THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Cloud Portability and Reliability Enhancement Using Encryption Mechanism

Mehak Gandhi

Department of Computer Science &Engineering

Lovely Professional University

Phagwara,Punjab,India

Mehak.23620@lpu.co.in

Keshav Dhir

Department of Computer Science &Engineering

Lovely Professional University

Phagwara,Punjab,India

Keshav.25128@lpu.co.in

Abstract: Cloud computing as per now is heart and soul of new era. Internet based computing is supported through the services provided by cloud computing. Interactive services including infrastructure, network access, provisioning and platform is provided through distributed or cloud computing. As services grows so does the users. Users can be malicious in nature and may lead to attack. This situation is required to be prevented. Security of cloud hence becomes critical. This paper discuss about encryption algorithm that are used to generate complex keys in cloud security. This method is more efficient because it gives versatile key that is efficient. The experimental result is shown in the given paper that is better than existing approach.

Keywords: Cloud computing, Encryption, Security.

I. INTRODUCTION

Cloud computing provides resources or services both in terms of hardware and software using network (typically internet). Physical machines thus can perform operations beyond their capabilities. Cloud provides services including IaaS, PaaS and SaaS. Everything user needs is physically close to them hence extensive use of cloud is on the prospect. As users increases so does security threats. Cloud resources could be the target through application of attacks. Several techniques being suggested and research over to avoid critical consequence ofthreats.

[1]Cloud computing becomes need of the hour since unlimited resources are up for grabs at absolutely low cost. Cost is encounters on the basis of pay per use. Due to benefits associated with cloud, large number of users interacted with cloud to use resources provided by cloud computing.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

IaaS

[3]Cloud provides virtualized computing resources over the internet through the use of IaaS(Infrastructure as a Service). It can be scaled up or down depending upon requirement of users. IaaS is extremely useful in continues changing environment. Characteristics of IaaS are listed asunder

- Virtualized computing resources provided byIaaS.
- IaaS service size is dynamic indicating that it can be scaled up or down depending uponrequirements.
- Policy based services critically associated withIaaS.
- Automated administrative tasks being used in IaaS.
- Pay per use eliminate capital expenses fromIaaSs

PaaS

[4]Platform as a service is also crucial service generated through cloud computing. User does not have to worry about the infrastructure through PaaS. Platform provided through cloud, utilized by users as if platform including operating system is loaded within user's machine. PaaS is also known as application platform service. Following features accompanied withPaaS

- Application execution platform is provided through the use ofPaaS.
- Support for higher level programming without additional cost andoverhead.
- Application maintenance and enhancement iseasy.
- Useful in multi user environment where multiple developers are operating on single developmentproject.

SaaS

[5]Software as a service is another asset associated with cloud owing to its success. Software plus services is another designated name assigned to SaaS. Licensed software are centralised hosted within cloud are accessed by users on pay per use basis. Features associated with SaaS are described asunder

- Multitenant architecture is followed withinSaaS.
- It is possible to use software meant for specific business industry known as verticalSaaS.
- It is possible to use software meant for general business industry known as horizontalSaaS.
- Open integration protocol is used within SaaS forcustomization.

The security and authentication mechanisms are required to be enforced at each level of service provided with the help of cloud.

II. LITERATURE SURVEY

Cloud computing as per now is heart and soul of new era. Internet based computing is supported through the services provided by cloud computing. Interactive services including infrastructure, network access, provisioning and platform is provided through distributed or cloud computing. As services grows so does the users. Users can be malicious in nature and may lead to attack. This

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

situation is required to be prevented. Security of cloud hence becomes critical. Security technique suggested by [6] includes one to many probabilistic order preserving encryption. Differential attacks are explored over the OPE (order preserving encryption). Background information of outsources document can lead to accurately predicting attacking nodes and preserving cipher text. Another security mechanism suggested by [7]. You et al. uses channel estimation error as base criteria for security breech detection. Channel estimation errors as increases security breech becomes more common. Outage and intercept probability is used to minimize the error in channel estimation to reduce attack probability. [9]proposed bidirectional authentication mechanism, statistical analysis and load balancing strategy was also suggested through analysed approach. Primarily storage security was considered.[10][11]proposed techniques and challenges associated with cloud computing. Comparison of techniques used for security purposes were mentioned and described through this literature. Because of security issues enterprises prefer to keep less sensitive data within cloud. [12]proposed memory replication mechanism to enhance security concern within LTE cloud. Replication procedure includes copying of sensitive information at multiple places. In case of failure sensitive information can be recovered from other replicated images. Storage space was heavily used in this approach. [13] proposed credit based scheduling using deadline mechanism for enhancing security and allowing the task to finish well within suggested time period. [14]proposed block level encryption within cloud. Block level encryption mechanism allows reduces redundancy along with encryption for security. Primarily public key encryption mechanism was used in block level encryption. [15]proposed analysis of various cloud computing security techniques along with issues associated with security concerns.

III. METHODOLOGY

Cloud computing as per now is heart and soul of new era. Internet based computing is supported through the services provided by cloud computing. Interactive services including infrastructure, network access, provisioning and platform is provided through distributed or cloud computing. As services grows so does the users. Users can be malicious in nature and may lead to attack. This situation is required to be prevented. Security of cloud hence becomes critical. Security technique suggested by [6] includes probabilistic order preserving encryption. Differential attacks are explored over the OPE(order preserving encryption). Background information of outsources document can lead to accurately predicting attacking nodes and preserving cipher text. Another security mechanism suggested by [7]. You et al. uses channel estimation error as base criteria for security breech detection. Channel estimation errors as increases security breech becomes more common. Outage and intercept probability is used to minimize the error in channel estimation to reduce attack probability. This paper presents concise but all round analysis of security concerns associated with cloud computing. Finally this literature presents future security work leading to protection of cloud data. The objectives associated with this approach is as under

- Introduce new redundancy handling mechanism to remove distinct keys associated with similar data.
- By removing redundancy, reliability can be ensured.
- Reducing cost of storage by eliminating redundant data and replace it with singular key Parameters for optimization

- Cost in terms of storage space requirements since cloud cost is on the basis of pay per use. more usage means more cost
- Space requirements reduces in case redundant data is limited
- Computational overhead is reduced in case number of keys reduces

The methodology describes the step to be followed to achieve desired security levels within cloud system. The detail steps are as under

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

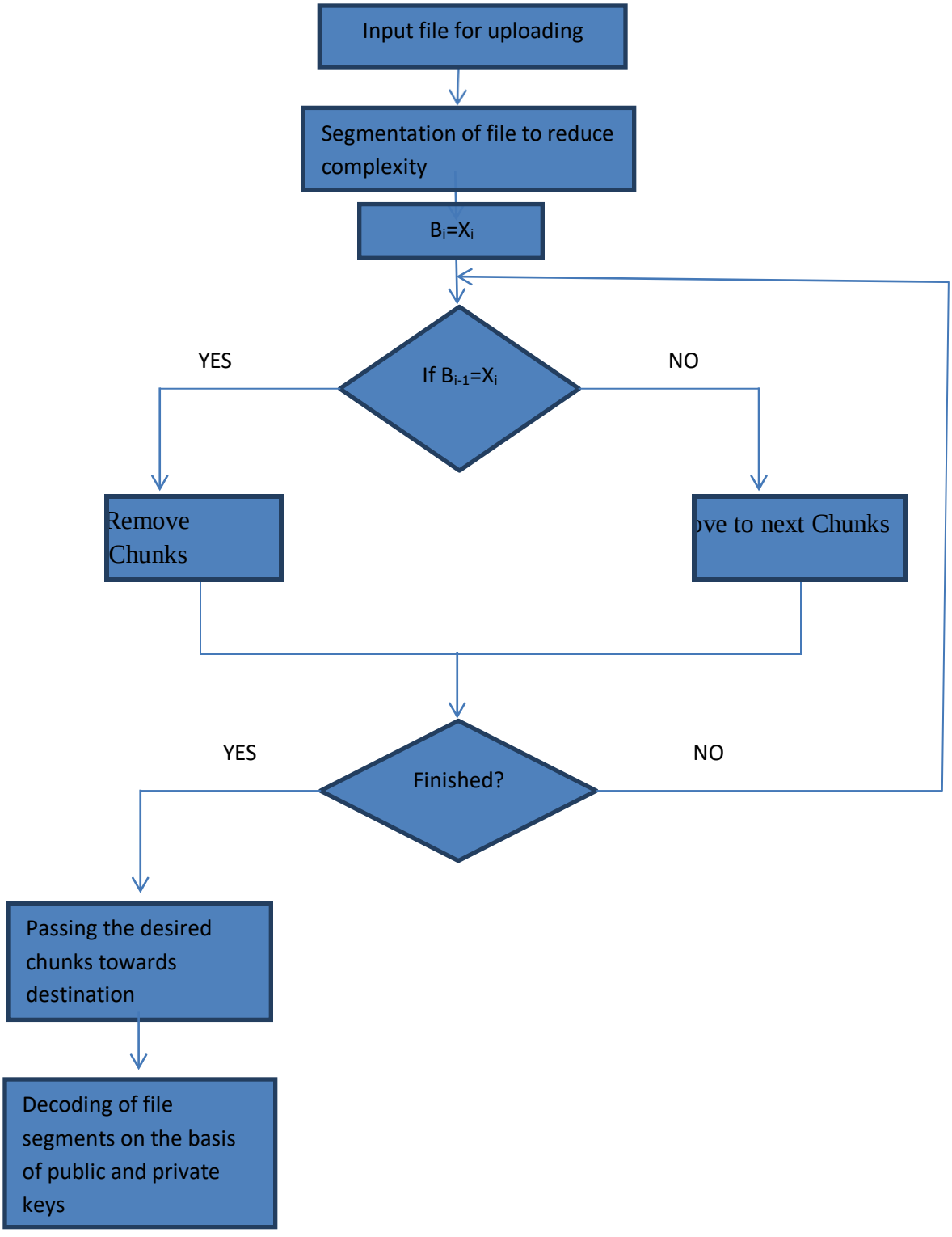

Figure 1.1 Security levels in cloud

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

IV. RESULTS AND PERFORMANCE ANALYSIS

The results given below describe about the simulation time produced by existing and proposed key generator for handling replication data in cloud computing. The results proposed are much better than existing methodology.

Table 1 Simulation Time of Existing and Proposed Methodology

Input File Size	Existing Key Size	Proposed Key Size
49	5.5	4.5
60	6	5.5
100	7.5	6
103	8.5	7.5
106	9	8

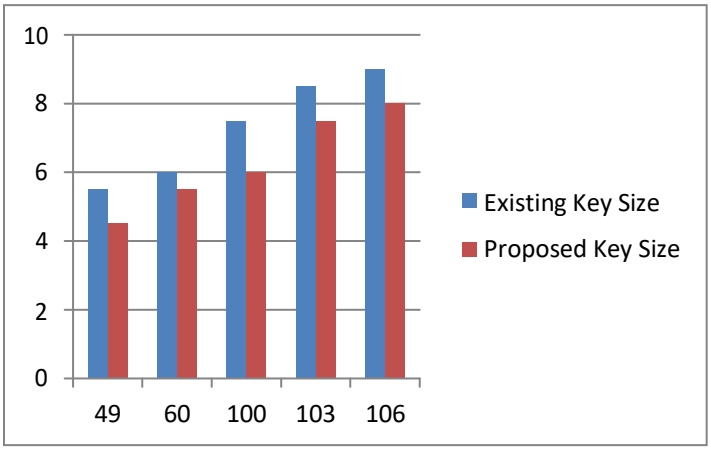

Figure1.2 Key Size Comparison chart

V. CONCLUSION

Security techniques are critically accompanied requirement within cloud system. Cloud system comes into exposure to wide variety of users. Some users out of millions at exposure to cloud may able to distort the working of cloud system hence forth many of the enterprise do not prefer sensitive data storage within cloud system. In order to resolve the problem access control, roles and other distinct mechanisms were defined within cloud system to enhance security. In this paper we propose a key based redundancy handling mechanism for enhancing security within cloud system. The key generated is complex in nature and provide efficient mechanism of tackling security issues by the use pseudo random generator for key. After key is generated and replication is handled file is uploaded on the cloud. By doing so security is enhanced and result is improved by 10 to20%.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

VI. REFERENCES

[1] N. Wahidah, B. Ab, K. Jenni, S. Mandala, and E. Supriyanto, "Review On Cloud Computing Application In P2P Video Streaming," *Procedia - Procedia Comput. Sci.*, vol. 50, pp. 185–190,2015.

[2] J. Aikat*et al.*, "Rethinking Security in the Era of Cloud Computing," no. June,2017.

[3] B. Nicolae, "BlobCR : Efficient Checkpoint-Restart for HPC Applications on IaaS Clouds using Virtual Disk Image Snapshots."

[4] C. Pahl and I. Centre, "Containerization and the PaaS Cloud,"2015.

[5] R. Buyya, "Introduction to the IEEE Transactions on Cloud Computing," vol. 1, no. 1, pp. 3–21,2013.

[6] K. Li, W. Zhang, C. Yang, and N. Yu, "Security Analysis on One-to-Many Order Preserving Encryption Based Cloud data Search," vol. 6013, no. c, pp. 1–9,2015.

[7] J. I. A. You, Z. Zhong, G. Wang, B. O. Ai, and S. Member, "Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors," vol. 2,2014.

[8] X. Wu, R. Jiang, and B. Bhargava, "On the Security of Data Access Control for Multiauthority Cloud Storage Systems," pp. 1–14,2015.

[9] B. Feng *et al.*, "An Efficient Protocol with Bidirectional Verification for Storage," vol. 3536, no. c, pp. 1–13,2016.

[10] G. Thomas, "Cloud computing security using encryption technique," pp.1–7.

[11] F. Sabahi, "Cloud Computing Security Threats and Responses," pp. 245–249,2011.

[12] S.Abdelwahab,B.Hamdaoui,M.Guizani and T.Znati, "REPLISOM : Disciplined Tiny Memory Replication for Massive IoT Devices in LTE Edge Cloud," vol. 4662, no. c,2015.

[13] A. Sharma and S. Sharma, "Credit Based Scheduling Using Deadline in Cloud Computing Environment," *ACM Comput. Surv.*, pp. 1588–1594,2016.

[14] Y. Zhao and S. S. M. Chow, "Updatable Block-Level Message-Locked Encryption," *ACM*, pp. 449–460,2017.

[15] P. You, Y. Peng, W. Liu, and S. Xue, "Security Issues and Solutions in Cloud Computing," *IEEE Access*,2012.