International Journal of Electrical, Electronics and Computer Engineering **5**(1): 41-45(2016)

ISSN No. (Online): 2277-2626

Enhancement in Sharing of Records on Secure Cloud using Advanced Encryption Standard and RSA

***Monika**[*] **and Gurpreet Kaur**[**]*

[*]*PG Scholar, Department of Computer Science and Engineering, Doaba Institute of Engineering & Technology, Kharar, Sahibzada Ajit Singh Nagar, (Punjab), INDIA*

[**]*Assistant Professor, Doaba Institute of Engineering & Technology, Kharar, Sahibzada Ajit Singh Nagar, (Punjab), INDIA*

(Corresponding author: Monika)

(Received 10 March, 2016 Accepted 02 April, 2016)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cloud computing provide us a means by which we can access the applications as utilities over the internet that allow us to create, configure, customize, share applications online. Data security, confidentiality, availability, location and relocation of data, load balancing are major issues in cloud computing. The new character brings lots of security challenges and load balancing techniques which have not been taken into account completely in the current cloud computing system. As a consequence, to build a cloud computing data security system is the basis to build cloud computing security system. It is very important for commercial users of the cloud computing to protect their business secrets. This is to obtain the highest possible level of privacy. Modern encryption algorithms play the main role in data security of cloud computing. In this work, we discuss the various possible solutions for the issues in cloud computing security. In this case lots of efforts are done from the service providers (servers), scientific association and so on in facilitating security issues. The main goal of this research is to provide techniques for solving problems of data security and load balancing related issues. The aim of the research is to ensure privacy and security at the server side using AES algorithm and at client side using RSA algorithm. This approach provides privacy and security at client side and also at the server side.

Keywords: Cloud computing; Cloud security; RSA Algorithm; AES Algorithm

I. INTRODUCTION

Cloud computing is new utility of the century, which many enterprises wants to incorporates in order to improve their way of working.[10] Cloud computing describes a new supplement, consumption and delivery model for IT services based on the internet and it typically involves the provision of dynamically scalable and often virtualized resources as a service over the internet. In other words cloud computing simply means internet computing generally the internet is seen as collection of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people & organizations. It implies sharing of resources to handle applications. The biggest challenge in successful implementation of Cloud computing technology is managing the security. Its ability to reduce cost associated with computing while increasing flexibility and scalability for computer process has proved to be a great advantage. The idea of cloud computing has gone beyond just businesses and is slowly turning into an essential IT service [2]. However, major IT firms have shown concern about the critical issues such as security that exist with the widespread implementation of cloud computing. One major challenge is to construct a well-defined technical solution to store private user data on a shared and uncontrolled infrastructure. When end users release their data to remote datacenters, they lose control over the data after the bits leave their client computers [14]. Existing scalable storage solutions scale up the data storage capacity and throughput, but have largely left privacy protection as a non-goal or future work [17].

A. Characteristics of cloud computing

NIST's definition framework for cloud computing with its list of essential characteristics has by now evolved into the de facto standard for defining cloud computing [8]. Multi-tenancy is not called out as an essential cloud characteristic by NIST but is often discussed as such. Although not an essential characteristic of cloud computing in the NIST model, CSA has identified multi-tenancy as an important element of cloud [9]. There are five key characteristics of cloud computing as defined by NIST [7]; these are:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

B. Cloud Computing Security Issues

Brodkin discusses a study of Gartner, which points out seven areas of concern around security issues in cloud computing [3]:

Privileged user access: Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Brodkin suggests getting as much information as possible about the people who manage the data.

Regulatory compliance: Customers are ultimately responsible for the security and integrity of their own data, even when a service provider holds it. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

Data location: While using the cloud, it's probably not known exactly where the data is hosted. In fact, even the country it will be stored in is unknown. Gartner advises to ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers [13].

Data segregation: Data in the cloud is typically in a shared environment alongside data from other customers. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

Recovery: Even if the user doesn't know where its data is, a cloud provider should state what will happen to the data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask the cloud service provider if it has "the ability to do a complete restoration, and how long it will take".

Investigative support*:* Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If the user cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then user's only safe assumption is that investigation and discovery requests will be impossible" [11].

Long-term viability: Ideally, the cloud computing provider will never go broke or get acquired and swallowed up by a larger company. [4] But user must be sure that its data will remain available even after such an event. "Potential providers should be asked how the user would get the data back and if it would be in a format that user could import into a replacement application," Gartner says.

II. PROBLEM STATEMENT

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry [15]. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe as an environment it is [16].

The new character brings a lot of new security challenges which have not been taken into account completely in current cloud computing system. As the foundation of cloud computing is relatively new, there are various unsettled issues that are yet to be resolved before cloud computing is completely accepted by the vast communityof users. Cloud computing being the most preferred computing technology still lacks in gaining user's trust in it due to privacy concerns. Amongst the two major cloud deployment models i.e. Public Cloud Deployment Model and Private Cloud Deployment Model, [12] the security issues are more in public cloud as compared to private cloud. Private cloud is more secure as it is maintained within the organisation that is using it but at the same time setting up a private cloud infrastructure is an expensive approach.

Whereas Public cloud is reasonably cost effective due to negligible infrastructure and maintenance cost but it is more vulnerable to security violations [1]. As any user can access it through Internet, it is the most preferred architecture when cost reduction is concerned, but relying on a cloud service provider to manage and hold user's private data raises privacy concerns. Data security, confidentiality, data location and relocation, data availability are major issues in cloud implementation.

Internet users unknowingly expose their confidential data at risk [5]. While doing normal activities on internet, their username and passwords of emails and bank accounts along with the browsing history and other information filled in forms is stored at one place by web browser and thus it becomes vulnerable and malicious users or websites can steal the user's private information [6]. Usually, sensitive information like user passwords is transmitted to the remote servers through non-encrypted networks. Even if encryption is used in some cases, it is only used for transmission of initial login information only while all other subsequent data is transmitted unencrypted as plain text only and hackers can easily attack this data. Hence users get exposed to potential risks when they are connected to cloud services using public networks.

As a consequence, to build a cloud computing data security system is the basis to build cloud computing security system. It is very important for commercial users of the cloud computing to protect their business secrets. This is to obtain the highest possible level of privacy. Modern Encryption algorithms play the main role in data security of cloud computing.

III. METHODOLOGY

The following steps are proposed to achieve the security implementations using AES algorithms for security at server side, by RSA at client side.

A. Execution Steps

(i) Sign up – using RSA algorithm.
(ii) Allotment of symmetric and public key to the user.
(iii) Search for file uploaded by the record user.
(iv) Login using RSA algorithm at client side and AES algorithm at sever side.
(v) Uploading data using AES algorithm.
(vi) Data is stored / retrieved from Storage server using AES algorithm.
(vii) Logout

B. Proposed Algorithm

Step I: Sign up if new user at the control panel.
Step II: Assign the symmetric and public keys to the user and search for file uploaded by the record user.
Step III: Login using RSA algorithm at client side and AES algorithm at sever side
Step IV: Uploading data using AES algorithm at the control panel.
Step V: Encrypted data is stored / retrieved from Storage server on the cloud.
Step VI: Download the encrypted file from the control panel when required.

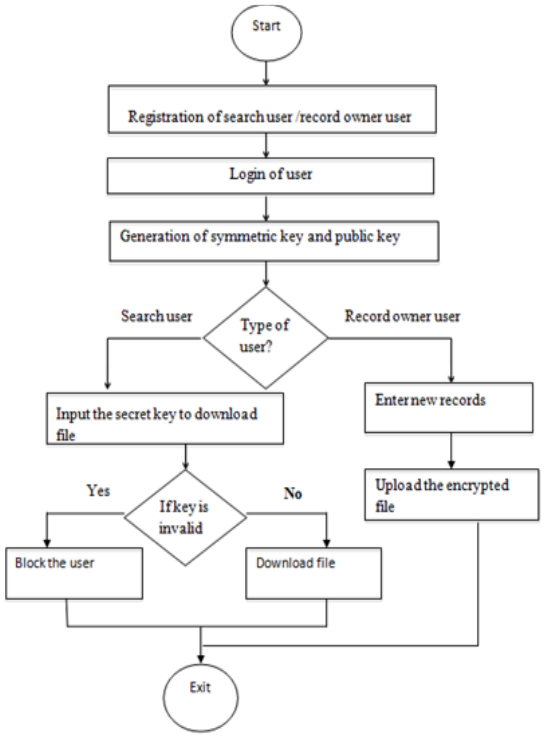

Fig. 1. Flow chart of proposed algorithm.

IV. RESULT AND DISCUSSIONS

Cloud computing provide us a means by which we can access the applications as utilities over the internet that allow us to create, configure, customize, share applications online. Data security, confidentiality, availability, location and relocation of data, load balancing are major issues in cloud computing. As a consequence, to build a cloud computing data security system is the basis to build cloud computing security system. It is very important for commercial users of the cloud computing to protect their business secrets. This is to obtain the highest possible level of privacy.

The proposed cloud framework achieves the objectives stated for this research work as it removes the concern of data confidentiality in public cloud. The encryption standards ensure that data remains segregated even when data is stored on common cloud storage. Modern encryption algorithms play the main role in data security of cloud computing. In this work, we discuss the various possible solutions for the issues in cloud computing security. In this case lots of efforts are done from the service providers (servers), scientific association and so on in facilitating security issues. The main goal of this research is to provide techniques for solving problems of data security related issues. The aim of the research is to ensure privacy and security at the server side using AES algorithm and at client side using RSA algorithm. Only the authenticated client can login and can access the files that have secret keys provided by the record owner. At server side only authenticated record owner can upload the files and files are encrypted using AES algorithm. This approach provides privacy and security at client side and also at the server side.

V. CONCLUSION

Cloud computing technology is in a stage of consistent development and as it will proceed towards its maturity, many new and even more cloud based issues and vulnerabilities will evolve. The challenges in privacy protection are sharing data while protecting personal information. The ability to control what information to reveal and who can access that information over the internet has become a growing concern. This thesis aimed at presenting a framework that clarified the impact of cloud computing on confidentiality preservation, by making step wise recommendations on confidentiality of data stored, processed and transmitted in cloud computing environment. The proposed framework achieves the objectives stated for this research work as it removes the concern of data confidentiality in public cloud. The encryption standards ensure that data remains segregated even when data is stored on common cloud storage. Data access is permitted only after the user is authenticated thus providing full control and ownership of data to the user. A well defined key management process is created so that the performance and complexity of the application is not compromised.

VI. FUTURE SCOPE

The current prevailing security questions concerning the availability and confidentiality of data in cloud computing environments are yet to be satisfactorily answered. This research work has focused on the confidentiality issues in public cloud computing environments. Only technical privacy and security controls were analyzed and developed in this thesis. In future research on the topic of public cloud security, the cloud computing confidentiality framework presented in this thesis can be extended by adding the data integrity mechanism that enhances the data security and implementing load balancing mechanism to manage resources on the network efficiently. Another newest and less attended deployment model of cloud computing i.e. hybrid clouds includes public cloud deployment as one of its core constituent and private cloud deployment model being the other. The implementation of hybrid cloud laboriously relies on the gateway between the public division and the private division of hybrid cloud and managing resources on the network by implementing effective load balancing mechanism, it can be a compulsive matter of research in future.

REFERENCES

[1]. Astrova I. , Grivas S.G. and Schaaf M., *"Security of a Public Cloud"* , ICIMISUC, pp. 564-569, 2012.

[2]. Behl, A., *"Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation",* WICT 2011, pp. 217 – 222, December 2011.

[3]. Brodkin, J. Gartner, *"Cloud-computing security risks", Retrieved from http://www.networkworld.com/.*

[4]. Chen, D. and Zhao, H., *"Data Security and Privacy Protection Issues in Cloud Computing",* ICCSEE 2012, pp. 647 – 651, March 2012.

[5]. Delettre, C., Boudaoud, K. and Riveill, M., *"Cloud computing, security and data concealment",* ISCC 2011, pp. 424 – 431, July 2011.

[6]. Gaurangkumar, K. and Minubhai, C., *"To achieve Trust in the Cloud",* ICACCT, pp. 16-19, 2012.

[7]. Gong, C., Liu, J., Zhang, Q., Chen, H. and Gong, Z., "The Characteristics of Cloud Computing", *39th International Conference on Parallel Processing Workshops*, pp. 275-279, 2010.

[8]. Hoff, C., Simmonds, P., Pohlman, M., Swain, B., Posey, L. et. al., *"Security Guidance for Critical Area of Focus in Cloud Computing V3. 0"*, Retrieved from Cloud security Alliance, from https://downloads.cloudseurity alliance.org/initiatives/guidance/csaguide.v3.0.pdf, November 2011.

[9]. Hofman, P. and Woods, D., "*Cloud Computing: The Limits of Public Clouds for Business Applications*", *IEEE Internet Computing,* Vol. **14**, Issue-6, pp.90-93, 2010.

[10]. Jadeja, Y. and Modi, K. , *"Cloud computing - concepts, architecture and challenges",* ICCEET 2012, pp. 877 – 880, March 2012.

[11]. Jansen, W.A., *"Cloud Hooks: Security and Privacy Issues in Cloud Computing",* HICSS 2011, pp. 1-10, January 2011.

[12]. Jensen, M., Schwenk, J. , Gruschka, N. and Iacono, L.L., *"On Technical Security Issues in Cloud Computing",* IEEE ICCC 2009, pp. 109-116, September 2009.

[13]. Kantarcioglu, M. , Bensoussan, A. and Sing Ru Hoe, "*Impact of security risks on cloud computing adoption",* AACCCC, pp. 670 – 674, September 2011.

[14]. Kumar, Abhishek., Gupta, Shubham, Rai, Animesh., Deep, Vikas., "An Analysis on Security Concerns in Cloud Computing", *International journal of innovation in engineering and technology,* vol. **2** Issue 2 April 2013, ISSN:2319-1058

[15]. Lv H. and Hu Y. , "Analysis and Research about Cloud Computing Security Protect Policy*",* ICISIE 2011, pp. 214 – 216, August 2011.

[16]. Mathur, P. , Nishchal, N. *, "Cloud computing: New challenge to the entire computer industry",* ICPGDC, pp. 223 – 228, October 2010.

[17]. Ming, T. and Yongsheng, Z., *"Analysis of Cloud Computing and Its Security", International Symposium On Information Technology In Medicine And Education,* Vol. **1**, pp. 379-381, 2012.

[18]. Ren K. , Wang C. and Wang Q., *"Security Challenges for the Public Cloud",* Published by IEEE Computer Society, pp. 69-73, January/February 2012.