CRM System in Cloud Computing with Different Service Providers

Mrs.I.Golda Selia[1], S.K. Madhumithaa[2]
[1]Asst.Professor/Dept of IT [2]M.Tech Information Technology
DR.M.G.R .Educational and Research Institute
University Chennai-95 India

Abstract
Enterprises always store the data in the internal storage of the organization itself. Especially in a Customer Relationship management system all the data of the customers will be stored in the internal storage itself. But the main disadvantage in the storage of the data is there may be hackers in the administrator side and they may get the information of the customer because the application of CRM system, encryption/decryption and storage of the data is done in the same service provider in a cloud computing environment. To avoid this kind of challenges cloud computing provides three different service providers for the security of the data in a cloud computing. This paper discusses about the main concept of providing the different service providers and their advantages and the techniques involves in providing the different service providers in a cloud computing environment.

Keywords - cloud computing, encryption and decryption, CRM, cloud services, service provider.

I. Introduction
Cloud Computing is a emerging technology in recent years. Weiss noted that there are several existing techniques used in the cloud computing[1].

Before the development of the cloud computing generally the enterprises used to store the data in the internal storage of the organization itself. The data stored will be very confidential and even it has some security measures and it is protected from the unauthorized user. But in the cloud computing environment the storage of data is somewhere from the client workplace and the data storage and security measures will be in the service provider of the cloud computing environment.

Generally the data is stored after it is encrypted. This is for the security of the client's or user's data. In Cloud computing the user data is stored followed by the encryption of the data. But if the storage and encryption of the data is in the same service provider then there is a possibility of accessing the keys and original data by the internal staffs or by administrators of the service provider.

In this paper we proposed a model to encrypt the data in one service provider and store the data in the different service provider. So once the data is stored in the application it is get encrypted and the encrypted data will not be present in the encryption service provider. Thus the storage of the data will be in the encrypted format and the administrators and the staffs have no knowledge about the encrypted keys and the service providers of the encryption and decryption.

This paper discusses about the literature review in chapter II and CRM system with different service provider in chapter III and conclusion as IV chapter.

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.

Fig1. Cloud computing Concept

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].

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.

Fig2. Architecture of Cloud services

III. Crm System in Cloud Computing With Different Service Providers

A. Core Concepts

This study proposes CRM system in cloud computing with different service providers. 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 a CRM system, the encryption/decryption system must delete all encrypted and decrypted user data.

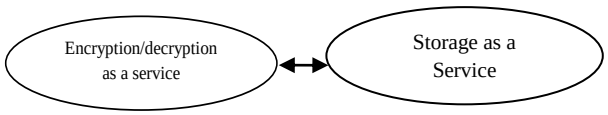

Fig3. Encryption/Decryption as an independent service

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.

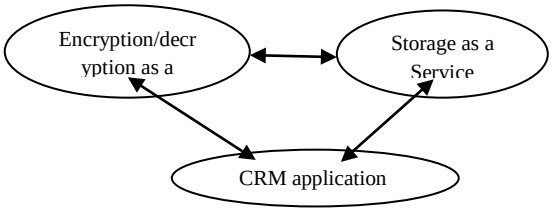

Fig4. Business model

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 discusses about a CRM application to demonstrate the separate cloud system. For example if a user wants to store an information in a CRM application, user will enter the details. The user details are entered and get stored in the CRM application then the data is encrypted and stored after getting encrypted in a separate encryption and decryption service provider. The CRM application cloud does not have any encryption keys to encrypt the data. Thus accessing of the encrypted data is thus prevented. The encrypted data stored in the cloud will be get stored in separate storage system, thus the encryption cloud server never knows about the original data. Once it is encrypted the encrypted data is stored in the Storage cloud. This is for data storage program.

The another concept is Data Retrieval Program. If a user wants to retrieve any data from the storage cloud first the user enters the unique ID provided by the CRM application. Once the ID matches it will give a request to the encryption/decryption cloud to decrypt the data.

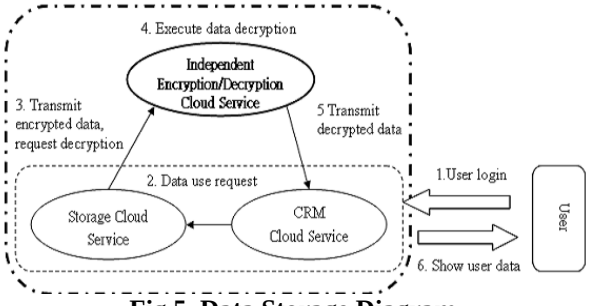

Fig 5. Data Storage Diagram

The encryption/decryption cloud will forward the request to the storage cloud. The storage cloud will send the original data to the encryption/decryption cloud, then that cloud will decrypt the original data and send it to CRM application. Then the user will retrieve the data from the application. The service providers will be separated thus protecting the data from the unauthorized users.

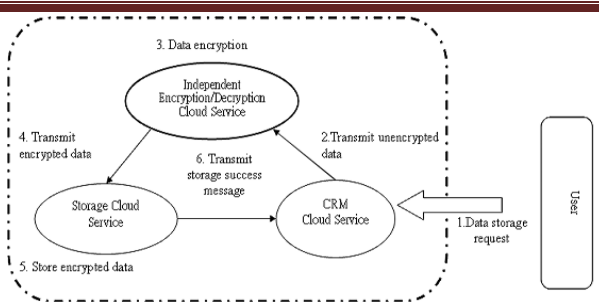

Fig6. Data retrieval Diagram

IV. Conclusion

For cloud computing to spread, users must have a high level of trust in the methods by which service providers protect their data. This study proposes a Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, emphasizing that authorization for the storage and encryption/decryption of user data must be vested with two different service providers. 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.

Future Enhancements

This paper comprises of the encryption and decryption service provider and storage provider. In future some more encryption and decryption standard may be used to encrypt the data efficiently and the storage provider quality may be increased.

References

[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 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/