Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

International Conference on Mobility in Computing- ICMiC13, Organized by Mar Baselios College of Engineering and Technology during December 17-18, 2013 at Trivandrum, Kerala, India, pg.119 – 123

SURVEY ARTICLE

A e-Contract Based Business Model for Cloud Computing

[1]Meenu Rajan, [2]Sarada B S

Department of Computer Science and Technology, Mar Baselios College of Engineering and Technology,
Trivandrum, India

[1] meenurajan77@gmail.com, [2] sarada.bs@gmail.com

***Abstract*: In cloud computing environment, enterprises usually use business model for deploying and executing their various business operations. In cloud computing business model, the communication between the storage service and encryption/decryption service may lead to unauthorized access or disclosure of user data by any internal crew or administrative hacker. In this study paper, we introduce a secure business model for cloud computing, based on separating the storage service from the encryption/decryption service. There is no communication between the storage service and the encryption/decryption service. The storage service will store only encrypted data, which is provided by the storage provider. The encryption/decryption service will encrypt/decrypt the plain user data and it is provided by the encryption/decryption service provider. After cryptographic operations, the encryption/decryption service will delete all the user data. In this proposed business model, a secure channel is deployed to preserve the integrity of messaging between the services. The communication connection establishment between the intra-cloud or inter-cloud services is provided as a trusted third party service provider. To illustrate the proposed business model, a CRM application is used.**

Keywords: Cloud Computing; Service Level Agreements; Encryption and Decryption Cloud Service; Data Privacy Protection; Security Connectivity.

I. INTRODUCTION

Cloud computing is a technology that integrates a number of computers together through a real time communication network, normally internet. It is a form of distributed computing over internet. This technology has the ability to execute various applications on different computers at the same time. The main goal of cloud computing is to achieve high performance and efficient use of shared resources. Normally, this technology is used for military and research purpose because it enables the execution of billions or trillions of computations at a time. Agility, Application Programming Interface (API), cost, virtualization, reliability, performance, security are some of the main characteristics of cloud computing.

In cloud computing, all the services are provided by the service providers. The service providers will provide services to the user based on their needs and requirements. Service providers also provide certain privacy policies for the protection of user's data. The service level agreement (SLA) will describe all the requirements for providing cloud services [4].By signing an SLA, the user agrees to the services provided by service provider and also accepts various protection policies offered by them. Six recommendations are available for SLA content [1]. Based on several fundamental models cloud computing provider offers their services as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Amazon, Jelastic, CloudBees are examples of service providers.

In cloud computing, enterprises store user data only after encryption. Encrypting the data before storage is an effective method for protecting the user's confidential data. If the encryption/decryption operations and the storage operations are provided by the same service provider, then there may be a chance for an internal crew to acquire the decryption key and the encrypted data which leads to a security issue [1]. Also there may be chance to hack the users confidential data from the communication channel during the transmission of data. To overcome these problems, we propose a business model for cloud computing by separating the encryption /decryption service from the storage service. In this model, both services are provided by two distinct service providers. There is no communication between these two service providers. The encryption and decryption service provider will perform cryptographic operations. The storage service provider will provide the storage for storing the encrypted data. No connection exists between these two service providers. A secure channel is established between the services in order to prevent hacking of user data during message transmission and the connection is provided as a service.

This paper discusses literature survey in section II, existing system in section III, proposed system in section IV and conclusion in section V.

II. LITERATURE REVIEW

1. Origin of cloud computing: In 1990's, the rapid growth of the internet and the use of sophisticated infrastructure and increase bandwidth enhanced the stability of various application services available to the user, thus marking the beginning of cloud computing. Cloud computing services use the internet as a transmission medium and transform information technology resource into services for end-users, including software services, computing platform services, development platform services, and basic infrastructure leasing. As a concept, the main significance of cloud computing lie in allowing the end users to access computation resources through the internet [3]. Some scholars suggested that cloud computing could be define as the integration of virtual resources according to user requirements, flexibly combining resources including hardware, development platforms and various applications to create services [1].

2. Security issues in cloud computing environment: SQL injection, Cross Site Scripting (XSS) attacks, DoS and DDoS attacks, Google Hacking and Forced Hacking are the various security threats in cloud computing. Avoiding the use of dynamically generated SQL in the code, finding the meta-structures used in the code, validating all user entered parameters, and removal of unwanted data and characters are few standard techniques used to detect the above mentioned threats. For an optimized cost performance ratio, a generic security framework should be worked out [3].

3. Business models in cloud computing: The services provided by the various service provides can be classified into three groups [4]. Cloud computing model has layered organisation. The architecture network required for cloud computing is almost similar to computer n/w and software [3].If the revenue for cloud service primarily comes from charging for infrastructure, this business model is referred to as "Infrastructure as a Service" (IaaS). If the revenue for cloud service primarily comes from charging for platform, this business model is referred to as "Platform as a Service" (PaaS). If the revenue for cloud service primarily comes from charging for software, this business model is referred to as Software as a service (SaaS). Weihardt et al has proposed a hierarchical holistic business framework [1].

4. Security issue in cloud communication: The intra cloud communication is secure from outside threat, but still there exists some security issues arising due to reasons like, (a) the transferred business data is visible to the cloud provider,(b) the transferred data getting snipped by neighbouring malicious instance within LAN etc. The inter cloud communication possesses high security issues as compared intra cloud communication because the business data is transferred through multiple cloud infrastructure [2].

5. Secure networking: In TCP/IP reference model, the data is transmitted from higher level to lower level. The security controls used by the application layer must be established in each application. PGP (Pretty Good Privacy) is one example for email encryption. The security controls in transport layer provide protection of data unit during the flow between the two hosts. Secure socket layer (SSL) is one protocol that provides communication security in this layer. The security control in network layer is not application specific. It provides secure network between two hosts. Data link layer provides secure communication on a specific physical link. Even though IP Sec is better than SSL, due to the managing overhead, SSL based VPN is an effective method for establishing secure connectivity channels. It can be achieved by forming virtual extranet within cloud or between clouds [2].

III. EXISTING SYSTEM

The existing business model is based on the concept of separating storage and encryption/decryption of user data [1] as shown in figure 1.

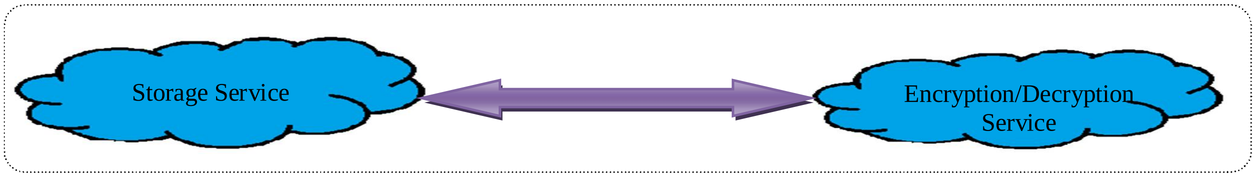

Fig 1: Separation of Storage and encryption/decryption

The security risks which arise due to both the storage service and the encryption/decryption service provided by the same service provider can be overcome by this business model. The drawbacks of this existing model is that, even though encryption/decryption service and storage services are provided by two distinct service providers, a communication link still exists between them. In this business model, the storage service stores encrypted data along with the user ID. Encryption/decryption service stores user ID along with decryption key for maintaining the accuracy. Thus the communication link between these two services causes a security issue of hacking the user data by any administrative person as depicted in figure 2. Another main issue is the secure channel between the services. The chances of hacking of user data from the communication channels are possibly high. This will also lead to secure communication issue in this existing business model.

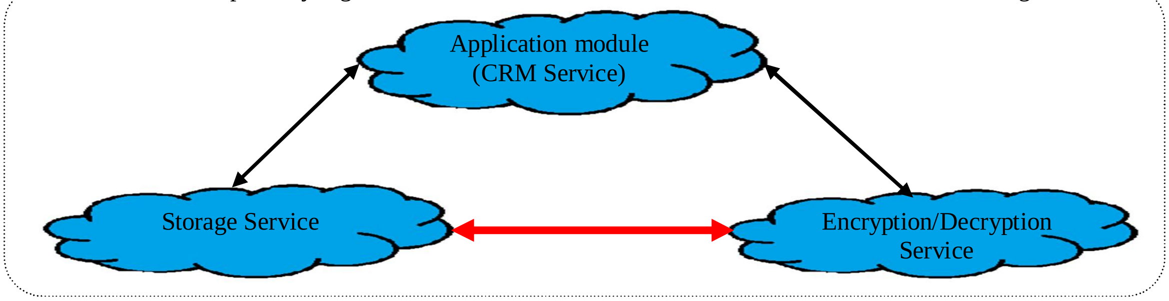
Application module (CRM Service)
Storage Service
Encryption/Decryption Service

Fig 2: Communication link between the storage service and the Encryption/Decryption service

IV. PROPOSED SYSTEM

In the proposed business model, the cryptographic service and the storage service are provided by two distinct service providers. The storage service stores only data in encrypted format. The encryption/decryption service will perform the encryption/decryption of user's plain data. Once the cryptographic operations are completed, the encryption/decryption service deletes all encrypted/decrypted user data. To illustrate the proposed business model, a CRM application is used. Various functions are specified by the providers like Salesforce.com's, CRM service, SAP's ERP services etc [1]. The conceptual illustration of the proposed business model is shown in figure 3. Three cloud services are used in this model for Storage service, CRM service and cryptographic service. As per the figure depicted, no communication link is established between the Storage service and the cryptographic service. Only the CRM cloud service will know where the encrypted data is stored and where the encryption/decryption of data is done. Thus hacking of user's confidential data by the internal crews can be prevented.

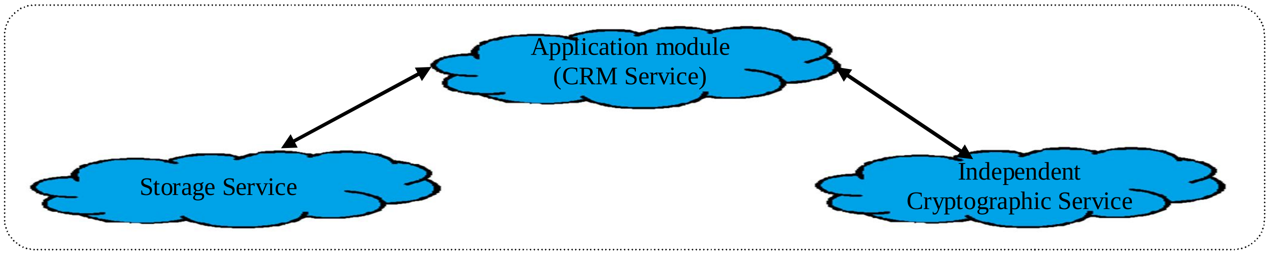
Application module (CRM Service)
Storage Service
Independent Cryptographic Service

Fig 3: Conceptual illustration of the proposed business model

In this business model, Data Retrieval program gets executed when user wants to get any client information Data Storage program gets executed when user wants to save any client information. Login process is used in order to ensure the authorised access to the CRM service. One Time Password scheme is used here. Each user is assigned a unique ID given by the CRM service for identification process. If the user wants to store any client information, the user will enter the details in CRM application. Then the CRM system will transmit the stored unencrypted user data to the encryption/decryption service for the cryptographic function. Once the cryptographic function is completed, Encryption/Decryption service deletes all the encrypted/decrypted user data. Encryption/decryption service can serve multiple users and need different keys for encryption/decryption operations. Therefore in cryptographic service, each user's unique ID and keys are stored together for maintaining the accuracy. After receiving the encrypted data, the CRM cloud service will send the encrypted data to the storage service for storing purpose. After successful storage, a success message will be displayed to the user. The steps involved in the data storage program are given in figure 4.

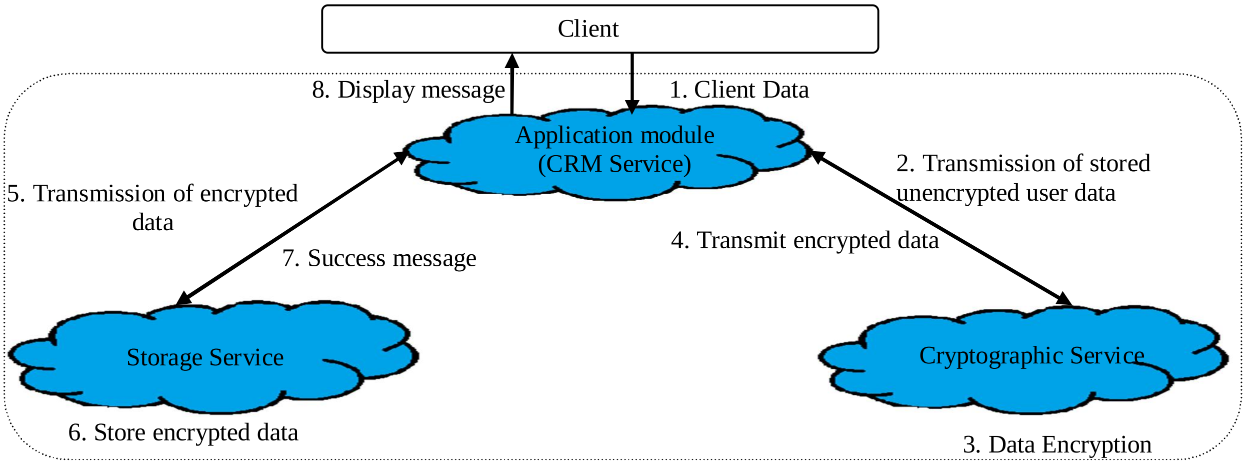
Client
8. Display message
1. Client Data
Application module (CRM Service)
5. Transmission of encrypted data
2. Transmission of stored unencrypted user data
4. Transmit encrypted data
7. Success message
Storage Service
Cryptographic Service
6. Store encrypted data
3. Data Encryption

Fig 4: Data Storage program

When user wants to retrieve any information, CRM will send a request to the storage service for data retrieval. Unique ID is transmitted to the storage service along with the request. Then the storage service searches for data based on the unique ID. Once the encrypted data is found, it will transmit the encrypted data along with the user ID to the CRM system. After receiving this data, the CRM will send the encrypted data to the cryptographic service for decryption. The cryptographic service uses the received user ID to index the decryption key for decrypting the received data. After decryption process, the decrypted data is sent to the CRM and finally displayed to the user. The steps involved in the data retrieval program are shown in figure 5. In both the data storage program and the data retrieval program, only the CRM cloud service knows where the encrypted data is stored and where the encryption/decryption operation is performed. There is no connection between the storage service and cryptographic service. Thus, unauthorised internal access to the user data is prevented.

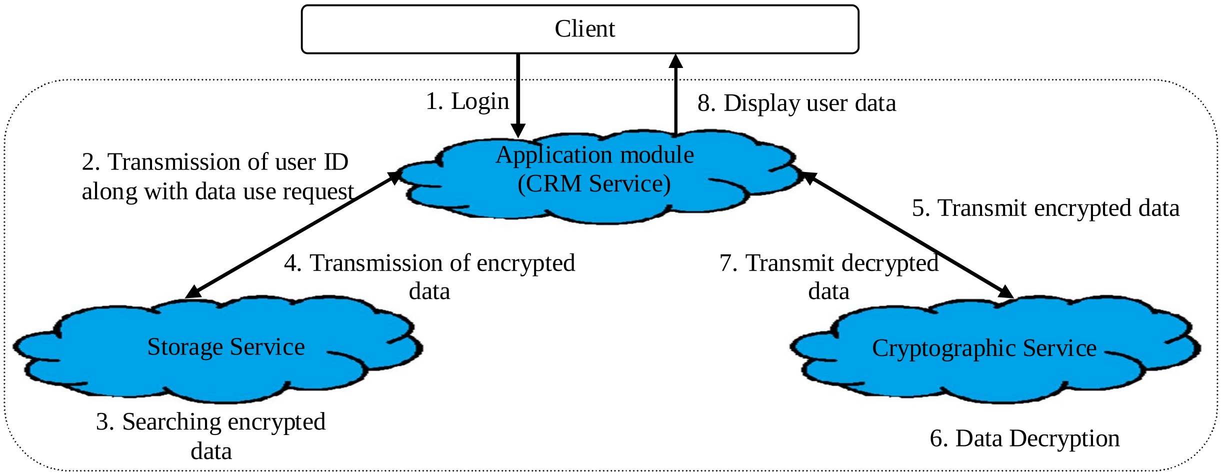
Client
1. Login
8. Display user data
Application module (CRM Service)
2. Transmission of user ID along with data use request
5. Transmit encrypted data
4. Transmission of encrypted data
7. Transmit decrypted data
Storage Service
Cryptographic Service
3. Searching encrypted data
6. Data Decryption

Fig 5: Data Retrieval Program

In this proposed business model, the collaboration of three cloud services: CRM cloud service, Storage service, Encryption/Decryption service is required. The transmission of data between the services is carried out through a secure channel. The secure connectivity service is established as a trusted third party service provider. Connectivity services will establish connections between the services based on eContract [2]. For the establishment of secure channels, the organization must subscribe to the services provided by the connectivity service. Based on the nature of collaboration, the organizations will form an eContract which will be signed by them. This eContract will specify the services that need connectivity channel of secure communication. Communication between the CRM service, storage service and the cryptographic service is carried out through the secure connectivity channel. The CRM service and cryptographic service form an eContract for establishing the secure connectivity channel between them namely, eContract 1. The storage service and CRM service form an eContract for establishing the secure connectivity channel between them namely, eContract 2. Based on eContract 1 & eContract 2, the connectivity service will provide a virtual extranet 1 and virtual extranet 2. Therefore CRM and storage service can communicate with each other within a virtual extranet 1 and CRM and encryption service can communicate with each other within extranet 2. Thus a secure channel is established between the services through a virtual extranet, as shown in figure 6. Therefore the hacking of data during transmission through the communication channel can be avoided.

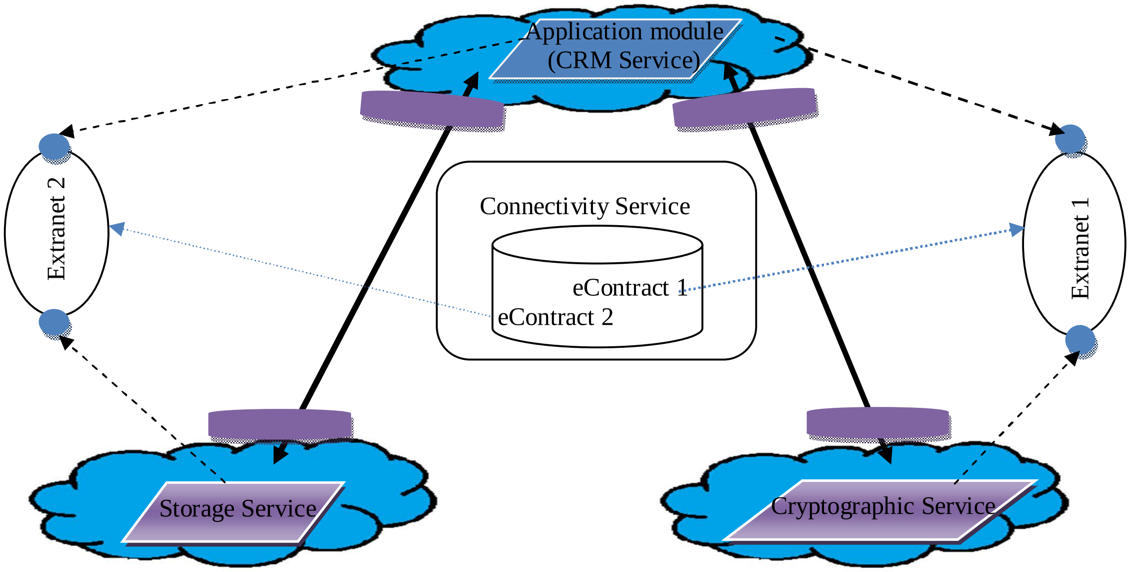

Fig 6: Business model with secure channel connectivity

V. CONCLUSION

This study paper proposes a secure business model for cloud computing based on the concept of separating encryption/decryption service from storage service, with no communication link between them. The communication between the services is carried out only through CRM cloud service. Only the CRM cloud service knows where the encryption/decryption of data is performed and the storage of data. The encryption/decryption service performs encryption/decryption and the storage service only stores encrypted data. A connectivity service is provided for establishing secure connectivity channel between the services. Connectivity services provide SSL based virtual private network for providing secure connectivity channel by forming virtual extranet within cloud or between cloud. The virtual extranet is established based on the eContract signed by the services. Thus a business model with secure connectivity channel based on complete separation between the services is proposed.

REFERENCES

[1] Jing-Jang Hwang ; Hung-Kai Chuang ; Yi-Chang Hsu ; Chien-Hsing Wu *"A Business model for cloud computing based on separate encryption and Decryption service"*, Information Science and Applications (ICISA), 2011 .

[2] Shiping Chen ; Nepal, S. ; Ren Liu "*Secure Connectivity for Intra-cloud and Inter-cloud Communication* " Parallel Processing Workshops (ICPPW), 2011 40th International Conference .

[3] A. Weiss, "*Computing in the clouds*", netWorker, vol. 11, no. 4, pp. 16-25, December 2007.

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

[5] 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.