ISSN 2250-3153

A Model for Data Protection Based on the Concept of Secure Cloud Computing

Gargee Sharma[1], Prakriti Trivedi[2]

[1] Pursuing M.tech (SE), GECA, Ajmer, India
[2] HOD, Department of Computer Engineering, GECA, Ajmer, India

Abstract- This paper examines the present scenario of threats being faced by the enterprises willing to outsource their data and information on a storage service provided by a third party Cloud service provider. In contrast to conventional solutions, which are well protected by standardized data access procedures, organizations tend to loose integrity of data when systems are outsourced to the cloud. Since the data is stored on the service provider's storage they must ensure to overcome the threats against integrity of data and preventing its unauthorized disclosure. At the same time enterprises willing to outsource data storage should be mindful of the terms and conditions of their cloud contract. To maintain integrity and privacy of information it is encrypted and stored on the storage service. But if storage as well as encryption-decryption is performed by the same service, the administrator might have access to the data and corresponding keys. The aim of this study is to propose a model for secure cloud computing based on separate data storage from cryptographic process. Another way, the service is split into two: one service provider is proposed to be responsible for storage and another for its encryption-decryption; along with it both providers are different in order to ensure information security. It is also proposed that after the completion of encryption and decryption process, the service must not retain the data and the information must be encrypted first and then stored on the storage service.

Index Terms- Secure Cloud computing, data integrity, system outsourcing, data storage service, service contract

I. MOTIVATION AND RESEARCH QUESTIONS

Cloud computing is already a hot topic in technology industry these days. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network [1].

Before the advent of Cloud era, crucial data was stored on storage media inside the organization itself. Various measures like firewalls were installed to keep a check on flow of data outside the organization and regulate the access internally as well. Hence, well framed security measures must be practiced by Cloud service providers to ensure the privacy and integrity of the client data. Above all, sound measures must be practiced against the administrators to keep a check on unauthorized access and disclosure

Cloud computing is concerned with the sharing and coordinated use of diverse resources in distributed environment [2]. This leads to the idea of outsourcing the parts to a third party. As with outsourcing concerns exist about the implications for computer security and privacy [3]. Data is an important asset for any organization and in order to avail the benefits of cloud, it has to outsource data from its computing center to the provider's computing center. Thus, the primary motivation is the assurance of secure Cloud service by reviewing the security risks imposed once the data is outsourced.

Major research questions for secure computing are:

A. Malicious usage:
Malicious users continue to leverage new technologies to improve their reach so that they are not detected easily and consistently improve the effectiveness of their activities. These nefarious users actively target the cloud service providers due their limited capabilities of fraud detection and relatively weak registration systems.

B. Non standardized SLAs:
While most service providers strive to ensure the security of user's assets, it is the responsibility of the users to understand the implications associated with the usage and hence comes the place for Service level agreements (SLA's) [4]

C. Privileged insiders:
The impact that malicious insiders as well as privileged users can have on an organization is considerable, given their level of access and ability to infiltrate organization and assets. They can cause financial as well as productive losses. Thus, it is the responsibility of the customers to keep a check on the policies and measures taken against such activities.

D. Distributed technology issues:
Attacks have surfaced in recent years that target the distributed technology inside the cloud computing environments. Distributed resources and other shared elements were never designed for compartmentalization. This gives an opportunity to the attackers to impact the operations of other cloud customers as well as to gain unauthorized access to others data.

E. Data outflow/leakage:
One of the major research questions is the prevention of data leakage. Not only degrading competitive spirit and financial implications, it could significantly impact employee, business partner, customer morale and trust. Worse still, there might be some legal violations too.

F. Eavesdropping:

Service hijacking is not a new concept. It comprises techniques like phishing, exploitation of software defects. If hijacker gains access to user assets like password they can eavesdrop user activities and redirect client to illegitimate sites.

G. Unknown risk:

Since the core concept of cloud find its root under the idea of multi-tenancy, which poses the existence of unknown risk profile, thus the customer must have a faith on its provider and actively monitor the policies stated in SLA and conduct independent audit to check the status of their security.

This study proposes a model for secure cloud computing based on separating the data storage service from cryptographic service consisting of two functions: encryption/decryption. Both the services are provided by two different service providers with an assumption that data will be stored in encrypted format on storage server and cryptographic service will not retain any data after it has been encrypted or decrypted.

II. BACKGROUND: LITERATURE SURVEY

A. Origin and definition of cloud computing

The boom in the cloud computing world has led to a new era of on demand delivery of hosted service over a shared network. Cloud computing is a complex infrastructure of software, hardware, processing and storage that is available as a service [5]. It has flexibility rendering user to customize the service suited to his needs. Innovations in virtualization and distributed systems have paved the path for interest in cloud computing.

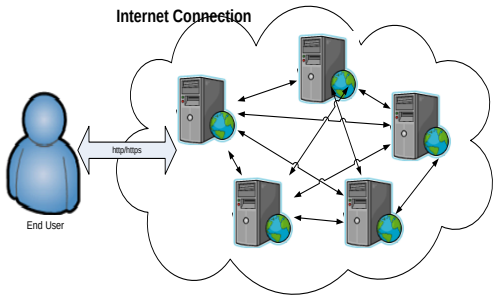

Figure 1: End user interaction with Cloud

Cloud environment provides immense possibility for internet application provides infinite space for storing as well as managing data and provides powerful computing capacity for users to complete all kinds of application. Users have started changing their habit of using computer totally, from services centered by desktop to services centered by Web. The aim of application of cloud computing is to combine all the resources, and let anyone use it. There are many definitions of cloud but collectively advocates the ease of use as long as the user is having a computer and connected to the internet. User does not need to buy hardware neither the software but simply charged for the resources being utilized adding a comfort factor as well as reducing the overhead. Overall, advent of cloud era has introduced virtualization with numerous benefits including reduced capital expenditure and administration costs, enhanced scalability and improved quality of service.

B. Cloud computing layered organization

In the years to come cloud computing services will become a solution for small and midsize companies to completely outsource their data-center infrastructure and for larger companies to have a way to get peak load capacity without building larger data centers internally. Cloud service providers tend to offer services that can be grouped into three categories [6], [7] it is illustrated below in Figure 2:

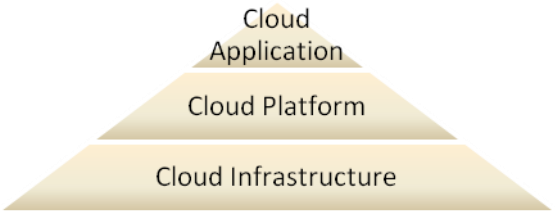

Figure 2: Layered organization of Cloud

Cloud infrastructure as a service (IAS): Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Instead of physically deploying servers, storage, and network resources to support applications, developers specify how the same virtual components are configured and interconnected, including how data are stored and retrieved from a storage cloud

Cloud platform as a service (PAS): Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services. It is real implementation of distributed services pulled up to deliver an application in accordance to user demand.

Cloud application as a service (SAS): a complete application offered as a service on demand. A single instance of the software runs on the cloud and services multiple end users or client organizations. Most common examples include Google Apps, Salesforce.com and many more.

C. *Business model framework:*

Based on the aforementioned layered structure, we can develop a business model framework for using the features of cloud environment, as shown in figure 3.

The framework is being developed after analyzing the existing cloud services, each representing a particular domain and collectively offering towards a common framework as a whole.

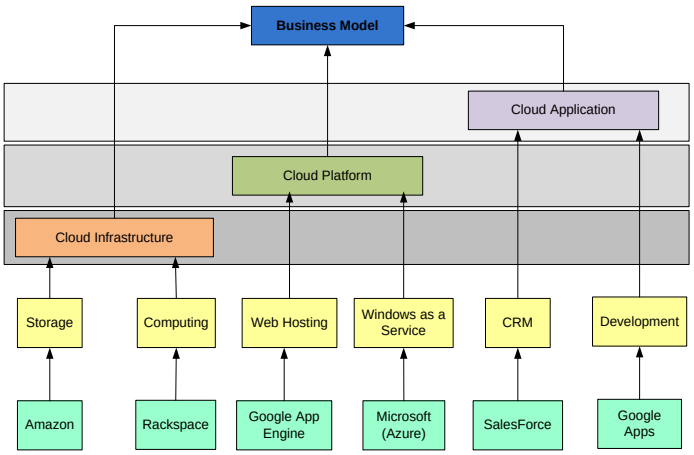

Figure 3: Business model for secure cloud computing

D. *Moving protection to the cloud:*

In cloud environment, the resources can be leased from a single service provider and the data can be stored on its corresponding storage server. This type of agreement can help an organization save infrastructure costs related to software and hardware, but storing data on providers storage may introduce a security breach as the business information might be disclosed to malicious insiders and privileged users as well. Thus, another storage strategy might be the client ensures encryption of data prior to its storage and provider may install firewall to prevent the leakage of decryption keys outsiders. But, the major question is that what measure should be taken if encrypted data and decryption key is handled by the same provider? Thus it poses a risk of unauthorized disclosure since the high level administrators/privileged users might have an access to the data

E. *Existing techniques for data protection in cloud*

For some years, tools for defending against hackers have been in the form of software to be installed on each device being protected or appliances deployed on-premise. However, to be effective, such protection needs to be constantly updated. Common methods for ensuring security of data in cloud consist of data encryption (cryptographic process) before storage, authentication process before storage or retrieval and constructing secure channels for data transmission. The protection methods find their routes in cryptographic algorithms and digital signature techniques. A brief overview is as follows:

The cryptographic algorithms are classified into two categories: symmetric and asymmetric algorithms. Symmetric algorithm uses a single key known as "secret key" both for encryption and decryption process whereas asymmetric algorithm uses two keys; one is the "public key" made available publically and the other one is the "private key", which is kept secret used to decrypt the data. Breaking the private key is rarely possible even if the corresponding public key is known well in advance. Examples of symmetric algorithm comprise of Data encryption standard (DES), International data encryption algorithm (IDEA), advanced encryption standard (AES) on the other hand asymmetric key algorithm include RSA algorithm [8]. Asymmetric algorithms are best suited for real world use and provides undeniable advantages in terms of functionality whereas symmetric algorithms is ideally suited for security applications like remote authentication for restricted websites which do not require full-fledged asymmetric set up.

The use of passwords for authentication process is popular among the users but the transmission of messages containing password may be vulnerable to illegal recording by the hackers hence posing a security breach in the system. Some more advanced authentication techniques may employ the concept of single-usage-password where the system may generate challenge token expecting the user to respond with an encrypted message using his secret key which converts the password to some derived value enabling a session. Once, the session is expired the whole process is repeated making each session unique in nature.

While using the cryptographic techniques for ensuring data security care should be taken for storing encryption and decryption keys. Rigorous methods should be adopted to prevent insiders and privileged user from gaining access to the encrypted data and decryption key simultaneously. Thus, the importance of SLA's is recognized in this context. The policies responsible for user data protection must be clearly mentioned in the provider's contract.

After reviewing the data security requirements following recommendations have been included in multiparty SLA suggested at the end to ensure data security in cloud: 1) encrypted data and decryption key must not be stored at the same place 2) access control techniques should be applicable for malicious insiders and privileged users 3) independent audits must be conducted to access the effectiveness of techniques employed for data storage 4) service providers must abide the ethics and legal laws and should be responsible for discrepancies if any 5) backup and reset methods against system crash and failures.

III. A MODEL FOR DATA PROTECTION BASED ON THE CONCEPT OF SECURE CLOUD COMPUTING

A. *Basic perceptions*

This study proposes a model for data protection through on the concept of secure cloud computing. The proposed model is based on separating the data storage from the cryptographic process including encryption-decryption. The concept is illustrated in fig- 4. In this model, both the separated processes are provided as services from different service providers. The storage service provider can't store the data in plain text, the data is first converted to encrypted format by the cryptographic process and then transferred via secure channel to the storage provider for storage. Also, cryptography as a service once completed the encryption or decryption of user data has to delete all the data.

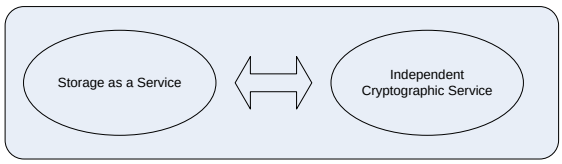

Figure 4: Illustrating separation of above services

Separation of duties can be analogously compared to examples from daily life. Consider an example of accounts department in a college, where the tasks of cashier and accountant are well defined. The cashier is responsible for handling cash and accountant for maintaining accounts. Thus, falsifying the accounts is not an easy task since every official document is to be countersigned and stamped with seals of two different people. Thus, distributing the power is a key to maintain security.

In cloud environment, the user selects service the provider on the basis of his requirements. Various functions are specified by the providers like Salesforce.com's CRM service, CRM, ERP tools from NetSuite, Visual Studio2010 for development from Microsoft [9], etc. The data generated from such services is stored on the storage service from one of the provider. The study proposes separation of storage service from cryptographic service. We take an example of CRM service (figure 5) for illustrating the concept of separating the aforesaid two processes.

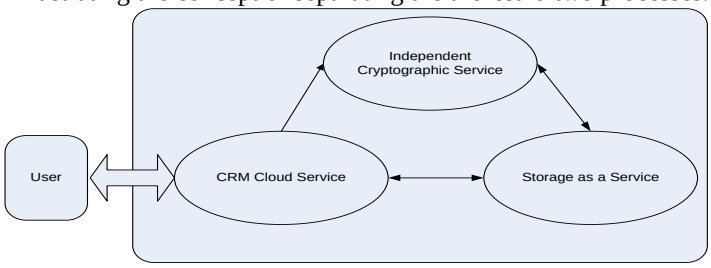

Figure 5: Conceptual illustration of proposed model

Thus, there are three service providers: one for storage, another for encryption and decryption and third for CRM application. The CRM application can be replaced by other cloud apps like ERP, accounting etc.

B. Operating principle

Suppose the user logs in (creating a new session) the system and retrieves some data. A data retrieval process will be executed as shown in figure 6

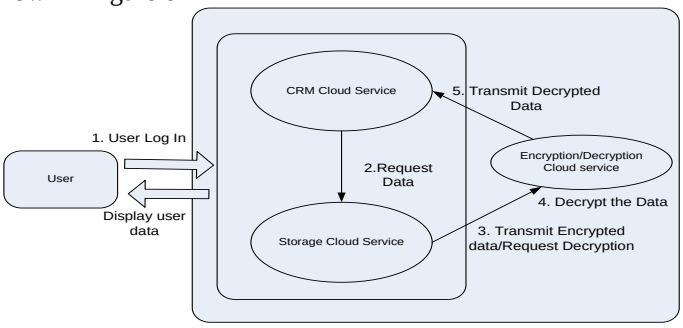

Figure 6: Data retrieval module

Each time the user access the CRM service, a new session is created following a well defined number of steps as explained below:

Firstly, execution of login program: which can be implemented through any standardized user authentication procedure viz. symmetric key-based login or challenge-response authentication.

Secondly, data retrieval module: if any data is to be retrieved from the CRM system, data is searched on the basis of user ID transmitted by CRM system. The data stored in encrypted format and needs to be decrypted before retrieval

Thirdly, hence the encrypted data is transmitted to cryptographic service along with user ID, requesting decryption

Fourthly, cryptographic server stores the pair of decryption key as well as User ID in order to ensure accuracy. Decryption key is retrieved on the basis of transmitted user ID and the decryption of the data is done by the cryptographic service

Fifthly, resulting data is transmitted to CRM application through a secure channel. Once the data is received by CRM app, cryptographic service deletes all the decrypted data and decryption keys in order to prevent disclosure.

Last but not the least sought data is displayed on the user interface.

Next, we explain the data storage module as shown in figure 7. Suppose the user logs in to store the data. Below is the list of steps followed to the same.

Firstly, user wants to store some data and initiates the data storage module

Secondly, since the data cannot be stored in plain text, unencrypted data is transmitted along with user ID over a secure channel to the cryptographic server for encryption.

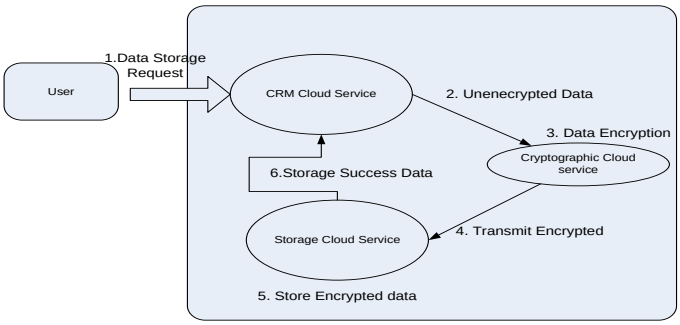

Figure 7: Data Storage module

Thirdly, data from different users are encrypted using different keys, hence user ID is used as an index to retrieve the encryption key and encryption is done by the cryptographic server.

Fourthly, the aim of this study is the separation of authority, hence encrypted data paired with user ID is transmitted for storage to the storage server

Fifthly, the pair including encrypted data and user ID is stored together at the storage server.

After the successful execution of step 4, all encrypted as well as unencrypted data must be deleted by the cryptographic service.

Last but not the least; a message is displayed to the user interface regarding the status of the whole process.

Retrieval and data storage modules require the integration of three cloud service providers, working and cooperating with one another in a lock step manner.

The primary goal of user for logging in the CRM service could be maintenance of data. Hence, feasible methods should be selected for implementing the same. For example, Client ID can be generated to index user ID or both can be merged and stored and interpreted accordingly when used. The proposed model is operable by the support of multiple cloud service providers serving their clients through a variety of applications like ERP, accounting, CRM and so on requiring the composed ID: resulting as merging of user ID with other IDs depending upon the type of application. Also, the different service provider must cooperate to achieve a common goal of serving the client.

C. Recommendation for multiparty SLA content

Service level agreement is a formal agreement stating the terms and conditions as well as code of conduct agreed among the stakeholders. It states the rights and obligations of the parties involved. SLA must be signed between the user and providers and the between the multiple providers as well. All parties are expected to imbibe the terms and conditions to separate the responsibilities and creating a cooperative environment to deliver the services to client as a whole. Below is the template for SLA (figure 8) between all the stake holders (including multiple service providers: cryptographic service provider, storage service provider, CRM provider and the client).

Sample SLA template

User_____(will be further referred as "Client")

Providers:

"CRM Provider"

"Cryptographic Provider"

"Storage Provider"

1. CRM Provider terms and responsibilities

a) It provider CRM service as an application to the Client.

b) When not in use, CRM provider may not retain Client's data

2. Cryptographic Provider terms and responsibilities

a) Provides encryption and decryption facility for Client's data and holds the encryption and decryption key simultaneously

b) When done with Client's data or when not in use it must delete all encrypted/decrypted as well as unencrypted data.

3. Storage Provider terms and responsibilities

a) It is responsible for storing Client's data already encrypted by cryptographic provider

b) Should not store data in plain text, always store in encrypted format

c) Should not hold encryption/decryption keys for security of Client data

Figure 8: Sample SLA template (stating the terms and responsibilities)

IV. Analysis and Discussion

Cloud computing is based on three types of service model: infrastructure, platform and software. A virtual environment is created where user access these services and resources through an internet connection hence, decreasing the overhead of buying and maintenance. As a result of the oozing benefits of Cloud it has become popular among organizations across the globe and have started storing their internal data on cloud, so it's the responsibility of the provider to store data in encrypted format. Since every luring thing has some drawback same is the case here. Attackers have devised ways to bypass security by gaining access to encryption and decryption keys as they are stored at the same storage provider's backup. But the data is not secure as the privileged users or malicious insiders may have access to the data and their corresponding keys leading to a situation of unauthorized disclosure.

Thus, the model proposes the separation of authorities and suggests a different service provider to take the responsibility of encrypting and decrypting user data and holding the keys for the same. Once, done with the data it is transmitted to storage service for storage. After the receipt of the successful completion, all encrypted/decrypted or unencrypted data must be deleted to ensure the security of data.

So, three service providers are involved in the operation of ensuring data security, hence comes the need for a legal contract among all the stakeholders stating the terms and responsibilities to imbibe and work in a cooperative way to serve the client as a whole. Therefore, a sample SLA template has been recommended to make the clear separation of their duties and policies.

References

[1] http://en.wikipedia.org/wiki/Cloud_computing.
[2] Zhidong Shen and Qiang Tong (2010) 2nd International Conference on Signal Processing Systems (ICSPS), *Published by IEEE Computer Society in IEEE Xplore Dalian*, V2-11 - V2-15.
[3] Wayne A. Jansen, NIST(2011), "Cloud Hooks: Security and Privacy Issues in Cloud Computing", *Proceedings of the 44th Hawaii International Conference on System Sciences*, 1530-1605
[4] http://www.chnsourcing.com/article/Article/abc/163420070809133104.html
[5] Rich Maggiani, (2009), "Cloud Computing Is Changing How We Communicate", *Professional communication conference, IPCC 2009*, pp 1-4.
[6] Bhaskar Prasad Rimal,Eunmi Choi,Ian Lumb (2009), "A Taxonomy and Survey of Cloud Computing Systems*",proceedings of IEEE on fifth international joint conference on INC, IMS, IDC*, pp.44-51.
[7] Shuai Zhang, Shufen Zhang, Xuebin Chen and Xiuzhen Huo, (2010) "Cloud Computing Research and Development Trend", Second International Conference on Future Networks, pp 93-97.
[8] Atul kahate, "Cryptography and network security", McGraw hill, Second edition, 2008, pp 87-198.
[9] http://www.techno-pulse.com/2009/12/top-cloud-computing-service-providers.htmlloud

First Author (Corresponding author) – Gargee Sharma, pursuing M.tech in (software engineering), from GECA Ajmer, India. Presently working as lecturer in Modern College of engineering, Pune. Having 3 years of teaching experience. Email id: gargee.mec@gmail.com.

Second Author: Prakriti Trivedi, HOD, department of computer engineering, GECA, Ajmer, India. M.E in Computer Sc engineering, having 10+ yrs of teaching experience and published several research papers and books.