ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 3, May 2012

A Trade Model for Cloud Computing Based on Isolating Cipher text and Decoding Services and Storage

P. Murali Krishna,
M. Tech, Department of CSE,
Audisankara College of Engg & Technology,
Gudur, murali2080@gmail.com

Prof C.Rajendra,
HOD, Department of CSE,
Audisankara College of Engg & Technology,
Gudur, srirajendra.c@gmail.com

***Abstract*— Enterprises habitually amass information in internal storage and set up firewalls to defend against intruders to access the information. The enterprises also stabilize data access agendas to avert insiders to expose the records without permission. In cloud, the information will be kept in databases, which are maintained by the service providers. The providers must have a possible way to guard their consumer's data, particularly to avert the information from expose by unauthorized insiders. Storing the information in encrypted type is a general technique of information privacy protection. If a cloud system is liable for multi tasking procedures on storage and encryption/decryption of records, the system executives may concurrently attain encrypted data and decryption keys. This situation drags the attention of executives to access the information without permissions and poses threat to data privacy.**

As a explanation, this paper proposes Trade model for cloud computing based on isolating Ciphertext and decoding services and storage.In addition, Trade modeling projected for two responsibilities, one is information storage system should not store information in plaintext, and second is information ciphertext and decoding should delete all records upon the computation on ciphertext or decoding is complete.To exemplify the above proposed model we taken Customer Relationship Management service as example. According to the core concept of the proposed Trade model the service uses three cloud structures, together with an encryption and decryption structure, a storage system, and a CRM application. One service executive provides the encryption and decryption system while remain executives drive the storage and application systems.

***Keywords*- Trade model; cloud computing; cloud ciphertext and decoding.**

I. INTRODUCTION

In latest years, cloud computing has develop into a major topic in the global technology industry. The enthusiasm embrace Google's research venture for building an Blue Print to support research desires of top-tier American universities. Weiss find that cloud computing services involve a number of vacant computing technologies [1], such as service-oriented efficacy computing [2],grid computing with bulky amount of computing resources [3],and provide a data centers for data storage services.

Prior to the implement of the theory of cloud computing, confidential industrial records was stored inside on storage media, confined by security measures as well as firewalls to avert external access to the records and together with organizational regulations to forbid not permitted internal access. In the cloud computing environment, storage service providers should have in place data protection practices to ensure that their user's data is safe from illegal right to use and disclosure. Additional prominently, the convention and measures for preventing advantaged users such as system

In a cloud computing environment, the service substance presented by service providers can be used to according to the requirements of the user For example, the candidate can request different amounts of storage, communication speeds, levels of data encryption and additional services. In addition to defining the service things, the bond normally also notes the time, quality and performance necessities provided with the service. Normally, these service agreements are referred to as Service Level Agreements (SLA). By signing an SLA, the user prove that he has inherent and approved to the stuffing of the importance service, and agrees with the user's data confidentiality and security policies

A normal approach to care for user data is that user data is encrypted earlier than it is stored. In a cloud computing environment, a user's data can in addition be stored subsequent additional encryption, but if the storage and encryption of a known user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and official staff) can use their decryption keys and domestic access rights to access user data. From the user's point of view, this could put his stored data at risk of unauthorized disclosure.

Creating client belief through the safety of user's data content is the key to the common acceptance of the cloud computing. This study proposes a trade reproduction for cloud computing based on the thought of using a divide encryption and decryption service. In the model, data storage and decryption of client data are provided independently, by two different providers. In addition, those working with the data storage organization will have no right to use to decrypted client data, and those working with client data encryption and decryption will erase all encrypted and decrypted client data later than transferring the encrypted data to the system of the data storage service provider.

Under the business model planned in this gain knowledge of, the data storage cloud system provider is approved to store the user's encrypted data, but does not have right of entry to the Decryption Key. Thus, the storage system can only regain encrypted client data, but is not capable to decrypt it. The cloud computing system responsible for encrypting client data has ability over all encryption keys required for data encryption but, given that the encryption contributor does not store the user's data, internal negligence of the decryption keys still poses no risk of illegal admission of the user's data.

Given that encryption is a self-regulating cloud computing service, a only one of its kind feature of the business model is that different services are provided by several operators. For example, the Encryption as a Service provider and the "Storage as a Service" provider help to provide a Cloud

Storage System with valuable data protection. This study provides a summary SLA for this form of trade model of combining various providers in a single service, which can start the support model between operators and the division of responsibility for the services they mutually provide to the user.

II. LITERATURE REVIEW

A. Origin and definition of cloud computing

The Internet began to develop fast in the 1990s and the progressively more complicated network communications and increased bandwidth developed in recent years has significantly improved the firmness of various application services available to users through the Internet, thus marking the foundation of cloud computing network services. Cloud computing services use the Internet as a broadcast medium and convert in order 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 primary consequence lies in allowing the client to access working out resources through the Internet, as shown in Fig. 1. Some scholars find cloud computing parallel to grid computing [3], but some also find similarities to utilities such as water and electrical power and refer to it as usefulness computing [2]. Because the use of resources can be autonomously familiar, it is also sometimes referred to *as autonomic computing* ***[5].***

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service. The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowchart and diagrams.

A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing.

In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere.

Key benefits of utilizing a cloud platform for developing and deploying applications include the potential for faster, less expensive development projects, increased application scalability and development projects that produce more given the same time and budget. Just as with traditional application development, requirements are key when looking toward a future in cloud computing.

The feature contains many explanations of cloud computing [6]. After compiling intellectual definitions of cloud computing, Vaquero, Rodero-Merino, Caceres, and Lindner suggested that cloud computing could be defined as the combination of practical property according to user necessities, flexibly combining assets including hardware, development platforms and a variety of applications to create services [7]. The individual features of cloud computing include the storage of user data in the cloud and the lack of any necessitate for software installation on the end user. As long as the client is able to attach to the Internet, all of the hardware assets in the cloud can be used as client-side communications. Commonly talking, cloud computing applications are demand-driven, provided that different services according to client necessities and service providers charge by metered time, instances of use, or defined period

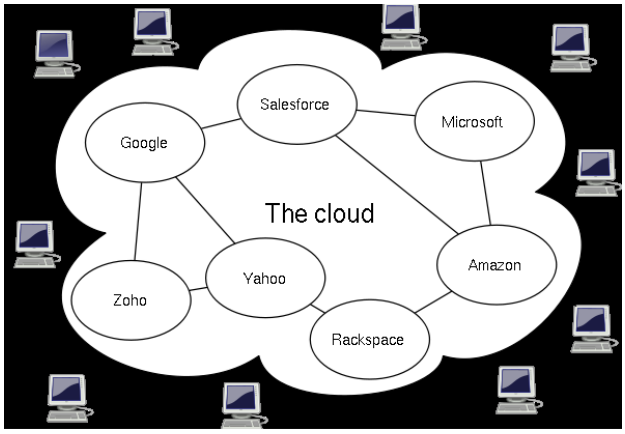


Figure 1. Cloud computing concept map

B. Cloud computing trade models

The hardware and structural design necessary for as long as cloud computing environment services are 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, Windows NT) is the platform for the operations of the basic communications, and text processing software such as MSWord and Excel are application services which run on the platform.

In this cloud services architecture these are mainly divided in to three levels: infrastructure, platform and application software. 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 possessions to execute calculations and access storage media and other equipment to store data.

Construction of a cloud computing submission as a service requires infrastructure, platform and application software which can be obtained from a single contributor or from different service providers. If the proceeds for cloud services mainly comes from charging for infrastructure, this trade model can be referred to as Infrastructure as a Service (IaaS). If proceeds comes primarily from charging for the platform, the trade model can be referred to as Platform as a Service (PaaS). If proceeds primarily comes from charging for applications or an operating system, the trade model can be referred to as Software as a Service (SaaS).

Summarizing existing cloud services, Weihardt et al.

proposed a holistic trade model framework [8], as shown in Fig. 2.

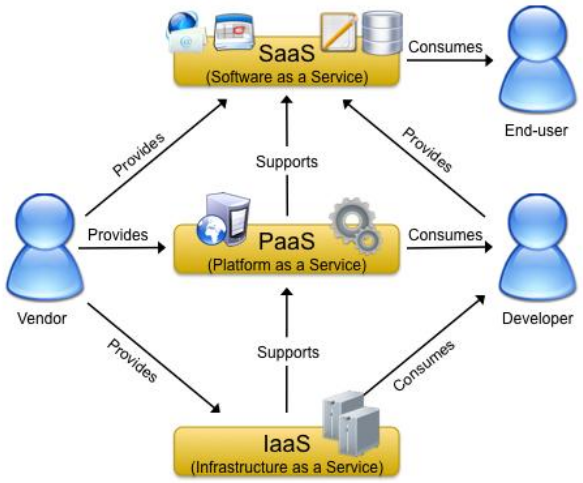


Figure2. Cloud computing trade operations structure

Fig. 2 presents a hierarchical structure, with Platform as a Service as the value-added communications service. The submission is built on the communications 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 tools used for trade operations can be leased from a single service provider along with the application, and the related trade data can be stored on tools provided by the same service contributor. This type of collection can help a company save on hardware and software infrastructure expenses, but storing the company's data on the service provider's tool raises the possibility that important trade information may be offensively disclosed to others.

Some researchers have recommended that user data stored on a service-provider's tool must be encrypted. Encrypting data earlier to storage is a frequent method of data protection, and service providers may be able to build firewalls to make sure that the decryption keys associated with encrypted user data are not visible to unauthorized users. However, if the decryption key and the encrypted data are seized by the same service provider, it raises the chance that high-level administrators within the service provider would have right of entry to both the decryption key and the encrypted data, thus presenting a risk for the illegal disclosure of the user data.

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

Common methods for defending user data include encryption prior to storage, user confirmation procedures prior to storage or recovery, and building secure channels for data broadcast. These protection methods normally necessitate cryptography algorithms and digital signature techniques, as explained below:

Common data encryption methods comprise 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 (ECC) . Commonly talking, symmetric cryptography is more competent, and is suitable for encrypting bulky volumes of data. Asymmetric cryptography wants more working out time and is used for the decryption keys wants for symmetric cryptography.

The use of passwords as a validation process is more familiar to common clients, but messages sent by the client are in danger to covert recording by hackers who can then use the data in the message to log into the service as the client. In more highly developed authentication systems, the system side will generate a random number to send the client a challenge message, requesting the client to transmit an encrypted response message in reply to the challenge message, thus authenticating that the client has the correct encryption key. Without this key, the consumer will not be allowed right to use. In the process of challenge and response the user's encrypted key uses the client's password to translate a derived value and. In this series, each message 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) verification system differs from most peoples' conception of a password. Most people identify with a password to be a password chosen by the user to be meaningful, and can be used again and again. The importance of OTP, however is the single-use nature of the password.

After receiving conformation from the user, the system side must create a secure communication channel to exchange information with the user. The Secure Sockets Layer (SSL) is a general method of building secure channels, primarily usingRSA encryption to broadcast the secret keys needed for the both sides to encrypt and decrypt data transmitted between them

When using cryptographic technology to defend user data, the keys used for encryption and decryption of that data must be strongly stored. In particular, cloud computing service providers must have specific methods for constraining domestic system management personnel to put a stop to 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 clarify how special license users are prevented from unacceptably accessing user data.

Kandukuri, Paturi and Rakshit offer six recommendations for SLA content [4], including

1) special privilege user data right of entry must be restricted to prevent unauthorized storage or retrieval,
2) cloud computing services must comply with significant laws,
3) clients data must be properly stored and encrypted,
4) a reset method must be provided in case of service disorder or system crash,
5) service must be sustainable and definite against service discontinuation due to change or termination

of the provider and

6) If cloud computing services are used for against the law purposes, the provider must be able to provide records to assist with investigations.

III A TRADE MODEL FOR CLOUD COMPUTING BASED ON ISOLATING CIPHERTEXT AND DECODING SERVICES AND STORAGE

A. Core Concepts

These learn proposes Trade Model for Cloud Computing Based on a Isolating Ciphertext, Decoding Service and storage. The thought is based on separating the storage and encryption/decryption of user data, as shown in Fig. 3. In this trade model, Encryption/Decryption as a Service and Storage as a Service are not provided by a single operator. In addition, 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 submission the encryption/decryption system must delete all encrypted and decrypted user's data.

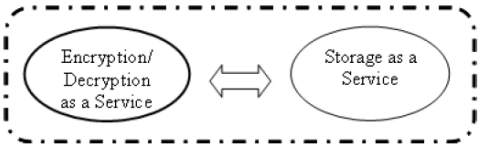


Figure 3. Encryption/Decryption as an independent service

The thought of dividing last word is often applied in trade management. For example, liability for a company's assets is divided between the accountant and cashier. In trade operations, the accountant is responsible for keeping accounts, while the cashier is conscientious for making payments.

By keeping these two functions separate, the company can prevent the accountant from falsifying accounts and embezzling business 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 forged documents, and these seals are normally entrusted to two different people. These examples of the division of authority are designed to avoid absorption of power which could move up prepared risks.

In a cloud computing environment, the user generally uses cloud services with explicit functions, e.g., CRM service, SAP's ERP services, etc. Data generated while using these services is then stored on storage conveniences on the cloud service. This study emphasize the addition of an independent encryption/decryption cloud service to this type of trade model, with the result that two service providers split responsibility for data storage and data encryption/decryption.

To demonstrate the concept of our proposed trade model, Fig. 4 presents an example in which the user uses separate cloud services for CRM, storage and encryption/decryption. According to the client's needs, CRM Cloud Services could be swapped for other function-specific application services

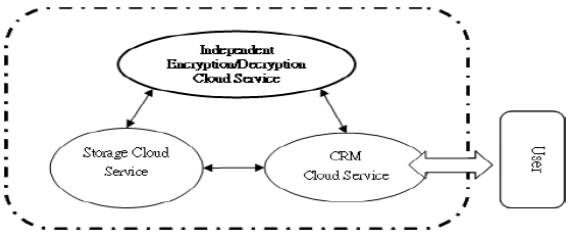


Figure 4. Trade model concept integration separate cloud services for data encryption/decryption. CRM and storage.

Prior to the appearance of an importance on the liberty of encryption/decryption services, CRM, ERP and other cloud services would concurrently provide their users with storage services. This study emphasize that Encryption/Decryption Cloud Services must be provided independently by a separate provider. The above diagram show the how the separate the information , in the form of encryption and decryption. The CRM cloud service that application enter the information that information send to cloud storage in the form of encryption and decryption.

.

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

This section presents a CRM application service example of the new trade model..

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

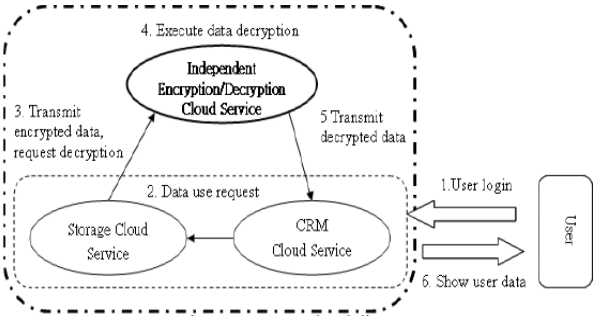


Figure4. Data retrieval diagram

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.

pace 1 of Fig. 6 shows the consumer distribution a information storage space Request to the CRM Service System which then initiates the information storage space Program, requesting data encryption from the Encryption/Decryption Service System as shown in pace 2. In Step 2, the CRM Service System and the Encryption/Decryption Service System set up protected information transmit channel to transmit the user ID and the data requiring storage from the CRM Service System to the Encryption/Decryption Service System.

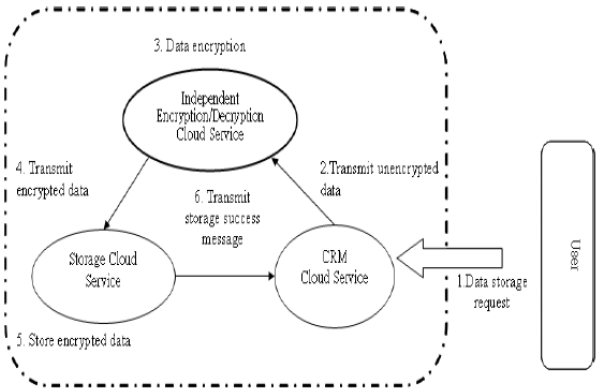


Figure 6. Data storage diagram

As the encryption of data from dissimilar users requires dissimilar keys, in pace the Encryption/Decryption Service System initiates data encryption, which involves using the conventional user ID to directory the user's encryption key which is then used to encrypt the expected information.

The Above figure 6 indicate the data storage diagram, how to store the client information, for example user interact the CRM Application the send the data in encrypted form to CRM cloud service. 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.

During the above example, the user's objective in logging into the CRM Service System is probably to maintain part of the client data, thus the system design must take data maintenance into consideration. practicable intend 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. In view of 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.

Within the new trade model, several cloud service operators together 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 previous explanation 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 together with the World Wide Web Consortium's (W3C) published Web Service, UDDI, WSDL and SOAP standard documentation.

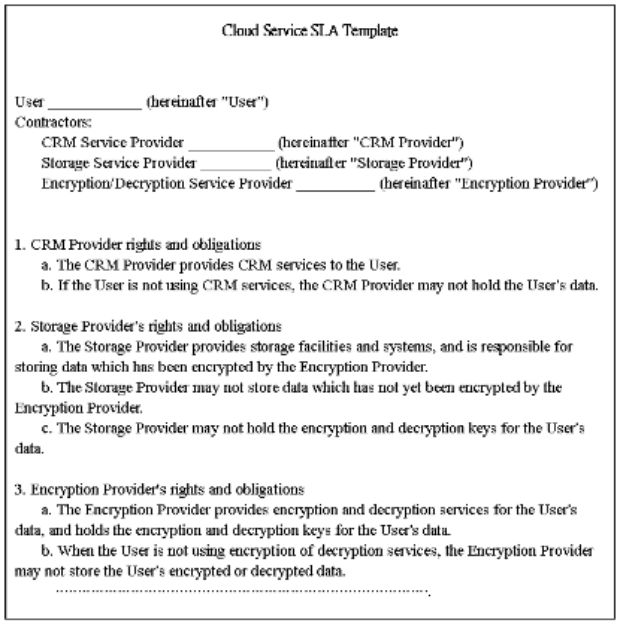
C. Recommended Service Level Agreement Content

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.

The use of passwords as a validation process is more familiar to common clients, but messages sent by the client are in danger to covert recording by hackers who can then use the data in the message to log into the service as the client. In more highly developed authentication systems, the system side will generate a random number to send the client a challenge message, requesting the client to transmit an encrypted response message in reply to the challenge message, thus authenticating that the client has the correct encryption key. Without this key, the consumer will not be allowed right to use. In the process of challenge and response the user's encrypted key uses the client's password to translate a derived value and. In this series, each message 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) verification system differs from most peoples' conception of a password



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)

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.

Common methods for defending user data include encryption prior to storage, user confirmation procedures prior tostorage or recovery, and building secure channels for data broadcast. These protection methods normally necessitate cryptography algorithms and digital signature techniques. In a cloud computing environment, the user generally uses cloud services with explicit functions, e.g., CRM service, SAP's ERP services, etc. Data generated while using these services is then stored on storage conveniences on the cloud service. This study emphasize the addition of an independent encryption/decryption cloud service to this type of trade model, with the result that two service providers split responsibility for data storage and data encryption/decryption.

IV.BENEFIT ANALYSIS AND DISCUSSION

Cloud computing environments contain three types of overhaul communications, platform and software. To the user, cloud computing virtualizes resources and, to access services, the consumer only requires a resources 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.

On the other hand this vegetation the overhaul provider's high-privilege inside 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.

Used for cloud computing to spread, users must have a high level of trust in the methods by which service providers protect their data. This lesson proposes a trade demonstration for Cloud Computing Based on a divide Encryption and Decryption Service, emphasizing that agreement for the storage space and encryption/decryption of user information must be vested with two dissimilar service providers. The person human rights of storage space 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 human rights 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 present is no approach 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 consumer information might be improperly disclosed.

After establishing "sovereign Encryption/Decryption Services" in cloud computing environments, users of cloud computing services 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 assistance and division of responsibilities in providing a common service to user's.

This learning provides a draft of a multi-signatory Service Level Agreement (SLA) in which the signatories can take in cloud computing leasing users, request service providers, encryption/decryption service providers, storage service providers, etc., with comfortable including the rights and obligations between operators and also includes data security policies between each operative and clients.

The core concept of this study is reliable with division of managing authority to reduce operational risk, thus avoiding the risk of wrongful confession of user data.

REFERENCES

[1] [1] A. Weiss, "Computing in the clouds", netWorker, vol. 11, no. 4, pp. 16- 25, December 2007.
[2] C. S. Yeo, S. Venugopal, X. Chu, and R. Buyya, "Autonomic metered pricing for a utility computing service", Future Generation Computer Systems, vol. 26, issue 8, pp. 1368-1380, October 2010.
[3] M. Baker, R. Buyya, and D. Laforenza, "Grids and grid technologies for wide-area distributed computing," International of Software:Practice and Experience, vol.32, pp. 1437-1466, 2002.
[4] [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.