Business Model for Cloud Computing

M. Jagapathi Babu [1], K.Madhu Sudhan Reddy [2]
[1]*Department of MCA, Srikalahastiswara Institute of Information and Management Sciences, Kapugunneri (Affiliated to S.V.University, Tirupati)*
[2]*Assistant Professor, Department of MCA, Srikalahastiswara Institute of Information and Management Sciences, Kapugunneri(Affiliated to S.V.University, Tirupati)*

Abstract- **Enterprises usually store data in internal storage and install firewalls to protect against intruders to access the data. They also standardize data access procedures to prevent insiders to disclose the information without permission. In cloud computing, the data will be stored in storage provided by service providers.**

Service providers must have a viable way to protect their clients' data, especially to prevent the data from disclosure by unauthorized insiders. Storing the data in encrypted form is a common method of information privacy protection.

If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the system administrators may simultaneously obtain encrypted data and decryption keys.

This allows them to access information without authorization and thus poses a risk to information privacy. This study proposes a business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service.

Furthermore, the party responsible for the data storage system must not store data in plaintext, and the party responsible for data encryption and encryption must delete all data upon the computation on encryption or decryption is complete.

I. INTRODUCTION

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.

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.

II. MODULES

The Modules involved are

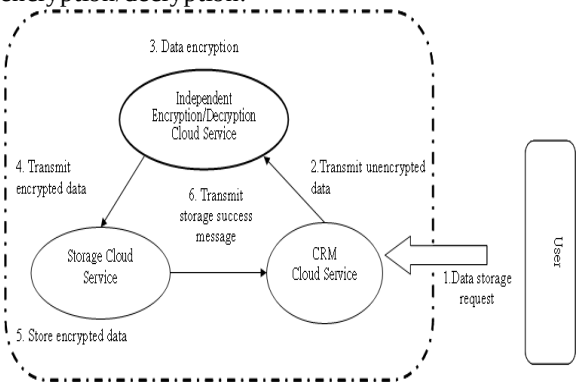
- User Registration and Control
- CRM Service
- Encryption/Decryption Service
- Accessing Storage service

User Registration and Control:

This study proposes a Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service. The concept is based on separating the storage and encryption/decryption of user data. 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. The concept of dividing authority is often applied in business management.

CRM Service:

In a cloud computing environment, the user normally uses cloud services with specific functions, e.g., salesforce.com CRM service, SAP's ERP services, 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.

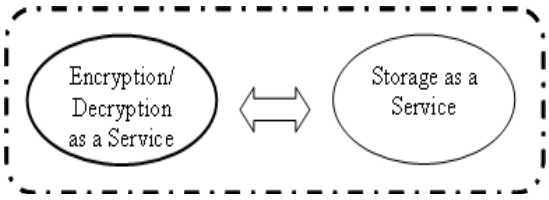


Encryption/Decryption Service:

When a user wants to access the CRM Cloud Service, he must first execute the Login Program. 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. 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. 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. 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.



Accessing Storage service:

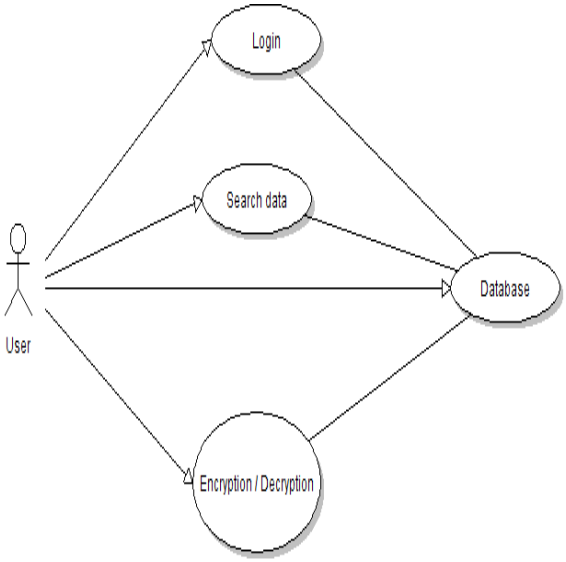
After the Encryption/Decryption Service System has decrypted the client's data, the decrypted client data is provided to the CRM Service System which then displays the client data to the user, completing the Data Retrieval Program. Prior to sending the decrypted client data, the Encryption/Decryption 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.

III. SYSTEM DESIGN

UML DIAGRAMS:

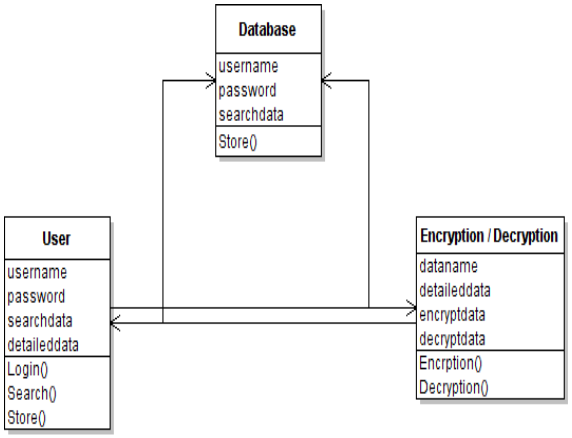
Use case Diagram

Use case diagrams are drawn to represent the functionality of the system.



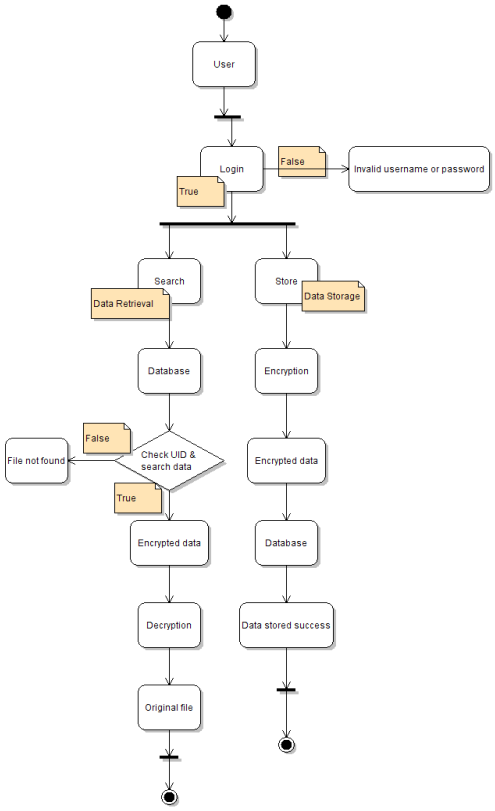
Class Diagram:

Class diagrams are used to represent the classes used in the system and their relationships.



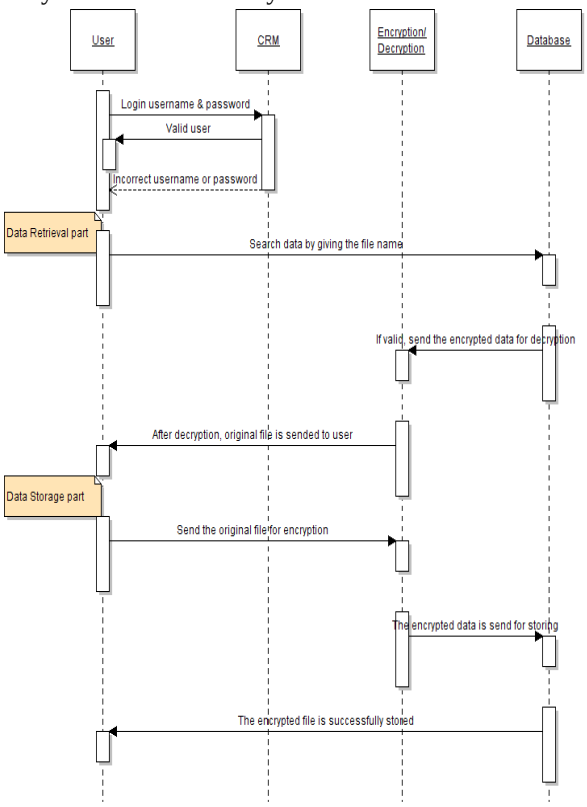
Activity Diagram:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency.



Sequence Diagram:

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.



IV. TECHNOLOGY DESCRIPTION

PHP:

PHP is a general-purpose server-side scripting language originally designed for Web development to produce dynamic Web pages. It is one of the first developed server-side scripting languages to be embedded into an HTML source document rather than calling an external file to process data. The code is interpreted by a Web server with a PHP processor module which generates the resulting Web page. It also has evolved to include a command-line interface capability and can be used in standalone graphical applications. PHP can be deployed on most Web servers and also as a standalone shell on almost every operating system and platform free of charge.

HTML:

Hyper Text Markup Language (HTML) is the main markup language for displaying web pages and other information that can be displayed in a web browser.

HTML is written in the form of HTML elements consisting of *tags* enclosed in angle brackets (like <html>), within the web page content.

MYSQL:

MySQL "My S-Q-L", officially, but also called "My Sequel") is the world's most used open source relational database management system (RDBMS) that runs as a server providing multi-user access to a number of databases. The SQL phrase stands for Structured Query Language.

Cloud-based deployment

Another deployment option is running MySQL on cloud computing platforms such as Amazon EC2. There are two common deployment models for MySQL on the cloud:

- Virtual Machine Image - cloud users can upload a machine image of their own with MySQL installed, or use a ready-made machine image with an optimized installation of MySQL on it, such as the one provided by Amazon EC2.
- MySQL as a Service - some cloud platforms offer MySQL "as a service". In this configuration, application owners do not have to install and maintain the MySQL database on their own. Instead, the database service provider takes responsibility for installing and maintaining the database, and application owners pay according to their usage.

OpenSSL:

OpenSSL is an open-source implementation of the SSL and TLS protocols. The core library, written in the C programming language, implements the basic cryptographic functions and provides various utility functions. Wrappers allowing the use of the OpenSSL library in a variety of computer languages are available.

V. SYSTEM TESTING

The main objective of software testing is to find errors. A successful testing is one that uncovers, as many as yet undiscovered errors, which helps to make the software more rugged and reliable.

Software testing is done at different levels. They are unit testing and system testing which comprises of integration testing and acceptance testing.

Unit Testing:

The purpose of unit testing is to find errors in the individual units, which could be logic-related errors. The test case can be derived from their program specification or design document. Units which cannot be tested in isolation may require the creation of small test programs known as harness.

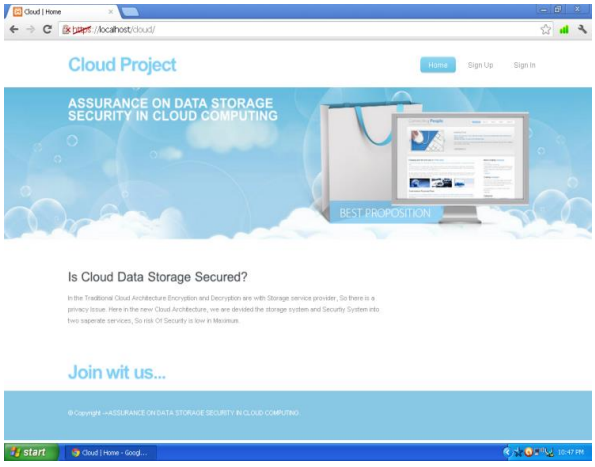
Here in our Project we have tested all module individually like login, signup, encryption, storage, decryption.

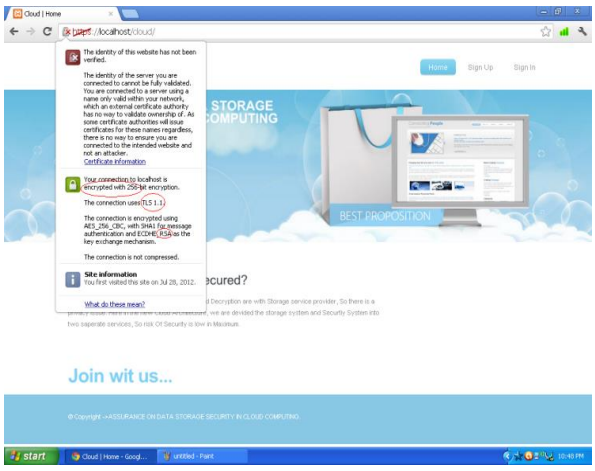
Integration Testing:

At the level of develop mentation each and every module will be tested individually. When coming to the integration testing, we have to integrate all modules and test the flow and working of modules together. Here in this project also done the same thing and passed the Integration test successfully.

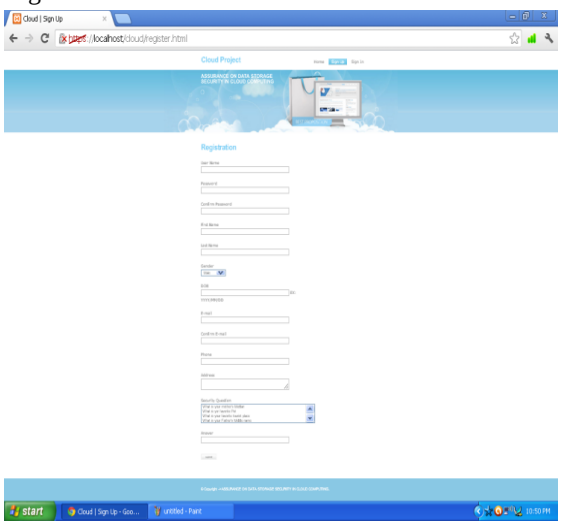
VI. SCREEN SHOTS

Home Page

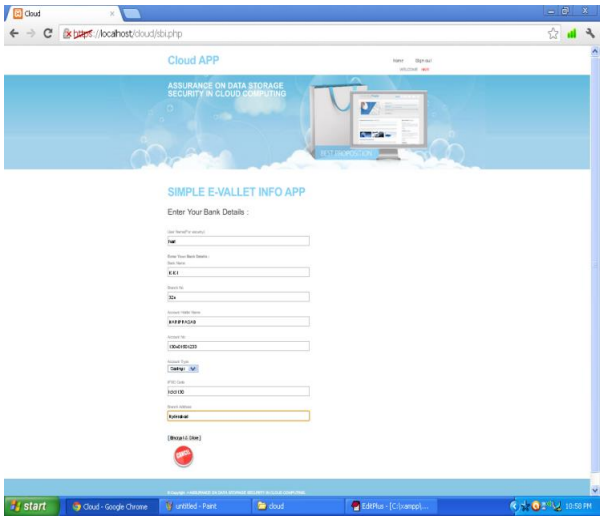




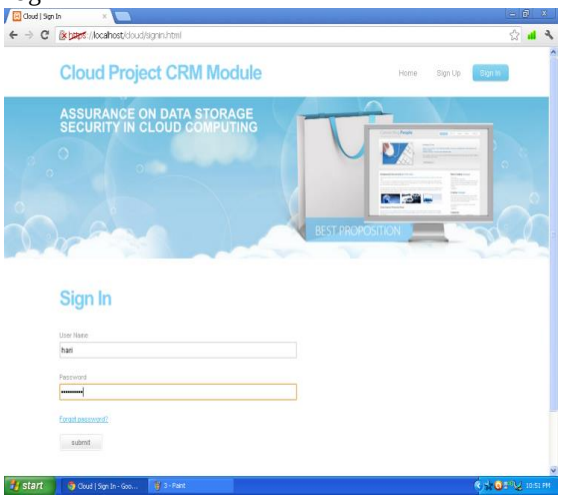
Register



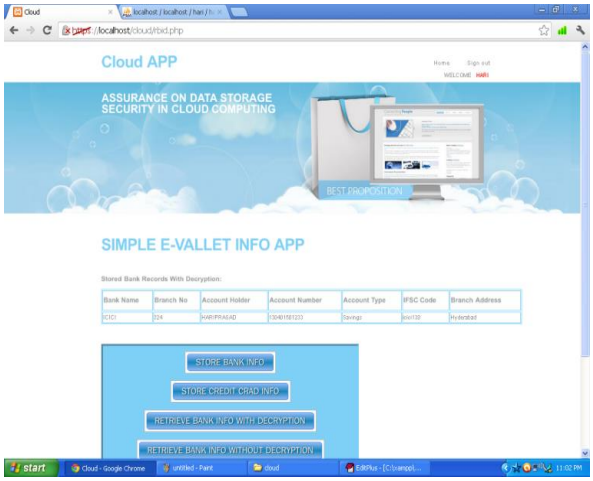
Store Bank Info



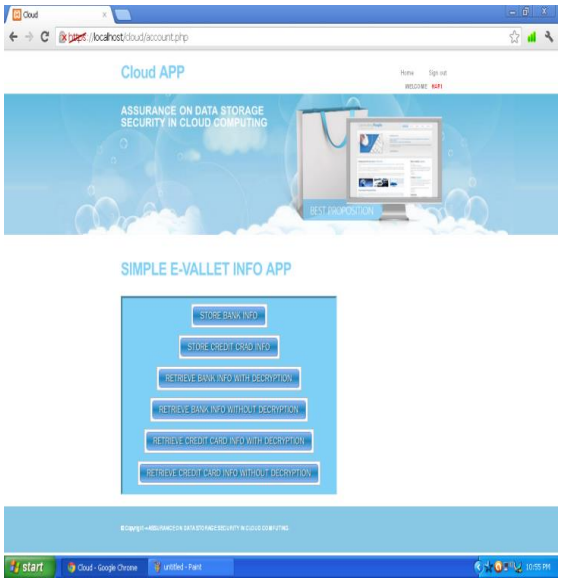
Login



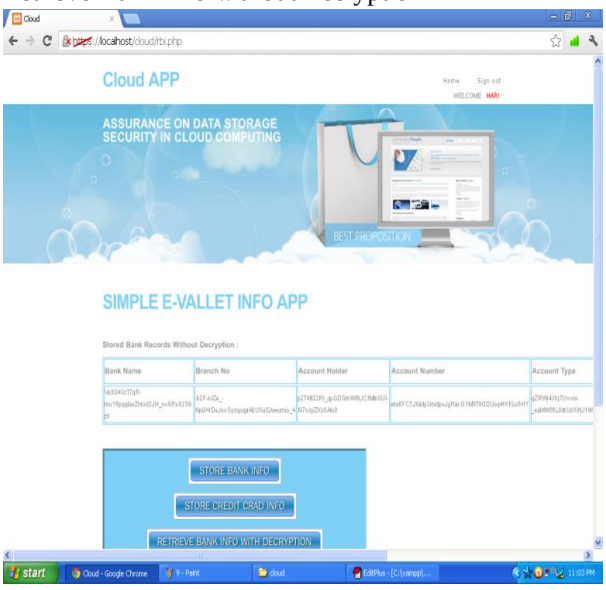
Retrieve Bank Info with Decryption



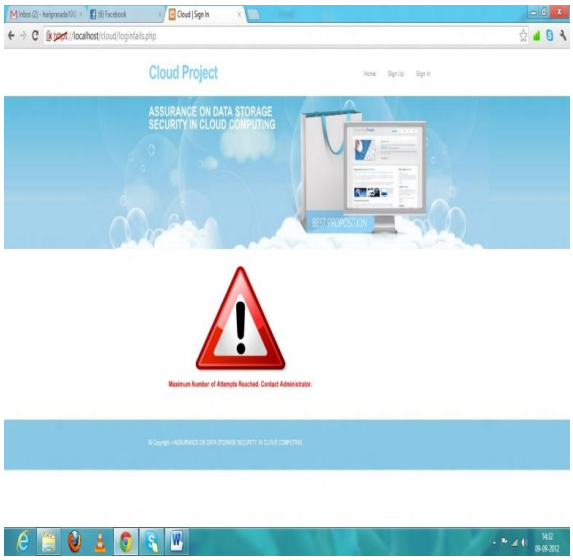
Accounts Page



Retrieve Bank Info without Decryption



Maximum Login Attempts Reached



VII. CONCLUSION AND FUTURE ENHANCEMENT

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.

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. 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.

BIBLIOGRAPHY

[1] A. Weiss, "Computing in the clouds", net Worker, vol. 11, no. 4, pp. 16-25, December 2007.
[2] C. S. Yeo, S. Venugopal, X. Chu, and R. Buyya, "Autonomic meteredpricing for a utility computing service", Future Generation ComputerSystems, vol. 26, issue 8, pp. 1368-1380, October 2010.
[3] http://www.php.net/
[4] http://www.wikipedia.org/
[5] http://www.w3schools.com/