gupta, Ms. Ruchika Arora, Ms. Neha Pandey / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.1934-1941

An Adopted Secured Business Framework in the Cloud Environment

Ms. Palvi Gupta*, Ms. Ruchika Arora, Ms. Neha Pandey*****
*,**,***(Department of Computer Science Engineering from "Institute of Engineering & Technology" (Alwar).

ABSTRACT

Infrastructure as a Service is a provision model in which a Cloud Service Provider (CSP) outsources the equipment used to support operations, including storage, hardware, servers and networking components. In such an service model customer stores his/her information in the hands of service providers, the insider attacker, hacking etc are vital corners to be handled, many have proposed solutions but lack in basic business modelling, we present an business framework which can take a perfect role in governing the security structure and adoptability for the customer and the services providers.

Keywords- cloud computing; service level agreements; encryption and decryption cloud service; data privacy protection

I. INTRODUCTION

According to the http://en.wikipedia.org ---- "**Cloud computing** is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet)". Cloud computing entrusts remote services with a user's data, software and computation.

There are many types of public cloud computing:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Storage as a service (STaaS)
- Security as a service (SECaaS)
- Data as a service (DaaS)
- Database as a service (DBaaS)
- Test environment as a service (TEaaS)
- Desktop virtualization
- API as a service (APIaaS)
- Backend as a service (BaaS)

Prior to the development of the concept of cloud computing, critical industrial data was stored internally on storage media, protected by security measures including firewalls to prevent external access to the data and including organizational regulations to prohibit unauthorized internal access. In the cloud computing environment, storage service providers must have in place data security practices to ensure that their clients' data is safe from unauthorized access and disclosure. More importantly, the regulations and measures for preventing privileged users such as system administrators from unauthorized access must be rigorously established and implemented.

Service providers follow specific policies and practices to protect their users' data, and these policies are usually stated in the service contract. Most current network application services have the same practice. For example, a Yahoo! webmail user must read the service contract online and show his consent to the service contract before he can use the webmail service. The content of the service contract covers definitions of service items, service scope, service change notification, scope of privacy protection, regulations on user data collection, use, sharing and release, and statements regarding user responsibilities. Showing the consent to the service contract is an essential step of the service application.

In a cloud computing environment, the service content offered by service providers can be adjusted according to the needs of the user. For example, the applicant can request different amounts of storage, transmission speeds, and levels of data encryption and other services. In addition to defining the service items, the agreement normally also notes the time, quality and performance requirements provided with the service. Generally, these service agreements are referred to as Service Level Agreements (SLA) [4]. By signing an SLA, the user shows that he has understood and agreed to the contents of the application service, and agree with the provider's data privacy and protection policies.

A common approach to protect user data is that user data is encrypted before it is stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure.

Creating user trust through the protection of user's data content is the key to the widespread acceptance of the cloud computing. This study proposes a business model for cloud computing based on the concept of using a separate encryption and decryption service. In the model, data storage and decryption of user data are provided separately by

two distinct providers. In addition, those working with the data storage system will have no access to decrypted user data, and those working with user data encryption and decryption will delete all encrypted and decrypted user data after transferring the encrypted data to the system of the data storage service provider.

Under the business model proposed in this study, the data storage cloud system provider is authorized to store the user's encrypted data, but does not have access to the Decryption Key. Thus, the storage system can only retrieve encrypted user data, but is unable to decrypt it. The cloud computing system responsible for encrypting user data has authority over all encryption keys required for data encryption but, given that the encryption provider does not store the user's data, internal mismanagement of the decryption keys still poses no risk of unauthorized disclosure of the user's data.

Given that encryption is an independent cloud computing service, a unique feature of the business model is that different services are provided by multiple operators. For example, the
Encryption as a Service provider and the "Storage as a Service" provider cooperate to provide a Cloud Storage System with effective data protection. This study provides a draft SLA for this type of business model of combining multiple providers in a single service, which can establish the cooperation model between operators and the division of responsibility for the services they jointly provide to the user.

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 a concept, cloud computing's primary significance lies in allowing the end user to access computation resources through the Internet, as shown in Fig. 1. Some scholars find cloud computing similar to grid computing [3], but some also find similarities to utilities such as water and electrical power and refer to it as utility computing [2]. Because the use of resources can be independently adjusted, it is also sometimes referred to as autonomic computing [5].

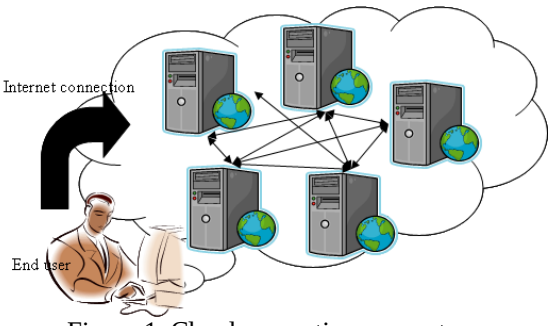


Figure 1. Cloud computing concept map

The literature contains many explanations of cloud computing [6]. After compiling scholarly definitions of cloud computing, Vaquero, Rodero-Merino, Caceres, and Lindner suggested that cloud computing could be defined as the integration of virtual resources according to user requirements, flexibly combining resources including hardware, development platforms and various applications to create services [7]. The special features of cloud computing include the storage of user data in the cloud and the lack of any need for software installation on the client side. As long as the user is able to connect to the Internet, all of the hardware resources in the cloud can be used as client-side infrastructure. Generally speaking, cloud computing applications are demand-driven, providing various services according to user requirements, and service providers charge by metered time, instances of use, or defined period.

B. Cloud computing business models

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., CPU, HDD, optical drive, etc.) performs basic functions such as performing calculations and storing data. The operating system (e.g., Windows XP) is the platform for the operations of the basic infrastructure, and text processing software such as MSWord and Excel are application services which run on the platform.

The architecture of cloud services can be divided into three levels: infrastructure, platform, and application software [7]. Application software constructs the user interface and presents the application system's functions. Through the functions of the operations platform, the application can use the CPU and other hardware resources to execute calculations and access storage media and other equipment to store data.

Building a cloud computing application as a service requires infrastructure, platform and application software which can be obtained from a single provider or from different service providers. If the revenue for cloud services primarily comes from charging for infrastructure, this business model can

be referred to as Infrastructure as a Service (IaaS). If revenue comes primarily from charging for the platform, the business model can be referred to as Platform as a Service (PaaS). If revenue primarily comes from charging for applications or an operating system, the business model can be referred to as Software as a Service (SaaS).

Summarizing existing cloud services, Weihardt et al. proposed a holistic business model framework [8], as shown in Fig. 2.

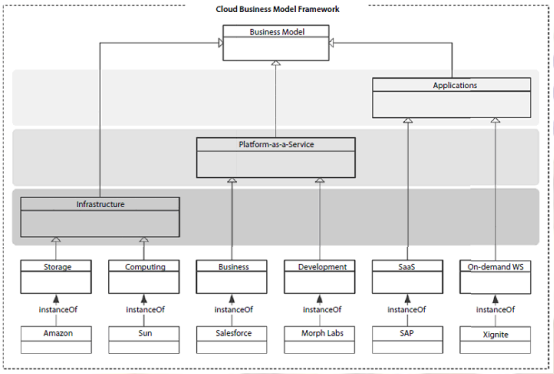


Figure 2. Cloud computing business operations structure

Fig. 2 presents a hierarchical 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 specific user interface.

C. User data privacy concerns in a cloud computing environment

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. This type of arrangement can help a company save on hardware and software infrastructure costs, but storing the company's data on the service provider's equipment raises the possibility that important business information may be improperly disclosed to others [9].

Some researchers have suggested that user data stored on a service-provider's equipment must be encrypted [10]. Encrypting data prior to storage is a common method of data protection, and service providers may be able to build firewalls to ensure that the decryption keys associated with encrypted user data are not disclosed to outsiders. However, if the decryption key and the 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 the encrypted data, thus presenting a risk for the unauthorized disclosure of the user data.

D. Existing methods for protecting data stored in a cloud environment

Common methods for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission. These protection methods normally require cryptography algorithms and digital signature techniques, as explained below:

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 [11] and Elliptic Curve Cryptography (ECC) [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.

The use of passwords as an authentication process is more familiar to general users, but messages sent by the user are vulnerable to surreptitious recording by hackers who can then use the data in the message to log into the service as the user. In more advanced authentication systems, the system side will generate a random number to send the user a challenge message, requesting the user to transmit an encrypted response message in reply to the challenge message, thus authenticating that the user has the correct encryption key. Without this key, the user will not be allowed access. In the process of challenge and response the client's encrypted key uses the client's password to convert a derived value and. In this program, each communication between the client and server is unique, and a hacker using an old message would fail to access the system. In addition, the One-Time Password (OTP) authentication system differs from most peoples' conception of a password [13]. Most people understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP however is the single-use nature of the password.

After receiving authentication from the user, the system side must create a secure transmission channel to exchange information with the user. The Secure Sockets Layer (SSL) is a common method of building secure channels [14], primarily using RSA encryption to transmit the secret keys needed for the both sides to encrypt and decrypt data transmitted between them.

When using cryptographic technology to protect user data, the keys used for encryption and decryption of that data must be securely stored. In particular, cloud computing service providers must have specific methods for constraining internal system management personnel to prevent them from obtaining both encrypted data and their decryption keys – this is critical to protecting user data. Operator policies for protecting user data must be clearly laid out in the Service Level Agreement (SLA) and must explain how special privilege users are prevented from improperly accessing user data.

Kandukuri, Paturi and Rakshit offer six recommendations for SLA content [4], including (1) special privilege user data access must be controlled to prevent unauthorized storage or retrieval, (2) cloud computing services must comply with relevant laws, (3) user data must be properly stored and encrypted, (4) a reset mechanism must be provided in case of service disruption or system crash, (5) service must be sustainable and guaranteed against service discontinuation due to change or dissolution of the provider and (6) if cloud computing services are used for illegal purposes, the provider must be able to provide records to assist with investigations.

III. AN ADOPTED SECURED BUSINESS FRAMEWORK IN THE CLOUD ENVIRONMENT

Cloud service provider (CSP) Lends his Infrastructure in the Model of IAAS And the Third party Lends Encryption and Decryption Software in the Model of SAAS, here the Entire Crypto system Keys Are distributed among the Customer and the Third party keeping the CSP away And Both the Third party and Customer can interconnect In accessing the data Which was preserved by the Customer in CSP, which answers the data security problem in an robust approach.

A. Core Concepts

This study proposes An Adopted Secured Business Framework in the Cloud Environment. The concept is based on separating the storage and encryption/decryption of user data, as shown in Fig. 3. In this business model, Encryption/Decryption as a Service and Storage as a Service (SaaS) are not provided by a single operator. In addition, the SaaS provider may not store unencrypted user data and, once the provider of Encryption/Decryption as a Service has finished encrypting the user data and handed it off to an application (e.g. a CRM system), the encryption/decryption system must delete all encrypted and decrypted user data.

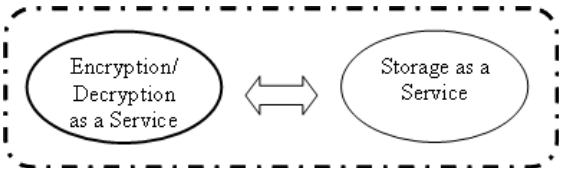


Figure 3. Encryption/Decryption as an independent service

The concept of dividing authority is often applied in business management. For example, responsibility for a company's finances is divided between the accountant and cashier. In business operations, the accountant is responsible for keeping accounts, while the cashier is responsible for making payments. By keeping these two functions separate, the company can prevent the accountant from falsifying accounts and embezzling corporate funds. Official documents frequently need to be stamped with two seals (i.e., the corporate seal and the legal representative's seal), thus preventing a staff member from abusing his position to issue fake documents, and these seals are normally entrusted to two different people. These examples of the division of authority are designed to avoid a concentration of power which could raise operational risks.

In a cloud computing environment, the user normally uses cloud services with specific functions, e.g., Salesforce.com's CRM service [15], SAP's ERP services [16], etc. Data generated while using these services is then stored on storage facilities on the cloud service. This study emphasizes the addition of an independent encryption/decryption cloud service to this type of business model, with the result that two service providers split responsibility for data storage and data encryption/decryption.

To illustrate the concept of our proposed business model, Fig. 4 presents an example in which the user 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).

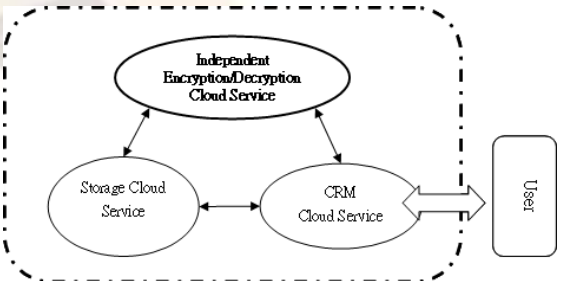


Figure 4. Business model concept integrating separate cloud services for data encryption/decryption, CRM and storage

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 that Encryption/Decryption Cloud Services must be provided independently by a separate provider.

B. Operating examples of the Encryption/Decryption as a Separate Cloud Service Business Model

This section presents a CRM application service as an example of the new business model.

After the user logs into the CRM system, if the CRM Service System requires any client information, it will execute a Data Retrieval Program. When this data needs to be saved, it will execute a Data Storage Program. The Data Retrieval Program is illustrated in Fig. 5 and is explained below.

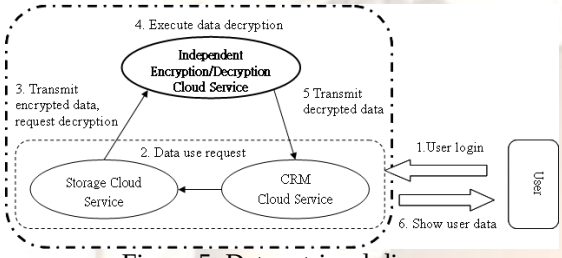


Figure 5. Data retrieval diagram

When a user wants to access the CRM Cloud Service, he must first execute the Login Program as shown in Step 1. This step can use current e-commerce or other services which have already securely verified the user's registration, such as symmetric key-based challenge and reply login verification, or through a One-Time Password.

After the user's login has been successfully verified, if the CRM Service System requires client information from the user, it sends a request for information to the Storage Service System, as shown in Step 2. In this step, the CRM Service System transmits the user ID to the Storage Service System where it searches for the user's data. This data is encrypted so, once found, a request must be sent to the Encryption/Decryption
Service System along with the user ID Step 3 shows the Storage Service System executing the transmission of encrypted client data and the user ID to the Encryption/Decryption Service System.

Since the Encryption/Decryption Service System can serve multiple users and the encryption/decryption for each user's data requires a different key, therefore each user's unique ID and keys are stored together. Therefore, in Step 4, the
Encryption/Decryption Service System uses the received user ID to index the user's data decryption key, which is then used to decrypt the received data. Using the correct decryption key to decrypt the data is critical to restoring the data to its original state.

After the Encryption/Decryption Service System has decrypted the client's data, in Step 5 the decrypted client data is provided to the CRM Service System which then displays the client data to the user in Step 6, completing the Data Retrieval Program. Prior to sending the decrypted client data, the Encryption/Decryption Service System and the CRM Service System can establish a secure data transmission channel (e.g., a Secure Sockets Layer connection) to securely transmit the decrypted client data. After the decrypted client data is sent, the Encryption/Decryption Service System is not allowed to retain the decrypted data and any unencrypted data must be deleted to prevent the encrypted data and the decryption key from being stored in the same system. This is a critical factor in ensuring the privacy of user data.

The above-mentioned Data Retrieval Program requires the collaboration of three different cloud service systems. Different methods of system collaboration are already supported by mature technologies, including two systems based on Universal Description Discovery and Integration (UDDI), Web Service Description Language (WSDL), and Simple Object Access Protocol (SOAP) to use Web Services or transmit Extensible Markup Language (XML) formatted data [17].

Next, we describe the Data Storage Program, as shown in Fig. 6. This program also involves the collaboration of three cloud service systems: CRM Service System, Encryption/Decryption Service System, and Storage Service System.

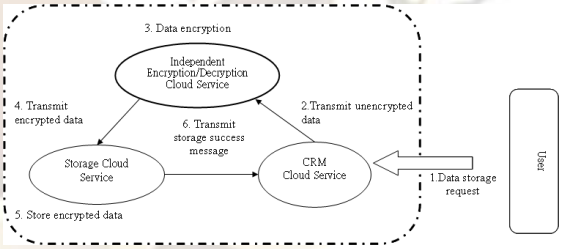


Figure 6. Data storage diagram

Step 1 of Fig. 6 shows the client sending a Data Storage Request to the CRM Service System which then initiates the Data Storage Program, requesting data encryption from the Encryption/Decryption Service System as shown in Step 2. In Step 2, the CRM Service System and the
Encryption/Decryption Service System establish a secure data transfer channel to transmit the user ID and the data requiring storage from the CRM Service System to the Encryption/Decryption Service System.

As the encryption of data from different users requires different keys, in Step 3 the

Encryption/Decryption Service System initiates data encryption, which involves using the received user ID to index the user's encryption key which is then used to encrypt the received data.

Following this study's emphasis on the principle of divided authority, once the client data is encrypted by the Encryption/Decryption Service System it must be transferred to the Storage Service System where the user ID and encrypted data are stored together. Therefore, when the Encryption/Decryption Service System executes Step 4, it must transfer the user ID and encrypted client data to the Storage Service System. Step 5 shows the Storage Service System receiving the user ID paired with the data for storage. In this business model, the following the completion of Step 4 at the Encryption/Decryption Service System, all unencrypted and decrypted user data must be deleted.

Step 6, the final step of the Data Storage Program, transmits a Data Storage Complete message from the Storage Service System to the CRM Service System, at which point the CRM
Service System may confirm that the client data has been stored. If it doesn't receive a Data Storage Complete message, it can re-initiate the Data Storage Program or, after a given period of time, proceed with exceptional situation handling.

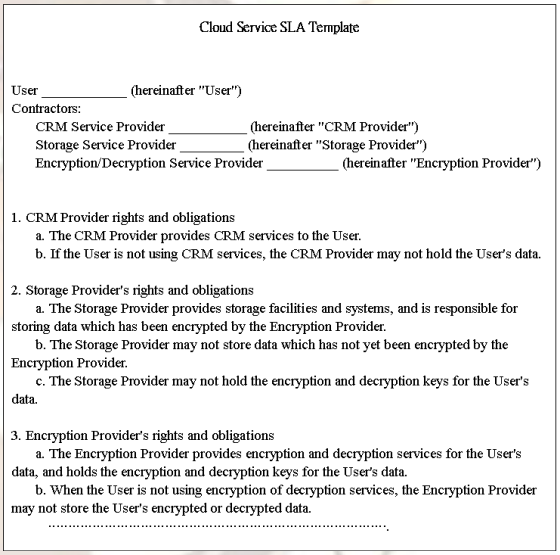
In the above example, the user's goal in logging into the CRM Service System is possibly to maintain part of the client data, thus the system design must take data maintenance into consideration. Feasible design methods include matching the encrypted client data with the corresponding user ID and client ID, thus allowing for the indexing of the user ID to obtain the corresponding client data. Then the client ID can be used to index the client data the user wishes to maintain. Considering the massive amount of client data, search efficiency could be improved by combining the user ID and client ID to form a combined ID used for searching for a specific client's data.

In the new business model, multiple cloud service operators jointly serve their clients through existing information technologies including various application systems such as ERP, accounting software, portfolio selection and financial operations which may require the user ID to be combined with other IDs for indexing stored or retrieved data. In addition, the foregoing description of the two systems can use Web Service related technology to achieve operational synergies and data exchange goals. These technologies can consider open international standards including the World Wide Web Consortium's (W3C) published Web Service, UDDI, WSDL and SOAP standard documentation.

C. Recommended Service Level Agreement Content

The above-mentioned example 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 users use the service. Unlike conventional Service Level Agreements (SLA), any SLA between the user 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 of a CRM Cloud Service includes a template for a multi-party SLA for the user, CRM operator, encryption/decryption service operator, storage service operator. The content is based on policies for ensuring data privacy, as shown in Fig. 7.



Cloud Service SLA Template

User _____ (hereinafter "User")
Contractors:
CRM Service Provider _____ (hereinafter "CRM Provider")
Storage Service Provider _____ (hereinafter "Storage Provider")
Encryption/Decryption Service Provider _____ (hereinafter "Encryption Provider")

1. CRM Provider rights and obligations
a. The CRM Provider provides CRM services to the User.
b. If the User is not using CRM services, the CRM Provider may not hold the User's data.

2. Storage Provider's rights and obligations
a. The Storage Provider provides storage facilities and systems, and is responsible for storing data which has been encrypted by the Encryption Provider.
b. The Storage Provider may not store data which has not yet been encrypted by the Encryption Provider.
c. The Storage Provider may not hold the encryption and decryption keys for the User's data.

3. Encryption Provider's rights and obligations
a. The Encryption Provider provides encryption and decryption services for the User's data, and holds the encryption and decryption keys for the User's data.
b. When the User is not using encryption of decryption services, the Encryption Provider may not store the User's encrypted or decrypted data.

Figure 7. Cloud services SLA template
(Based on policies to ensure data privacy)

IV. BENEFIT ANALYSIS AND DISCUSSION

For the Above Mentioned Problem, A third party provides an SAAS model Security Software which will be responsible for the Data integrity and adoption of the security in the hands of data owner. It will make a great transformation in cloud security environment for both the benefits of Cloud service provider and the Customer.

Benefits of the Cloud Service Provider:

- Increases the data security Reliability
- Increase in Confidence over Cloud service Provider
- Minimize the data security Job
- Increases in the productivity

Benefits of the Customer:

- Security is in the hands of Customer
- Holds the keys for accessing the data
- High Privacy preserved System

Cloud computing environments include three types of service: infrastructure, platform and software. To the user, cloud computing virtualizes resources and, to access services, the user only requires a means of accessing the Internet, e.g., a smart phone or PDA, or even a Smart Card or other active smart chip, thus reducing purchasing and maintenance costs for software and hardware. Because key industrial data is stored on the service provider's equipment, the service provider must protect the user's data, for example by encrypting the user's data prior to storage. However, this leaves the service provider's high-privilege internal staff (e.g., system administrators) with access to both the Decryption Key and the user's encrypted data, exposing the user's data to risk of potential disclosure.

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 An Adopted Secured Business Framework in the Cloud Environment, emphasizing that authorization for the storage and encryption/decryption of user data must be vested with two different service providers. The privileges of Storage as Service provider include storing user data which has already been encrypted through an Encryption/Decryption Service System, but does not allow this service provider access to the Decryption Key or allow for the storage of decrypted data. 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.

After establishing "Independent Encryption/Decryption Services" in cloud computing environments, users of cloud computing services (e.g., CRM, ERP, etc.) will use the services of at least two cloud computing service providers, so agreements between these service providers are required to establish a model for cooperation and division of responsibilities in providing a common service to clients. This study provides a draft of a multi-signatory Service Level Agreement (SLA) in which the signatories can include cloud computing rental users, application service providers, encryption/decryption service providers, storage service providers, etc., with content including the rights and obligations between operators and also includes data security policies between each operator and clients.

The core concept of this study is consistent with division of management authority to reduce operational risk, thus avoiding the risk of wrongful disclosure of user data.

REFERENCES

[1] Gill, A.Q.; Bunker, D. Dependable, Autonomic and Secure Computing (DASC), 2011, pp. 760-767.

[2] Hongxin Hu; Gail-Joon Ahn; Kulkarni, K. Dependable and Secure Computing, IEEE Transactions on Volume: 9, Issue: 3, 2012, pp. 318-331.

[3] M. Baker, R. Buyya, and D. Laforenza, "Grids and grid technologies for wide-area distributed computing," International Journal of Software: Practice and Experience, vol.32, pp. 1437-1466, 2002.

[4] B. R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[5] R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.

[6] R. Buyya, 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.

[7] L. M. Vaquero, L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

[8] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W. Michalk, and J. Stößer, "Cloud computing – a classification, business models, and research directions," Business & Information Systems Engineering (BISE), vol. 1, no. 5, pp. 391-399, 2009.

[9] N. Hawthorn, "Finding security in the cloud," Computer Fraud & Security, vol. 2009, issue 10, pp. 19-20, October 2009.

[10] A. Parakh and S. Kak, "Online data storage using implicit security", Information

Sciences, vol. 179, issue 19, pp. 3323-3333, September 2009.

[11] 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.

[12] V. Miller, "Uses of elliptic curves in cryptography," Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986.

[13] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.

[14] A. Elgohary, T. S. Sobh, and M. Zaki, "Design of an enhancement for SSL/TLS protocols," Computers & Security, vol. 25, no. 4, pp. 297-306, June 2006.

[15] Salesforce.com, Inc., "Force.com platform," Retrieved Dec. 2009, from http://www.salesforce.com/tw/

[16] SAP AG., "SAP services: maximize your success," Retrieved Jan. 2010, from http://www.sap.com/services/index.epx

[17] D. Benslimane, S. Dustdar, and A. Sheth, "Services mashups: the new generation of web applications". IEEE Internet Computing, vol. 12, no.5, pp. 13–15, 2008.