

## A Secure Model for Cloud Computing Based Storage and Retrieval

Yaga Reddemma<sup>1</sup>, Lingala Thirupathi<sup>2</sup>, Sreekanth Gunti<sup>3</sup>

<sup>1,3</sup>Department of CSE, PRRM College of Engineering, Shabad, Ranga Reddy, Andhra Pradesh, India

<sup>2</sup>Asst.Prof, Department of CSE, Malla Reddy Institute of Engineering & Technology, Secunderabad, Andhra Pradesh, India

---

**Abstract:** Enterprises protect their internal storage and retrieval process using firewalls and also protect it from insider attacks by formulating secure data access procedures. If the enterprises are willing to store data in cloud, cloud computing service providers have to take care of data privacy and security. A common way to achieve security is encryption/decryption mechanism employed by cloud service providers. However, performing both tasks such as storage and encryption/decryption mechanism by cloud server causes security problems as the administrators know the sensitive information and may involve in illegal practices. To overcome this problem, this paper presents a mechanism where the storage is done by one provider while encryption/decryption mechanisms are provided by another service provider. In the proposed system the party that uses cloud storage services must encrypt data before sending it to cloud while the service provider who is responsible for encryption/decryption must delete data once encryption/decryption process is completed. To illustrate the proposed mechanism, this paper uses a CRM service example that demonstrates how the parties involved in secure storage and retrieval when data is saved to cloud. It also provides insights into multi-party SLAs for the proposed system.

**Keywords**—SLAs, cloud computing, encryption and decryption, secure storage and retrieval

---

### I. Introduction

Cloud computing has become a reality recently. Many vendors such as Google, IBM, and Microsoft came up with cloud solutions that enable people and organizations gain access to huge computational and other resources in pay per use fashion. According to Weiss, cloud computing involved many existing technologies [1]. They include utility computing in service oriented fashion [2], grid computing [3] and large data centers that are used to store huge amount of data of cloud users. Before cloud computing came into existence, organizations used to store data in their internal storage media and security is provided by various means to prevent attacks from external and internal users. As organizations need more and more resources they may opt to use cloud services. In such case, their data is directly stored in cloud server maintained by service provider. The data security plays an important role when data is stored in cloud server. Cloud service providers take care of security of their users' data. However, from user perspective, cloud is not secure. This is because the administrators of cloud storage servers are privileges to have unauthorized access to data of clients. This has to be prevented. This is the motivation behind taking up this research work. This paper proposes the mechanisms to prevent it.

Generally service providers provide certain security and service policies which are to be accepted by the clients or users. Every application which needs people involvement has some sort of agreement with clients or users. For instance Yahoo! Web mail needs users consent for its terms and conditions. In cloud environment also the clients might have different storage requirements at different times. These requirements and server's rules and regulations and any other issues are clearly mentioned in the agreements. Often they are known as service level agreements (SLAs) [4]. The signing on SLAs indicate that users have accepted to the terms and conditions and both service provider and client. Generally security to storage is provided by using encryption and decryption concepts. System administrators are able to access to the private data of users in cloud computing. If this is the case, users' data may not be secure. This paper focuses on this security threat.

We propose a new mechanism where the storage and encryption/decryption are separated into two different cloud servers. In one cloud server data storage takes place securely while other server only takes care of encryption and decryption operations to see that data of user remains secure. This paper uses CRM concept to demonstrate the new mechanism proposed.

### II. Related Work

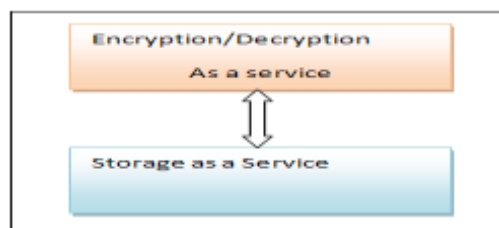
With the advent of Internet began all related technologies to grow in a fast pace. People of all walks of life started using these technologies either directly or indirectly. Businesses became truly global in nature. There are no geographical and time restrictions for merchandise as it can be done online. Recently cloud computing [5] technology came into existence. It is an emerging technology that enables individuals and organizations to gain

access to huge state-of-the-art resources through Internet in pay per use fashion without capital investment. This concept helps people at large to make use of resources through Internet and pay per use. The resource usage can be adjusted based on the customer requirements [6]. Cloud computing has many kinds such as PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and SaaS (Software as a Service) [7]. The SaaS provides software to cloud clients as service. The IaaS provides infrastructure such as data centers, storage, and secure servers etc to cloud clients. The PaaS provides development platform that enables programmer to write applications that interacts with cloud.

There are many data privacy concerns in cloud computing. Improper disclosure of business data to third parties is one of the major concerns [8]. Encryption must be used to properly secure user's data in cloud [9]. For protecting cloud data the existing methods include FIPS, TDEA, AES, RSA cryptography [10] and ECC [11]. These technologies are capable of providing security to cloud storage. However, there are some problems with these technologies including encrypting/decryption technology for ensuring safe storage. However, the storage and security (encryption/decryption) are mixed in the same server. This may allow administrators of the service provider to have illegal access to cloud storage. This paper addresses this problem by proposing a business model that separates the storage cloud service from encryption/decryption service. This ensures that those services work independently in a loosely coupled fashion. The administrators of both the services can't directly access the data thus making it more secure.

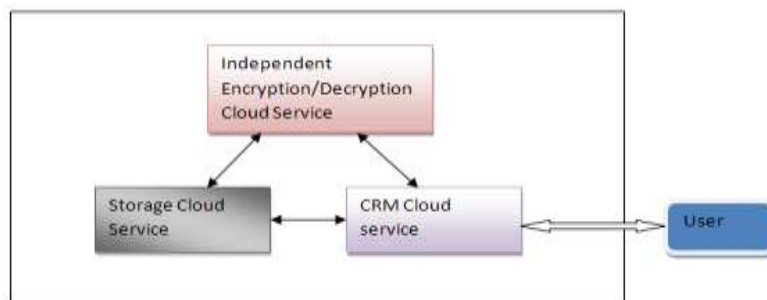
### III. Proposed Business Model

The proposed business model separates data storage service from that of encryption and decryption service. The separation is as visualized in fig. 1. Storage service is provided by one cloud service provider and encryption/decryption service is provided by another service provider.



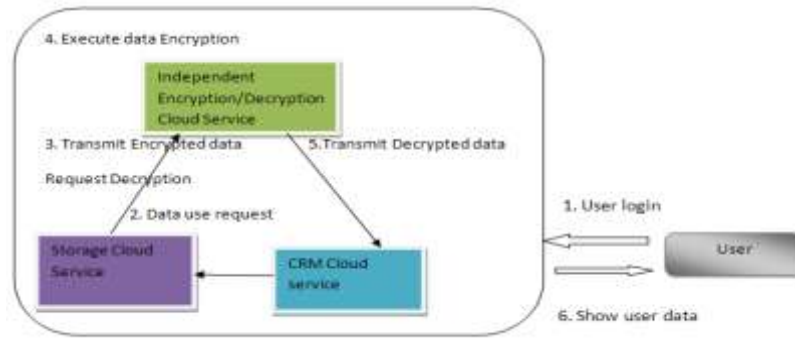
**Fig 3: Encryption/Decryption as an independent service**

This separation is required as the cloud server administrators might have illegal access to data of the users. To prevent this, the services such as storage and encryption/decryption are separated and moved to different cloud servers. Generally users use cloud environment for specific purposes. For instances SAP's ERP services [12], Salesforce.com's CRM service [13] and so on. The data generated by these operations is saved to cloud storage. However, this study advocates an additional cloud server that takes care of encryption/decryption activities which are independent of storage service. This split responsibilities of both the servers have division of labor in functioning that provides more secure to user's data.



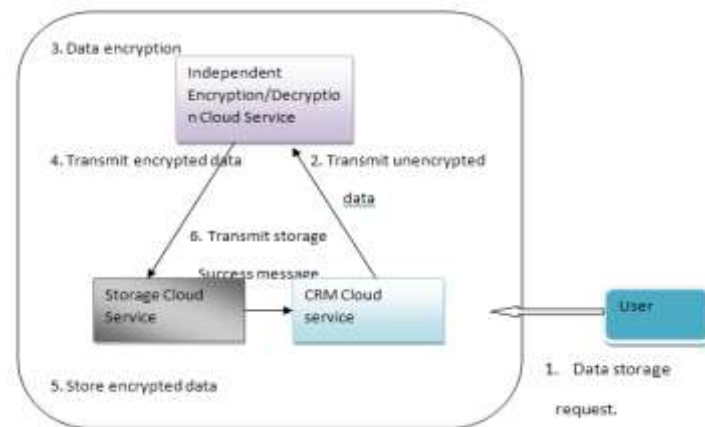
**Fig. 2 –Proposed Business Model for storing user's data in cloud**

As can be seen in fig. 2, user CRM service is taken to demonstrate the new business model. As per this model users interact with CRM cloud service. In turn the CRM service interacts with both storage could service and also encryption/decryption cloud service. The interaction among them is bidirectional. The storage cloud service and encryption/decryption service and CRM service are having bi-directional communication among them.



**Fig. 3 –Data retrieval mechanism in the proposed business model**

First of all user’s credentials are authenticated by CRM cloud service. Once authentication is done user can access CRM server through which he performs data retrieval and data storage operations. Fig. 3 shows data retrieval operation in detail. As per the user’s instructions the CRM cloud service interacts with storage cloud service and makes data usage request. Then the storage cloud service sends encrypted data which is available in to encryption/decryption service and requests for decryption. The encryption/decryption service takes encrypted data and simply decrypts it and sends the decrypted data to CRM cloud service. SSL (Secure Sockets Layer) is used for encryption and decryption purposes. The last step is that the CRM cloud service sends requested data to end user. Thus secure communication is taking place across all components as part of proposed data retrieval mechanism.



**Fig. 4 – Data storage mechanism in the proposed business model**

As can be seen in fig. 4, after due authentication, the end users sends data storage request to CRM cloud service. In turn the CRM cloud service sends unencrypted data to encryption/decryption cloud service. The encryption/decryption cloud service actually encrypts the given content and sends it to storage cloud service where it is stored. Then the storage cloud service sends resultant message to CRM cloud service.

#### IV. Service Level Agreements

Service level agreements between the parties involved in cloud computing is essential. In other words there must be business agreements between the cloud service provider and cloud user. The SLA template should cover all possible agreements. This will make it clear to both the parties so that they stick to their promises. The proposed business model involves cloud user, CRM service, storage cloud service and encryption/decryption service. The template for SLAs among them is provided in fig. 5.

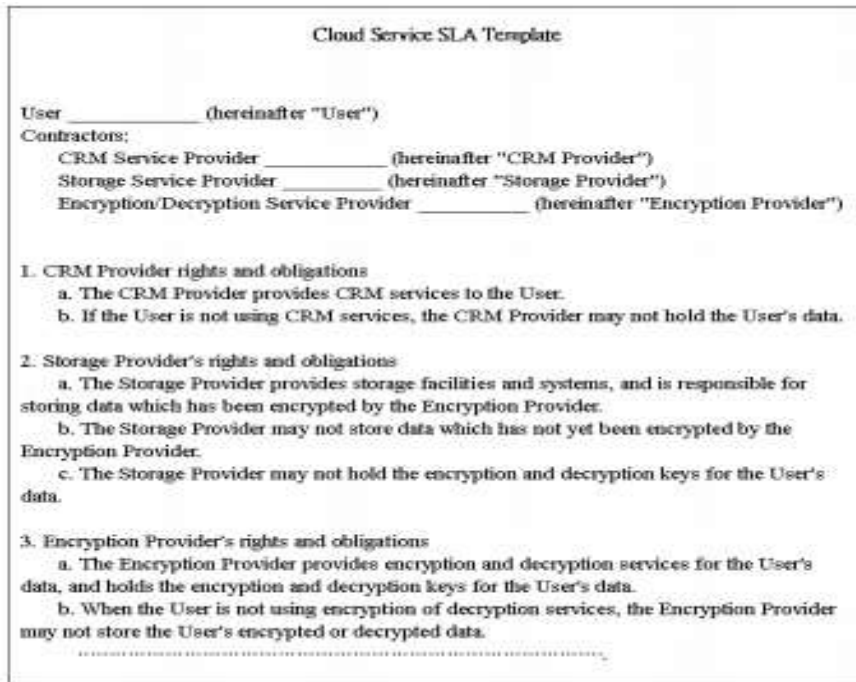


Fig. 5 – SLA Template

The proposed business model when SLAs are incorporated becomes a perfect business model where all partners or parties follow ideal practices keeping their agreements in mind. The business model is very secure as all parties involved in SSL communication and the separation of encryption/decryption service from storage service makes is more robust and secure.




## V. Conclusion

This paper has presented a new security mechanism to protect data of cloud users. It proposes separation of storage and encryption/decryption services into two different cloud service providers. The data storage is taken place at one cloud server while the security mechanisms are applied at another cloud server. This ensures the transparency in storage and retrieval. When user sends data to cloud service provider, he has to send it as plain text to encryption/decryption service provider. Then the encryption/decryption service provider encrypts data and sends it to another service provider who is responsible for storage. Thus a secure storage of data is ensured. When user wants to get information from cloud server, a request is made to this effect and the cloud server where data is stored sends encrypted data to cloud server responsible for encryption/decryption. That server decrypts the data and finally the plain text is sent to user securely. In addition to this, in the proposed system multi-party Service Level Agreements (SLAs) are also suggested for father improvement of the system.

## References

- [1] A. Weiss, "Computing in the clouds", netWorker, vol. 11, no. 4, pp. 16-25, December 2007.
- [2] C. S. Yeo, S. Venugopal, X. Chu, and R. Buyya, "Autonomic metered pricing for a utility computing service", Future Generation Computer Systems, vol. 26, issue 8, pp. 1368-1380, October 2010.
- [3] M. Baker, R. Buyya, and D. Laforenza, "Grids and grid technologies for wide-area distributed computing," International Journal of Software: Practice and Experience, vol.32, pp. 1437-1466, 2002.
- [4] B. R. Kandukuri, V. R. Paturi and A. Rakshit, "Cloud security issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.
- [5] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.
- [6] R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.
- [7] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.
- [8] N. Hawthorn, "Finding security in the cloud," Computer Fraud & Security, vol. 2009, issue 10, pp. 19-20, October 2009.
- [9] A. Parakh and S. Kak, "Online data storage using implicit security", Information Sciences, vol. 179, issue 19, pp. 3323-3333, September 2009.
- [10] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.
- [11] V. Miller, "Uses of elliptic curves in cryptography," Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986.
- [12] SAP AG., "SAP services: maximize your success," Retrieved Jan. 2010, from <http://www.sap.com/services/index.epx>
- [13] Salesforce.com, Inc., "Force.com platform," Retrieved Dec. 2009, from <http://www.salesforce.com/tw/>

**About Authors:**

	<p><b>Yaga Reddemma</b> received the B.Tech Computer Science, A.P, India and Currently doing M.Tech in Computer Science and Engineering at PRRM College of Engineering, Ranga Reddy, Andhra Pradesh, India.</p>
	<p><b>Lingala Thirupathi</b> received the B.Tech (Information Technology),M.Tech (SoftwareEngineering) atSreenidhi Institute of Science &amp; Technology,Secunderabad,AP, India &amp; currently working as anAsst.Professorat Malla Reddy Institute of Engineering &amp; Technology, Secunderabad, AP, India.</p>
	<p><b>Sreekanth Guntipursing</b> the M.Tech Computer Science Engineering, Hyderabad, A.P, India at PRRM College of Engineering, Ranga Reddy, Andhra Pradesh, India.</p>