International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

*Research Article*

# Dynamic Business Model Outsourcing for Data Integrity in Clouds

**Vijay Benjamin Lochan†* and Narender Kumar Gupta†**

†Department of Computer Science and Engineering, SHIATS, Allahabad, India

Accepted 26 March 2015, Available online 29 March 2015, **Vol.5, No.2 (April 2015)**

***Abstract***

*Cloud computing is a relatively new business model in the computing world. Cloud-based outsourced storage relieves the client's load for storage management and preservation by providing an equivalently scalable, low-cost, location-independent platform. Clients no longer have physical control of data indicates that they are facing a potentially frightening risk for missing or corrupted data. To keep away from the security risks, business model are significant to make sure that the integrity and availability of outsourced data. 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. Storing the data in encrypted form is a common method of information privacy protection. However the global nature of cloud brings about some challenges in security domain when physical control over our information in cloud is impossible. Thus, encrypting critical data becomes essential, and strongly advisable. The server-side encryption in an untrustworthy environment like public cloud is too risky. On the other hand, client-side encryption can undermine the benefits of cloud since it is a time-consuming task for encryption and decryption. This study proposes a business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service in order to get rid of security risks. A CRM (Customer Relationship Management) service is described in this paper as an example to illustrate the proposed business model.*

***Keywords:*** *Cloud Computing, Data Integrity, Encryption, Decryption, CRM, business model, outsourcing, SLA*

## 1. Introduction

Cloud computing is emerging as a vital practice for the online provisioning of computing resources as services. This technology allows scalable on-demand sharing of resources and costs among a large number of end users. It enables end users to process, manage, and store data efficiently at very high speeds at reasonable prices. Customers of cloud computing do not need to install any kind of software and can access their data worldwide from any computer as long as an Internet connection is available.

Many definitions have been presented for cloud computing (Foster *et al*, 2008; L. M. Vaquero *et al,* 2009*;* M. Armbrust *et al*, 2009). Foster *et al*, 2008 defined cloud computing as "a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet." Cloud computing provides various computing services online based on SLAs between the provider and the consumer.

Cloud computing providers offer many services to their customers (A. Monaco *et al,* 2012) including 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), test environment as a service (TEaaS), and many more.

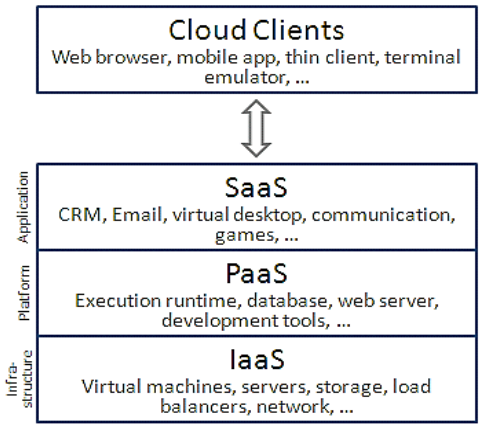


**Fig.1.** Cloud Services

With cloud computing, you eliminate those headaches because you're not managing hardware and software

*Corresponding author: **Vijay Benjamin Lochan** is a M.Tech Scholar; **Narender Kumar Gupta** is working as Associate Professor

that's the responsibility of an experienced vendor like salesforce.com (http:// www. salesforce.com/tw/). The shared infrastructure means it works like a utility: You only pay for what you need, upgrades are automatic, and scaling up or down is easy. Cloud-based apps (D. Benslimane *et al,* 2008) can be up and running in days or weeks, and they cost less. With a cloud app, you just open a browser, log in, customize the app, and start using it.

Businesses are running all kinds of apps in the cloud, like customer relationship management (CRM), HR, accounting, and much more. Some of the world's largest companies moved their applications to the cloud with salesforce.com (http:// www. salesforce. com/tw/) after rigorously testing the security and reliability of our infrastructure.

## 2. Background

In this section, we will provide an inclusive background on cloud computing key concepts and pricing generally and within the cloud.

### *2.1. Cloud computing service models*

Cloud computing is emerging as one of the most promising technologies. Its providers supply many services through service models to their customers. Infrastructure as a service (IaaS) is among these service models: computers are offered as physical or virtual machines to support end users' operations. The service provider is responsible for running and maintaining the service. It leases the use of the machines to customers typically on a pay per-use basis. Therefore, the price represents the amount of resources allocated. Other forms of resources in IaaS include IP addresses, firewalls, load balancers, images in a virtual machine image library, and virtual local area networks (VLANs). Examples of IaaS providers include Google Compute Engine (https:// cloud.google .com/products/compute-engine), Windows Azure Virtual Machines (http:// www. windowsazure. com/en-us/), Amazon Cloud Formation (http://aws. amazon.com/ cloudformation), Rackspace Cloud (http://www.rackspace.com/cloud), and Terremark (http://www.terremark.com).

Another major type of service model offered by service providers is platform as a service (PaaS). In this type of service, a computing platform is offered to customers. This computing platform includes operating systems, hardware, programming language execution environments, servers, and databases. Developers can benefit immensely from PaaS because they can rent complex hardware and change operating systems dynamically while developing their applications. The drawback is that PaaS lacks some flexibility and may not match the rapidly evolving requirements of some of their customers. Examples of PaaS providers include Amazon Elastic Beanstalk(http://aws.amazon.com), Cloud Foundry (http://www.cloudfoundry.com), Heroku(http://www. heroku.com), Google App Engine(http:// www.google. com/intl/en/ enterprise/ apps), Windows Azure Compute (http:// www. windowsazure. com/en-us/), and Salesforce.com (http:// www.salesforce.com/tw/).

Software as a service (SaaS) is another type of service model offered to customers. In this model, software applications are installed in the cloud and operated by service provides, and end users can access the software from cloud clients. The service provider is responsible for maintaining the software. SaaS has many advantages, such as easier administration, elasticity, worldwide accessibility, and compatibility. End users are typically charged a flat fee monthly or yearly. Examples of SaaS include Google Apps (http://www.google.com/intl/ en/enterprise/apps), Microsoft Office 365 (http://www.microsoft.com/en-my/office365/ online-software. aspx), Innkeypos (http://www.youtube.com/user/InnkeyPOS),Quickbooks Online (http:// quickbooksonline. intuit.com), and Limelight Video Platform.

Many other types of service models are provided. In storage as a service (STaaS), a service provider leases storage to end users by subscription. In security as a service (SECaaS), the security of a service provider is integrated efficiently and cost-effectively in a cooperative infrastructure. Test environment as a service (TEaaS) is another service provided to users, in which on-demand test environments and their data are given to customers. Figure 2 illustrates the basic types of service models in cloud computing.


**Fig. 2:** The basic types of service models in cloud computing

### *2.2 Existing methods for protecting data stored in a cloud environment*

Common methods for protecting user data include encryption prior to storage (A. Parakh *et al,* 2009) 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 and Elliptic Curve Cryptography (V. Miller *et al,* 1986) (ECC). 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 (R. Rivest *et al,* 1978) 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. 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 (L. Lamport *et al,* 1981), 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 (A. Elgohary *et al,* 2006) (SSL) is a common method of building secure channels, 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 (Balachandra Reddy Kandukuri *et al,* 2009) offer six recommendations for SLA content, 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.

### *2.3 Evolution from outsourcing to cloud computing*

The relation between cloud computing and outsourcing is best illustrated by taking current challenges of outsourcing into account: On the one hand, customers expect a cost-effective, efficient and flexible delivery of IT services from their service providers, at a maximum of monetary flexibility (i.e., pay per - use models). At the same time, more and more customers demand innovations or the identification of a customer-specific innovation potential from their service providers (Leimeister *et al,* 2008). Out of these challenged and constraints posed by clients, the new phenomenon of cloud computing has emerged. Cloud computing aims to provide the technical basis to meet customer's flexibility demands on a business level. Interestingly, new cloud computing offers to meet these business demands were first addressed by providers that have not been part of the traditional outsourcing market so far. New infrastructure providers, such as Amazon or Google, that were previously active in other markets, developed new business models to market their former by-products (e.g., large storage and computing capacity) as new products. With this move, they entered the traditional outsourcing value chain and stepped into competition with established outsourcing service providers. These new service providers offer innovative ways of IT provisioning through pay-per-use payment models and help customers to satisfy their needs for efficiency, cost reduction and flexibility. In the past the physical resources in traditional outsourcing models have been kept either by the customer or the provider. On the contrary, cloud computing heralds the paradigm of an asset-free provision of technological capacities.

## 3. Proposed System

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 (Jing-Jang Hwang *et al,* 2011) 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 (C. Weinhardt *et al,* 2009). Figure 3 shows Activity Diagram of the proposed system.

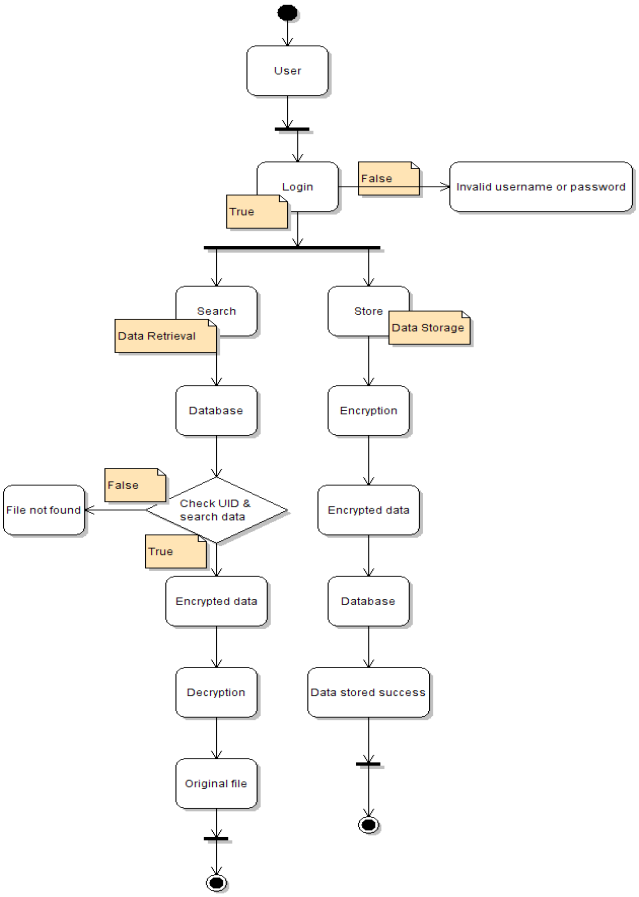


**Fig.3:** Activity Diagram of the proposed system

## 4. Customer Relationship Management

Think that user needs Infrastructure as a service and Software as a service. So that these two services are integrated and must be in touch with the user's requirement. The integrated thing will be called as Client Relationship Management (CRM).

The Cloud services providers are clients to CRM(*ex: Microsoft Dynamic CRM online, saffront* (http:// www. soffront. com)) cloud and the user is an indirect client to the clouds under CRM, as a whole it is a cloud computing architecture.

CRM is an integrated suite of applications, can improve the customer experience by getting clouds to collaborate seamlessly. It should support the adaptation of the different clouds, flexibility in user interface with drag and drop and promise better come end.

The document which defines the relationship between the service provider and client called SLA. It contains the information regarding the service definitions, performance management, problem management, customer duties and responsibilities, security, warranties and remedies, disaster recovery and business continuity and information about bills and dues.

## 5. Methodology

### *5.1. 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. 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.

### *5.2. CRM Service*

In a cloud computing environment, the user normally uses cloud services with specific functions, e.g., Salesforce.com's CRM service (http:// www.salesforce .com/tw/), SAP's ERP services (http:// www.sap.com/services/index.epx), 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). 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.

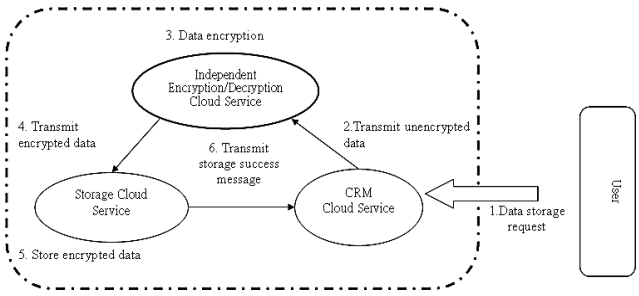


**Fig. 4** Business model concept integrating separate cloud services for data encryption/decryption, CRM and storage

*5.3. Encryption/Decryption Service*

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. 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 (Uma Somani *et al,* 2010), 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.

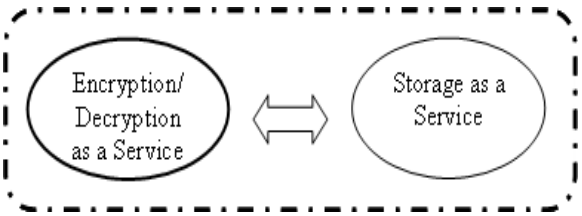


**Fig. 5** Encryption/Decryption as an independent service

*5.4 Accessing the Storage service*

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.

## 6. Analysis and accountability of proposed system

Cloud computing environments include three types of services (L. M. Vaquero *et al,* 2009): 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 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.

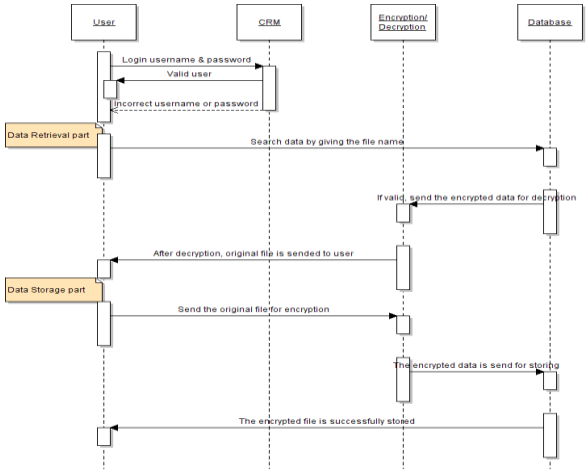


**Fig. 6** Analysis of Business model

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. Figure 6 show the analysis and accountability of proposed system step by- step.

## Conclusion

1. As the advantages are concerned in this study, we are concentrating on the latest security policies, mechanisms and SLA with the reduction of management risks.
2. 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.
3. 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.
4. 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.
5. In this new business model, user data in the Storage Service System is all saved encrypted.
6. 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

## References

I. Foster, I. Yong, Z. Raicu and S. Lu (2008), Cloud Computing and Grid Computing 360-Degree Compared, *Grid Computing Environments Workshop*.

L. M. Vaquero, L. Rodero-Merino,J. Caceres, and M. Lindner (2009), A breaking the clouds: towards a cloud definition, *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50-55.

M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, (2009), Above the Clouds: A Berkeley View of Cloud Computing, *Publication of Reliable Adaptive Distributed Systems Laboratory*, University of California, Berkeley.

A. Monaco (2012), A View inside the Cloud, http://theinstitute.ieee.org/technology-focus/technology-topic/a-view-inside-the-cloud.

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

A. Parakh and S. Kak (2009), Online data storage using implicit security *Information Sciences*, vol. 179, issue 19, pp. 3323-3333

V. Miller (1986), Uses of elliptic curves in cryptography, Advances in Cryptology - *CRYPTO '85, Lecture Notes in Computer Science*, pp.417-426.

R. Rivest, A. Shamir, and L. Adleman (1978), A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM*, vol. 21, no. 2, pp.120-126.

L. Lamport, (1981), Password authentication with insecure communication, *Communications of the ACM*, vol. 24, no. 11, pp. 770-772.

A. Elgohary, T. S. Sobh, and M. Zaki (2006), Design of an enhancement for SSL/TLS protocols, *Computers & Security*, vol. 25, no. 4, pp. 297-306.

Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr.Atanu Rakshit (2009), Cloud Security Issues, *IEEE International conference on service computing*, pp. 517-520.

Leimeister, S., T. Böhmann and H. Krcmar (2008). IS Outsourcing Governance in Innovation-Focused Relationships: An Empirical Investigation. *16th European Conference on Information Systems* (Eds,

Golden, W., Acton, T., Conboy, K., van der Heijden, H. and Tuunainen, V. K.), Galway, Ireland.

Jing-Jang Hwang and Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu (2011), A Business Model for Cloud Computing Based on separate Encryption and Decryption. 978-1-4244-9224-4/2011/*IEEE*,

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

Soffront CRM services, http://www.soffront.com.

Effective CRM solutions for small and medium size business, *saffront.*

SAP AG., SAP services: maximize your success, Retrieved-1Jan.2010,from http:// www.sap. com/services/index.epx

Uma Somani, Kanika Lakhani, Manish Mundra (2010), Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing, *IEEE*, ieeexplore. ieee.org/ iel5/5676248/ 5679597/

Salesforce.com, Inc., Force.com platform, Retrieved-Dec.-2009,from--http:// www. salesforce.com/tw/ Google-Compute-Engine,

https://cloud.google.com/products/compute-engine.

Windows-Azure, http: //www. Windowsazure . com /en-us/.

Amazon Cloud Formation, http:// aws.amazon.com/ cloudformation.

Rackspace Cloud, http://www.rackspace.com/cloud.

Terremark, http://www.terremark.com.

Amazon Web Services, http://aws.amazon.com/.

Cloud Foundry, http://www.cloudfoundry.com.

Heroku, http://www.heroku.com.

Google Apps, http:/ /www.google. com/ intl/en/ enterprise/apps. Microsoft Office 365, http://www.microsoft.com/ en-my/ office365/online-software.aspx.

Innkeypos, http://www.youtube.com/user/InnkeyPOS.

Quickbooks-Online, http:// quickbooksonline. intuit.com.

Google-App-Engine, https://appengine.google.com/.