IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-7 E-ISSN: 2347-2693

A Result Base Various Approaches of Data Security in Cloud Computing

Gurbachan Singh*, Er. Khushboo Bansal

Department of CSE, Desh Bhagat University

Available online at: www.ijcseonline.org

Received:13/Jun/2016 Revised: 23/Jun/2016 Accepted: 19/Jul/2016 Published: 31/Jul/2016

Abstract- *In this paper we are studied cloud computing techniques. The Homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions, and private information retrieval schemes and enable widespread use of cloud computing by ensuring the confidentiality of processed data.*

Keywords: *Encryptions, security, compression, validate data integrity*

I. INTRODUCTION

Cloud computing is a new concept in recent years, and a newly computing framework is proposed. Cloud computing is the development of distributed computing, parallel computing and grid computing [1]. The goal of cloud computing is to simplify the computing and storage for like public water and electricity, the user can be convenient to use these resources only could be connected to network, and to pay by the volume that they used. Cloud computing is usually have a distributed infrastructure, and can carry on real-time monitoring of the distributed system, in order to achieve the efficient usage of it [2]. The computing make computers act on the cloud and the computer makes parallel computing technology into people's life [3]. Users service themselves relying on some internet information resources which lie on some nodes, such as computing resources, software resources, data resources and management resources. This service framework emphasize the demand driven, user dominant, on-demand services, no centralized control and users don't care where the server. The parallel computing and virtualization technology has become the core support technology after the concept of cloud computing was put forward.

There are existing two means of cloud computing [4]. One aspect is describes the infrastructure, which used to construct applications and the role equivalents to the PC operating system: the other aspect is describes cloud computing applications based on the infrastructure. The different from grid computing is that cloud computing have a wider meaning about the computing platform, and can support the application of the grid. The existing implementation of cloud computing reflects characteristics of the following three aspects:

1) The hardware infrastructure established on large-scale and cheap server cluster.

2) The collaborative development between application and the underlying service, maximize the use of resources.

3) Through multiple redundancies between cheap servers, achieved high availability of software.

1.1 Architecture

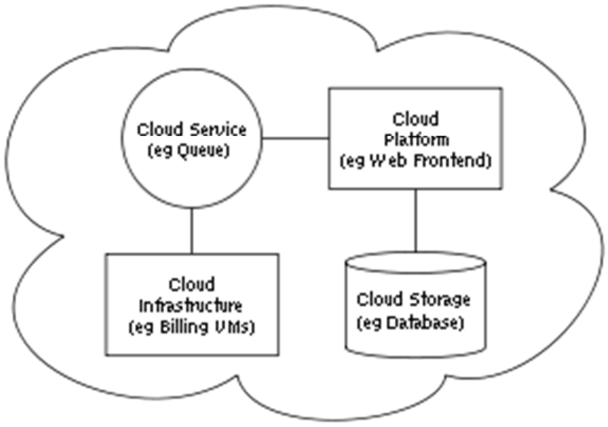

Figure 1.1 Architecture of Cloud Computing

Cloud structural engineering, the frameworks construction modelling of the product frameworks included in the conveyance of distributed computing, ordinarily includes numerous cloud components communicating with one another over a free coupling instrument. For example a message line. Elastic provision suggests insight in the utilization of tight or free coupling as connected to systems, for example, these and others.

2. Methodology Used

[1] At the first step, user sends the request for the validation of the data to the server.

[2] When the given request is accepted then it validates data and the private key will be generated.

[3] After the private key whole data will start uploaded and encryption will be done further.

[4] And if it does not validate then it will generate error message.

[5] At last if primary key is not matched then it will generate the re-password message or if it matches it will start downloading the data.

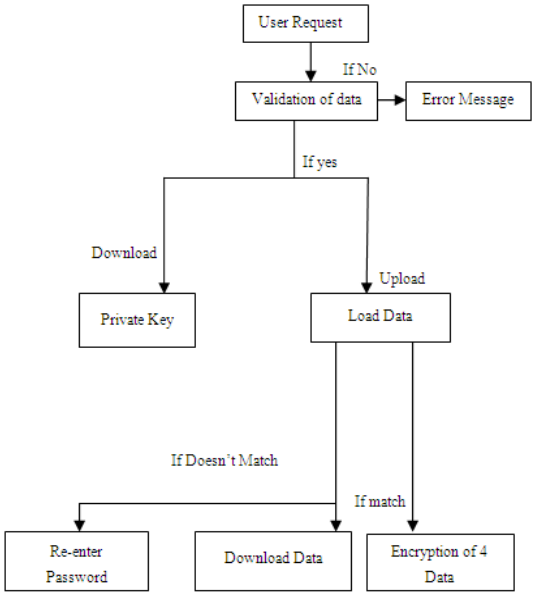

Figure 2 Flow diagrams for purposed work

3. RESULTS

4.1 Performance Analysis

Table 4.1 Encrypted File Size for encryption of data of different file sizes

Sr. No.	Files (in bytes)	Purposed work	Fully Homomor-phism	DES
		Encrypted Files (in bytes)		
1	2681	5276	6368	5768
2	3431	6964	8348	7688
3	4386	8684	13008	9668
4	5546	16304	19544	17704
5	22588	43184	55136	48912

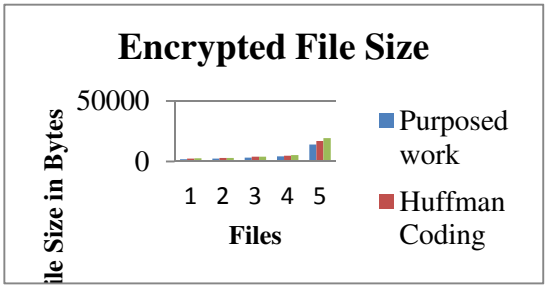

Figure 3 Comparison graph for encryption size after encryption

Figure 3 represents the comparison graph for encryption size using purposed approach and fully Homomorphic and DES approach.

Table 4.2 Computation time for encryption of data of different file sizes

Sr. No.	Files (in bytes)	Purposed work	Fully Homomor-phism	DES
		Time (in ms)		
1	2681	105	132	118
2	3431	125	165	142
3	4386	231	285	256
4	5546	302	365	343
5	22588	503	606	555

This table represents the value for computation time for encryption of different size files. The values for computation time have been evaluated for purposed work and fully homographic and DES encryption approach.

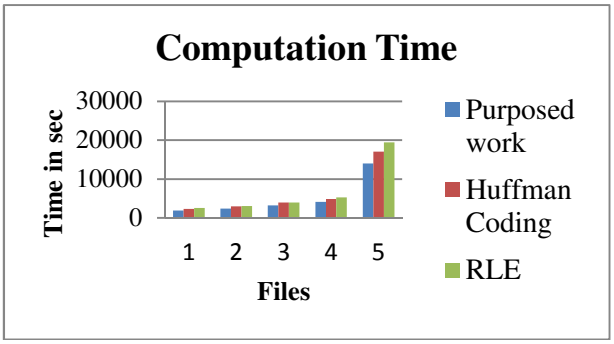

Figure 4 Comparison graph for computation time for encryption

This figure represents the comparison graph for computation time using purposed approach and fully Homomorphic and DES approach

Table 4.3 Compressed File Size after compression of data of different sizes

Sr. No.	Files (in bytes)	Purposed work	Huffman Coding	RLE
		Compressed File Size (in bytes)		
1	2681	1910	2346	2576
2	3431	2430	2995	3068
3	4386	3230	3964	4018
4	5546	4168	4864	5264
5	22588	14044	17048	19428

This table represents the value for compressed file size for encryption of different size files. The values for compression size have been evaluated for purposed work and Fully Homomorphic and DES encryption approach.

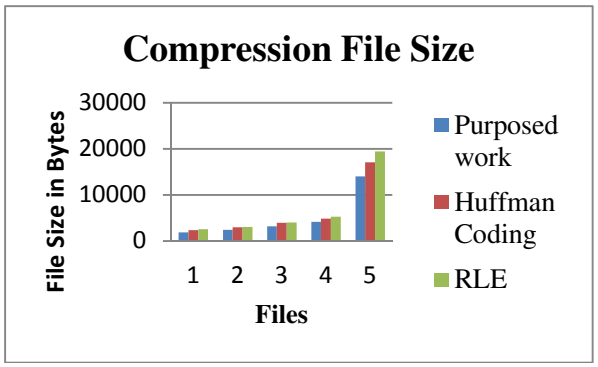

Figure 5 Comparison graph for compression file size after compression

This figure represents the comparison graph for compression file size using purposed approach and Huffman coding and RLE compression approach.

4. CONCLUSION & FUTURE SCOPE

In the previous work a diverse cryptography viewpoints that represent a danger to distributed computing are investigated. That is use to study the particular security issues brought by the utilization of cryptography in a distributed computing framework. In previous work to improve the learning items move-ability and interoperability is not just distributed computing API measures ought to be pushed by the key cloud suppliers additionally learning assets benchmarks ought to be characterized by the Open Cloud Computing Education Federation.

In the purposed work the data has been stored on the cloud by different users for secure purpose. The authorization of the users has been evaluated by providing different user name and email id. The user request transmit the cloud the cloud sends a secret key to the user and after this if the authorized user provide that key then the user can access the account. After this user have to store data on the cloud in secure manner by using homorphic encryption. The homomorphic encryption use different arithmetical and logarithmic formulas for conversion of data from secret information to cipher text. These operations provide the security to data because these are without key operations that have to be transmitted to the user. The purposed work provides better storage management of the data on the cloud environment. It also reduces the storage capacity of the data and can be easily stored on data. The purposed work the encryption size and compution time has been used for performance evaluation. The purposed work provide 15% more efficiecy than previous work using fully homomorphism and DES approach.

6.2 Future Work

In the future reference other compression and encryption approaches can be implemented on the cloud for security of the data. This purposed work can be used for efficient utilization of cloud environment.

REFRENCES

[1] Ahmed DheyaaBasha, Irfan Naufal Umar, and Merza Abbas, Member, IACSIT "Mobile Applications as Cloud Computing: Implementation and Challenge", 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, pp 467 – 471, 2013.

[2] Alabbadi, M.M "Cloud computing for education and learning: Education and learning as a service (ELaaS)", IEEE Conf. on Interactive Collaborative Learning (ICL), vol.134 , PP 589 – 594, 2011.

[3] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing", IEEE conf. on Parallel Distributed and Grid Computing (PDGC), pp.1-9, 2009.

[4] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE Trans. on Cloud Computing., vol. 11, no. 6, pp. 670 - 684, 2002.

[5] Gaurav Raj, Dheerendra Singh, Abhay Bansal, "Load balancing for resource provisioning using Batch Mode Heuristic Priority in Round Robin (PBRR) Scheduling", Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), pp. 308 – 314, 2012.

[6] Jianfeng Yang, Zhibin Chen "Cloud Computing Research and Security Issues" Computational Intelligence and Software Engineering (CiSE), Vol. 978-1-4244-5392, pp 1 – 3, 2010.
[7] Jaber, A.N. "Use of cryptography in cloud computing", IEEE Control System, Computing and Engineering (ICCSCE), PP 179 – 184, 2013.
[8] Kalagiakos, P. Karampelas, P "Cloud computing learning" IEEE Application of Information and Communication Technologies (AICT), pp. 1 – 4, 2011.
[9] Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth "A Layered Security Approach for Cloud Computing Infrastructure" 2009 10th International Symposium on Pervasive Systems, pp 763 – 767, 2009.
[10] Md. Imrul Kayeset al. "Test Case Prioritization for Regression Testing Based on Fault Dependency" 2009 10th International Symposium on Pervasive Systems,pp.3-11, 2013
[11] Mohammed Achemlal, Saıd Gharoutand Chrystel Gabber "Trusted Platform Module as an Enabler for Security in Cloud Computing" Network and Information Systems Security (SAR-SSI),, Vol. 978-1-4577-0737, pp.7-11, 2011.
[12] Sravan Kumar R, AshutoshSaxena "Data Integrity Proofs in Cloud Storage", 2011 Third International Conference on Communication Systems and Networks, Vol. 978-0-7695-4355,pp.03/11, 2011.
[13] Qiang Guan, Chi-Chen Chiu, Song Fu "A Cloud Dependability Analysis Framework for Characterizing System Dependability in Cloud Computing Infrastructures"IEEE International Conference on Dependable Computing, pp. 11 – 20, 2012.
[14] RuWei Huang, Si Yu, Wei Zhuang and Xiao Lin Gui, "Design of Privacy-Preserving Cloud Storage Framework" IEEE Ninth International Conference on Grid and Cloud Computing, pp. 128 – 132,2010,
[15] RuWei Huang, Si Yu, Wei Zhuang and Xiao Lin Gui, "Research on Privacy-Preserving Cloud Storage Framework Supporting Cipher text Retrieval"IEEE Ninth International Conference on Grid and Cloud Computing,pp.6-10,2011.
[16] Ranjita Mishra, Sanjit Kumar Dash "A Privacy Preserving Repository for Securing Data across the Cloud" IEEE International Conference, Vol 978-1-4244-8679, pp.6-10, 2011.
[17] Ryan K. L. Ko, Markus Kirch berg, Bu Sung Lee "From System-centric to Data-centric Logging – Accountability, Trust & Security in Cloud Computing" IEEE International Conference on Computer Society,pp. 1 – 4, 2011.
[18] Sang-Ho Na, Jun-Young Park, Eui-Nam Huh "Personal Cloud Computing Security Framework" IEEE Asia-Pacific Services Computing Conference,pp. 671 - 675 ,2010.
[19] Shucheng Yu, CongWang, Kui Ren and Wenjing Lou "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" at IEEE INFOCOM ,pp. 1 - 9 ,2010.
[20] Sravan Kumar R, AshutoshSaxena "Data Integrity Proofs in Cloud Storage" IEEE International Conference on Communication Systems and Networks,Vol. 978-0-7695-4355,pp. 1 – 4, 2011.
[21] Sheikh, F.B., Haider, S., "Security threats in cloud computing", IEEE International Conference Internet Technology and Secured Transactions, pp.214 – 219, 2011.
[22] Sabahi, F., Shahrekord, "Cloud computing security threats and responses", IEEE International Conference on Communication Software and Networks, pp.245 – 249, 2011.
[23] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," IEEE 1st International Conference on Parallel, Distributed and Grid Computing,pp.234-238 ,2010.
[24] Victor Echeverr´ıa, Lorie M. Liebrock, and Dongwan Shin "Permission Management System: Permission as a Service in Cloud Computing" IEEE Computer Software and Applications Conference Workshops,pp. 371 – 375, 2010.
[25] Wang En Dong "Oriented Monitoring Model of Cloud Computing Resources Availability", IEEE International Conference on Computational and Information Sciences, vol. 13874396, pp.1537 – 1540, 2013.
[26] Wentao Liu, Wuhan Poly tech., "Research on cloud computing security problem and strategy", IEEE International Conference on Consumer Electronics, Communications and Networks, pp.1216 – 1219, 2012.
[27] Xiao Zhang, Hong-tao Du ,Jian-quan Chen, Yi Lin, Lei-jie Zeng "Ensure Data Security in Cloud Storage" IEEE International Conference on Network Computing and Information Security vol.978-0-7695-4355pp.284-287,2011.

