Improving Privacy and Portability of Data Migration between inter Clouds

[1] M Madhavi [2] G Balakrishna [3] J V S Arundathi

[1]Associate Professor in Dept. of Computer Science and Engineering, Anurga Group of Institutions.
[2]Assistant Professor in Dept. of Computer Science and Engineering, Anurga Group of Institutions.
[3]Research Scholar in Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation.

Abstract – Most of the communication in the network is based on the efficient reliability and the availability of the resources which improve the throughput. Reliable resources over the network channelizes a route for data transfer and access. Ongoing mechanical advances have started the prominence and achievement of cloud. This new worldview is picking up a growing enthusiasm, since it gives cost effective designs that help the transmission, stockpiling, and intensive processing of information, but the major concern is with the Security and reliability of the data stored and transmitted among the clouds and network. To enhance the security in the cloud RSA Cryptography is applied to the data storage as it has evolved with public and private keys. The analysis of the algorithm has been done on the offline and online Google docs Redundancy handling mechanism provides minimum space usage at data storage provider as Data Service Provider (DSP) is accompanied by the amount of storage used. The size of the files is reduced and the security of the documents stored and transferred is improved with the RSA cryptography. A critical comparative analysis of cryptographic defense mechanisms, and be-yond this, it explores research directions and technology trends to address the protection of outsourced data in cloud infrastructures.

Keywords: *Interoperability, Portability, Security, reliability, RSA, Redundancy, Cost.*

1. INTRODUCTION

The information security is a prime area of concern since vital information may be at stakes due to security problems in transfer process or medium which is followed [1]. In order to tackle the issue, several strategies are in place. Every strategy works towards generating keys associated with the presented data. The redundancy of data given to the encryption process leads to the generation of multiple keys for similar data [2]. Also, the generated keys and data are stored at data and key storage providers. Storage of data and keys at storage providers require cost [3]. Size of the keys and data are directly proportional to cost. Before describing details of techniques used to ensure security, cloud and its attributes are described.

Cloud computing becomes a need of the hour nowadays but many experts argue about it [4]. Highly scalable services are provided by the cloud. Users can utilize the services on pay per use basis. Cloud computing theoretically provides infinite resources but due to growing number of users, practically services and resources becomes limited. The services and resources required to be distinguished on the basis of the scale of utilization along with cost. Although energy consumption and starvation problems nowadays, associated with cloud computing but still improvement in services could lead to the better framework for concurrent users to access resources more than capacity of the machine user hold and hence leads to more popularity and user community attracted towards the cloud.[5].

Cloud interoperability is required during the transmission of data to and from the cloud servers. The cloud service provides ensures QoS(quality of service) through security mechanisms. The security mechanisms used may or may not use redundancy handling mechanism to conserve space. In the proposed system security mechanism along with redundancy handling mechanism is enforced for ensuring the quality of service. Before some of the attributes will be defined, the term cloud should be explained. Cloud computing used widely from long time and provides opaque framework where services are visible to the user but internal working is hidden [6]. Key attributes in cloud computing are as below:

- **Service-Based*:*** Cloud main objective is to provide a service-oriented framework by hiding details and showing only necessary features to the user. This mechanism is also termed as abstraction.
- **Scalable and Elastic*:*** Services associated with cloud are not fixed. Services and be added as and when required depending upon mass usage of services. In other words scalable environment is provided by cloud computing [7]. Elasticity in framework indicates resources are provided on different platforms accessible by multiple users at a time. In other words, concurrency is supported through the use of cloud computing framework.

Received: 15 May 2018/Accepted: 20 June 2018

- **Shared:** The pool of resources is provided by the use of advanced computing environment [8]. Resource if free can be accessed by any number of resources provided resource is not exclusive in nature. An exclusive resource cannot be shared and that resource accessing required queue to be maintained.
- **Metered by Use**: Multiple payment modes are supported by cloud infrastructure [9].Services are accessed on pay per use basis. Service provider and clients are bound by the service level agreement. A user needs to pay for accessing the services mentioned within SLA. The problem however is, even if service is down for the period of time, still user is required to pay for that service.
- **Uses Internet Technologies**: Services are delivered to the user by the use of the internet. The protocol such as hypertext transfer protocol (HTTP), file transfer protocol (FTP), Terminal network (Telnet) etc. are used for this purpose [10].

The Encryption techniques collaborated with cloud computing to ensure high degree of security and reliability is prime objective of this study.

2. RELATED WORK

Describes IBE technique with outsourcing computation and also offloads the key generation operations to Key Update Cloud service provider [11]. It also focuses on critical issues of identity revocation. It accomplishes consistent productivity for both calculation at PKG and private key size at a client, User needs not to contact with PKG amid key-update, as it were, PKG is permitted to be disconnected subsequent to sending the disavowal rundown to KU-CSP, No protected channel or client verification is required amid key-update amongst client and KU-CSP.

Design a virtual encryption card framework that gives encryption card usefulness in virtual machines. In this framework, it displayed the vEC-PPM, which deal s with the encryption resource plan [12][13][14]. It saved clients' information utilizing a trusted equipment of virtualization in view of TPM. It additionally settled a trusted chain amongst clients and encryption cards in light of the composed protocols. The design of the virtual encryption card empowers the security and productivity of the encryption benefit. A usage examination shows that the effectiveness of framework is similar to that of the native mode. Later on, it proceeds with an examination, trying to plan a virtual encryption cards bunch to help higher encryption speed and more reasonable similarity with virtualization. A safe billing protocol for smart applications in distributed computing [15]. It utilized homomorphic encryption through adjusting the Domingo-Ferrer's plan, which can perform different number arithmetic operations to fulfill smart grid billing necessities in a safe way. This plan keeps up the exchange off amongst security and versatility contrasted and other homomorphic plans that depend on either secure, yet inelastic in terms of arithmetic operations assortment. Additionally, it proposed an instrument that guarantees both security and integrity during correspondence between substances. The execution of the proposed system is very satisfactory; it is sufficiently productive to use in lightweight applications and can be helpfully connected to cloud-based applications. Security enhancement mechanisms including symmetric, public key and homomorphic cryptosystems to enable experts to comprehend encryption plans for information on distributed storage [16][17][18][19]. AES is utilized as a part of most secure applications for information on distributed storage. Completely homomorphic encryption plans are promising for cloud condition however a long way from being useful due to their execution rate. Homomorphic assessment of AES has fascinating applications as a reasonable encryption conspire for information on distributed storage.

A protected cloud data encryption framework, named the Circulated Ecological Key (DENK in short), with which all records are encoded by one encryption key got from numerous coordinating keys which are keys gotten from approved clients' secret key keys and a believed PC's natural key [20][21][22]. An effective and unquestionable FHE in light of another mathematic structure that is without commotion [23].

Described various way which is used in cloud computing for data security [24]. The information is put away on to an incorporated area called data centers having a substantial size of information storage. In this way, the customers need to put stock in the supplier on the accessibility and additionally information security. Before moving information into general society cloud, issues of security gauges and similarity must be tended to. Cloud computing guarantees to change the financial matters of the server farm, yet before sensing and managed information move.

To resolve the problem with the existing literature proposed literature present efficient solution. The encryption mechanism with the redundancy handling mechanism is proposed as described in the next section.

3. METHODOLOGY

The methodology of proposed work consists of the registration process at first place. The registration in proposed system will be a two-phase process. In the first phase, registration at data storage provider is made. After successfully registering, a user can load files at data storage provider end. To generate keys users require performing registration at the key service provider. In order to retrieve the files, users must log in to the DSP and then KSP. The keys generated could be used in order to decrypt the file. The mechanism also uses redundancy handling mechanism

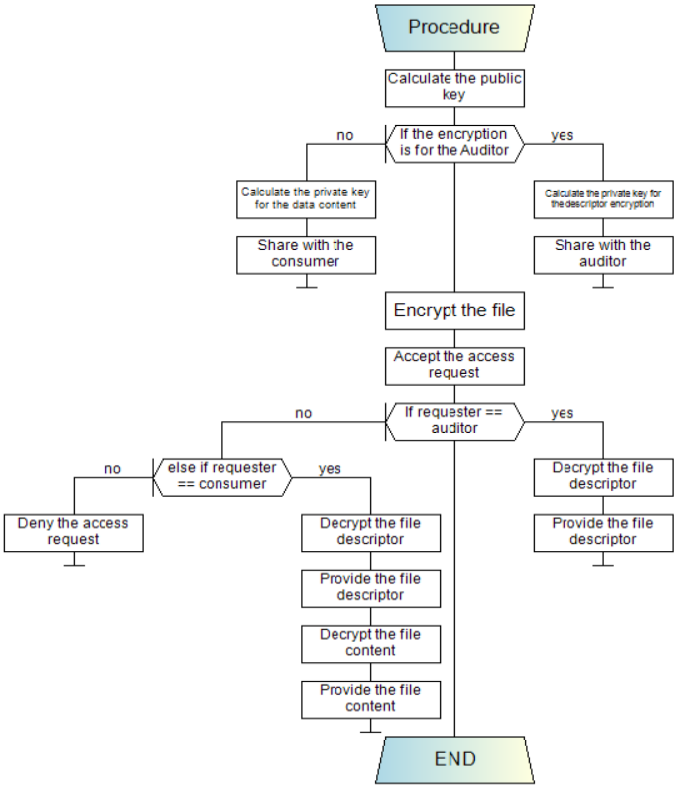
Received: 15 May 2018/Accepted: 20 June 2018

for preserving space for extra file loading. Also, an online source of files like Google docs can be used to retrieve the files and perform encryption and decryption.

The detailed steps are described as under

Registration at DSP: The registration at DSP comprises of unique username and password. Username and password once registered at DSP can be used for accessing file uploading module

Registration at KSP: The key service provider (KSP) is used in order to generate the keys for the file which is uploaded. The proposed system is capable of generating the keys for files generated from an online source.



Generating Keys:

1. Randomize two prime number selection as A & B, where A is greater than B
2. Calculate the product of two prime numbers as K = A * B
3. Consider a random polynomial of order N as $\gamma(N)$
4. Calculate the intermediator of the key as $\gamma(N) = (A-1) * (B-1)$
5. Calculate the public prime component as E such that GCD (E, $\gamma(N)$) == 1
6. Generate the Public Key PK as PK = (E, $\gamma(N)$)
7. Generate the File Descriptor Private Key as FDPvK = (D1, $\gamma(N)$), where D1 = E$\gamma(N)$ / | $\gamma(N)$|
8. Generate the File Content Private Key as FCPvgggfK = (D2, $\gamma(N)$), where D2 = $\gamma(N)$E/ |$\gamma(N)$|

In order to generate keys, a user must log in to the KSP. The files uploaded, are encrypted and corresponding keys are generated. The redundant files are neglected and rests of the files are uploaded with the public and private keys generated.

Encryption and Decryption Process:

For encryption and decryption, AES and RSA algorithms are hybridized. The algorithm yield cipher text after receiving files as plaintext.

Encryption Process:

1. Segregate the File Descriptor and the File Content as consider as FD and FC respectively
2. If FD is not encrypted, then encrypt with PK & FDPvK, else continue to the next part
3. If FC is not encrypted, then encrypt with PK & FCPvK, else continue to the next part
4. If FD & FC both are encrypted, then merge the encrypted FD & FC and upload the file to the cloud storage

Decryption Process:

Received: 15 May 2018/Accepted: 20 June 2018

1. If the requester label is FDR, then process the file descriptor and decrypt.
2. Else If the requester label is FCR, then process the file content and decrypt file descriptor and content both.

Verification of the overall procedure is in terms of time consumed and size of the file that can be uploaded.

1. If the access request is been made for the auditing access, then verify the request with the key combination of PK & FDPvK.
2. Once, the verification is valid, and label the request as FDR. Else terminate the request.
3. Else If the access request is been made for the data access, then verify the request with the key combination of PK & PCPvK
4. Once, the verification is valid, and label the request as FCR. Else terminate the request.

4. RESULT AND PERFORMANCE ANALYSIS

The result is presented in terms of file size that can be uploaded. Reliability of encryption and decryption in terms of time consumed is also a performance metric. The comparison in terms of quality is given as below:

Performance Metric	File Size permitted Existing(KB)	File Size Proposed(KB)
Offline Source	20	50
Offline Source	22	57
Offline Source	50	102
Offline Source	65	165
Offline Source	85	200
Online Source	0	1024
Online Source	0	2048
Online Source	0	3000

Table 1: Permitted Space Comparison

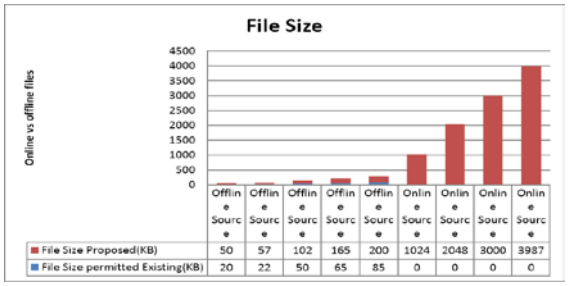


Figure 1: Plot of Space utilization by existing and proposed system

The time consumed also is an issue which can be further improved since time consumed greatly depends upon the speed of the internet used to access files from online source.

Source	File Size(KB)	Time Consumed Existing(ms)	Time consumed proposed(ms)
Offline	20	12	10
Offline	22	15	11
Offline	50	21	19
Offline	65	25	25
Offline	85	29	28
Online	1024	--	40
Online	2048	--	88
Online	3000		100
Online	3987		176

Table 2: Time Consumption Comparison

Received: 15 May 2018/Accepted: 20 June 2018

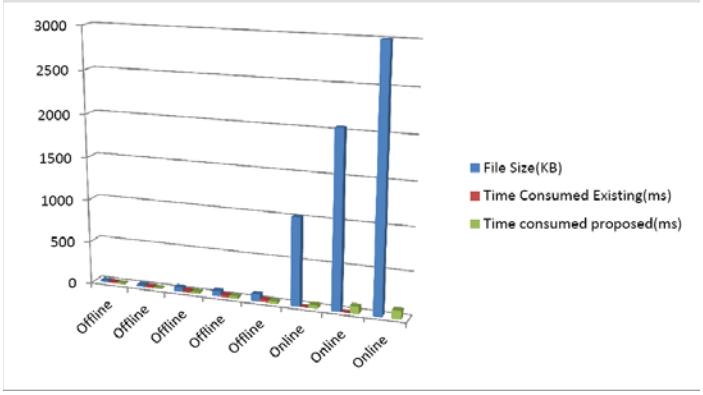


Figure 2: Plot of time consumption

Time consumption can further be worked upon and can be minimized using technique of deduplication along with random key in encryption process. Time consumption also greatly depends speed with which internet works. Slow speed of internet causes higher time consumption than lease line internet connection.

5. CONCLUSION

Cloud computing not only provides the resources to the users but also give a big challenge of security. There are securities requirements for both users and cloud providers but sometimes it may conflict in some way. Security of the cloud depends upon trusted computing and cryptography. In our review paper some issues related to data location, security, storage, availability, and integrity. Establishing trust in the cloud security is the biggest requirement. The problems and corresponding solutions may be required further investigation in terms of key size and complexity. The complexity of key can be further enhanced by the use of pseudo-random number generator within the key generation phase. By incorporating complex key structure, cloud performance and user interaction can be further enhanced using complex keys and by reducing attacks.

REFERENCES

[1] F. Sabahi, "Cloud Computing Security Threats and Responses," pp. 245–249, 2011.
[2] X. Wu, R. Jiang, and B. Bhargava, "On the Security of Data Access Control for Multiauthority Cloud Storage Systems," pp. 1–14, 2015.
[3] J. Aikat et al., "Rethinking Security in the Era of Cloud Computing," no. June, 2017.
[4] K. Hwang, X. Bai, Y. Shi, M. Li, W.-G. Chen, and Y. Wu, "Cloud Performance Modeling with Benchmark Evaluation of Elastic Scaling Strategies," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 1, pp. 130–143, Jan. 2016.
[5] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 367–380, Feb. 2016.
[6] M. Armbrust et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, p. 50, 2010.
[7] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," Proc. - 10th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2008, pp. 5–13, 2008.
[8] S. J. Nirmala, N. Tajunnisha, and S. M. S. Bhanu, "Service provisioning of flexible advance reservation leases in IaaS clouds," vol. 3, no. 3, pp. 154–162, 2016.
[9] M. Marwan, A. Kartit, and H. Ouahmane, "Secure Cloud-Based Medical Image Storage using Secret Share Scheme," 2016.
[10] D. V. Dimitrov, "Medical internet of things and big data in healthcare," Healthc. Inform. Res., vol. 22, no. 3, pp. 156–163, 2016.
[11] J. Li, J. Li, X. Chen, C. Jia, W. Lou, and S. Member, "Identity-based Encryption with Outsourced Revocation in Cloud Computing," pp. 1–12, 2013.
[12] S. Seo, M. Nabeel, and X. Ding, "An Ef fi cient Certi fi cateless Encryption for Secure Data Sharing in Public Clouds," pp. 1–14, 2013.
[13] S. Wang, J. Zhou, J. K. Liu, J. Yu, and J. Chen, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing," vol. 6013, no. c, pp. 1–13, 2016.
[14] D. Xu, C. A. I. Fu, G. Li, and D. Zou, "Virtualization of the Encryption Card for Trust Access in Cloud Computing," vol. 5, 2017.

Received: 15 May 2018/Accepted: 20 June 2018

[15] A. Alabdulatif, H. Kumarage, I. Khalil, M. Atiquzzaman, and X. Yi, "Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure," IET Wirel. Sens. Syst., vol. 7, no. 6, pp. 182–190, 2017.
[16] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE : Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage," vol. 1374, no. c, pp. 1–12, 2016.
[17] L. Jiang, D. Guo, and S. Member, "Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage," vol. 5, 2017.
[18] C. Liu, S. Member, L. Zhu, J. Chen, and S. Member, "Graph Encryption for Top-K Nearest Keyword Search Queries on Cloud," vol. 3782, no. c, pp. 1–11, 2017.
[19] C. Song, Y. Park, J. Gao, S. K. Nanduri, and W. Zegers, "Favored Encryption Techniques for Cloud Storage," pp. 267–274, 2015.
[20] N. Veeraragavan, "Enhanced Encryption Algorithm (EEA) for Protecting Users ' Credentials in Public Cloud."
[21] S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight Searchable Public-key Encryption for Cloud-assisted Wireless Sensor Networks," IEEE Trans. Ind. Informatics, vol. XX, no. XX, pp. 1–12, 2017.
[22] M V Narayana, G Narsimha, SSVN Sarma, "Secure- ZHLS: Secure Zone Based Hierarchical Link State Routing Protocol using Digital Signature", International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22927-22940.
[23] K. L. Tsai et al., "Cloud encryption using distributed environmental keys," Proc. - 2016 10th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2016, pp. 476–481, 2016.
[24] A. El-yahyaoui, "A verifiable fully homomorphic encryption scheme to secure big data in cloud computing," 2017. G. Thomas, "Cloud computing security using encryption technique," pp. 1–7.

Received: 15 May 2018/Accepted: 20 June 2018