# An Efficient Cloud Security And Data Access Protocol Using Ebfish Approach

Yogesh Vishwakarma

***Abstract: Cloud computing is technique where multiple data unit can be process over large component architecture. Different data entity unit participate in communication and provide response to user request. Data computation mechanism and storage in secure format is main task performed by cloud. Data accessing, data auditing is again delivery duty by cloud. In this paper previous security mechanism performed by cloud and their limitation is discussed. Here previous auditing hashing technique is also discussed. Our proposed approach describes the solution for proper security which enhances the blowfish algorithm given in existing model. Our experiment performed using Java8 using security library and new version of security algorithm implemented by us. Proposed result shows the efficiency in computation derived by our algorithm.***

***Keywords: Cloud security , cloud data access, hashing approach, Blowfish , Security operations.***

## I. INTRODUCTION:

Cloud computing is a conversational expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud computing is a term without a commonly accepted demonstrable scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time.

The phrase is also more commonly used to refer to network-based services which appear to be provided by real server hardware, which are in fact served by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the necessity without affecting the end user. Single cloud means a network which alone provides facilities to all user requests and also manages software and hardware to the users.

**Challenging issues in single cloud**

Single cloud creates a large number of security issues and challenges. A list of security threats to Single cloud is presented. These challenges are ranged from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the Single cloud implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection on the data.

Even if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud service provider and the cloud user is considered a general backbone in cloud computing.

They proposed a technique a theoretical framework for the design of proof of retrievability ,they have proven their work best on the previous retrievable techniques and they have proposed a variant on the Juels-Kaliski protocol and describe a prototype implementation. We demonstrate practical encoding even for files F whose size exceeds that of client main memory. also they have worked on consider the challenges encountered when designing practical POR protocols. First, we show how to construct outer codes that can encode large files efficiently, while still preserving a high minimum distance.

We define and construct practical adversarial error-correcting codes that, intuitively, give no advantage to an adversary in corrupting the encoded file than distributing corruptions randomly across file blocks. Secondly, as random disk access is expensive, we present techniques to encode large files incrementally, in only one pass through the file. Finally they have concluded their work that they got output and achieves lower storage overhead, tolerates higher error rates, and can be proven secure in a stronger adversarial setting. Finally, we provided a Java implementation of the encoding algorithm of the new variant, in which files are processed and encoded incrementally, i.e., as they are read into main memory and the further work according to them further optimization and well work in proofing of original file can be done on the system.

## II. LITERATURE REVIEW:

In this paper [1] they have proposed protocol to support public verifiability. The proposed protocol supports public verifiability without help of a third party auditor. In addition, the proposed protocol does not leak any private information to third party verifiers. Through a formal analysis, we show the correctness and security of the protocol. After that, through theoretical analysis and experimental results and proven the performance of their proposed work is very good as compare to the existing work a remote data integrity checking protocol that

supports data dynamics which was proposed earlier in previous work, they have worked on their work in order to compute Communication, Computation and Storage Costs –the various cost produce while The communications between the verifier and the server occur in the Challenge and GenProof steps, and analyze the computational cost of client, server and verifier .

Their proposed work produces proposed protocol supports data dynamics at the block level, which includes block insertion, block modification and block deletion. Our protocol can easily support dynamic data updates because the tagging was depending on the content available on block of data, each data tag depends only on block not on any other statistics. finally they have concluded their work as proposed protocol supports data insertion, modification and deletion at the block level, and also supports public verifiability. The proposed protocol is proved to be secure against an untrusted server. It is also private against third party verifiers, and the proven technique by them was in terms of costing and experimentally and practically approach was proven as best as they determined to be done and still the work on exact mapping between data and tags need to be improved was mentioned by their research future work, the objective to achieve data level Dynamics at minimal costs in future work.

They [2] present a scheme for data storage retrievability in Cloud Computing using third party audit (TPA), which can fulfill the demands of data integrity, data confidentiality, data extraction, credibility control of third-party audit etc. they have proposed the three tier work and taken tpa-third party authenticator, csp-cloud service provider and user and the architecture proposed in this way

The overall summarized is stated that we have discussed the various papers taken into consideration and the techniques have been used ,also we have summarized here the participants in this architecture and we described the sample interaction scheme in the scenario of data integrity verification techniques.

Performance of the monitored system was taken and computational cost, client and server communication cost is monitored in all the defined techniques in order to prove the best technique over the previous which they have discussed.

## III. PROBLEM DESCRIPTION

The traditional cryptographic technologies for data integrity and availability, based on Hash functions and signature schemes cannot work on the outsourced data. In the base paper attribute based encryption algorithm used which is again the problem while working with the attribute, there should be identical knowledge about the parameters. Attribute based encryption work well towards while the knowledge of all the parameter is required.

Attribute based encryption technique is not efficient while a robust searching and file accessing system is required, where the file knowledge and data decryption should not be performed by any of the meaning.

It is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. Moreover, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users.

Therefore, it is crucial to realize public audit ability for CSP, so that data owners may resort to a third party auditor, who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data.

The proposed work given an architecture where the strong combination of symmetric key encryption and the latest version of SHA-2 hashing technique is utilized where a strong environment structure is produced by our algorithm.

## IV. PROPOSED WORK

Proposed work and Algorithm Overview:

In order to prove our best among the available recent algorithm taken combination is of recent encryption technique for data security storage and further hashing function technique SHA-2 is using for the dynamic integrity verification process. Our proposed system also used RSA algorithm for the data security and data processing for the upload over the cloud server and simulation performance.

SHA-2 contains the key length of 256 bit which is not breakable with the brute force attack system which is the key main point of the hashing scheme, also the MAC security provided in case of encryption where the highest number of security is being transformed.

Our proposed work aims to provide a high security combination approach while dealing with the cloud security approach, as the general method either work with the security encryption or hashing data verification technique. Thus our proposed work implied which work on both the area as a algorithm where the data hash value is calculated at the time of implementing encryption and data storage performance into the cloud data center.

Further the SHA2 hash code is used to generate as challenge from the TPA side and then a response form generation from the cloud side. Thus the data verification process works with the help of hashing technique SHA-2 function.

RSA algorithm makes use of symmetric encryption advantage and help in working with the same key usage with different attribute.

## V. EXPERIMENTAL & RESULT ANALYSIS

In order to perform experiment to justify our proposed security algorithm over the existing work, a setup over Netbeans Tool using JDK 8 is performed. A server setup using WAMP server is executed and data store is described. A parameter such as computation time and cost is computed and compared with existing security algorithm.

Computation time: A time different between the process completion and process initialization is computed and called as computation time.

Ct= final after execution time in ms – initial time in ms

Ct= Fi-Ini;

Where Ct is computation time, Fi is final execution time monitored and Ini is initial execution time monitored.

As per the understanding of scenario we have further establish the Apache framework using Java language and Swing framework.

**Result analysis**

As the requirement of the system and implemented by us here is the comparison analysis is made based on the key size, server computation time, TPA computation time where the system proven our proposed scenario as best among the available technique.

| Technique Approach | Data size 10 KB (computation time in ms) | TPA Verification time (in ms) | Data size 50 KB(computation time in ms) | TPA Verification time(in ms) |
|---|---|---|---|---|
| **AES Algorithm** | 400 | 573 | 582 | 568 |
| **Blowfish Algorithm** | 134 | 231 | 242 | 236 |
| **RC4 Algorithm** | 20 | 29 | 36 | 42 |
| **RSA Algorithm** | 573 | 454 | 674 | 786 |
| **Blowfis** | 9 | 23 | 14 | 13 |
| **h2-256 Proposed** | | | | |

Table 1 – comparison in terms of Computation time

| Technique Approach | Data size 10 KB (computation cost in $) | TPA Cost | Data size 50 KB(computation time in ms) | TPA Cost |
|---|---|---|---|---|
| **AES Algorithm** | 12.1 | 18.21 | 14.53 | 13.4 |
| **Blowfish Algorithm** | 10.43 | 21.54 | 12.795 | 19.32 |
| **RC4 Algorithm** | 19.32 | 12.76 | 30.52 | 43.46 |
| **RSA Algorithm** | 43.2 | 46.45 | 34.2 | 37.45 |
| **Blowfish 2-256 Proposed** | 9,59 | 12.34 | 11.21 | 17.43 |

In the table above the data shows the static discussion analysis for computation time in between existing and proposed technique performed by the system. As per the result monitored above shows the efficiency of our algorithm. This proves the better approach and efficiency of our proposed work system.

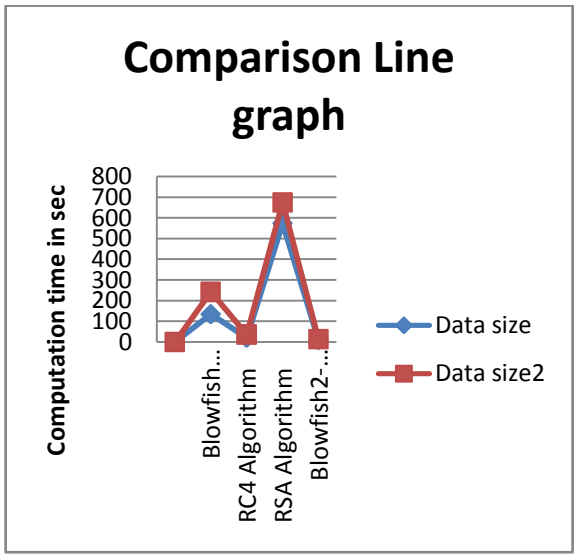


Figure 1 – Graphical Analysis of key system

In the figure 1 above the comparison analysis graphically is defined where the system architecture with given graph is mentioned. In the presence of graph above it is stated that the proposed algorithm work efficient while comparing with existing technique.

## VI. CONCLUSION

Cloud environment and security over the cloud is an important factor to work on. The considered existing and proposed work were performed and implemented using Java Apache Framework and thus the result were monitored using different considered parameter. As per our observation the proposed algorithm is efficient and reliable in terms of encryption scheme which follow symmetric key encryption and also in case of integrity verification which is the latest hashing SHA volume to prove and execute our system over the existing algorithm.

Our approach found the advantage of RSA encryption algorithm over the existing Attribute based encryption. Which make advantage of symmetric key encryption and performed the fast process over the existing work scenario to prove the efficiency of our algorithm. Our work is computed using the parameter computation time which is efficient than existing attribute based encryption algorithm.

The security and integrity verification in cloud is always required as the number of users and portals are switching their workspace to the cloud environment instead of traditional server configuration. thus our work in this field lead the solution to store and verify the originality of available scenario.

## VII. FUTURE WORK

As per discussion the proposed algorithm outperforms best in its field where both the encryption and hashing perform best among. Our further work is going to perform real time implementation algorithm in computed real scenario application.

A experiment and real live platform is going to provide the new interface for user to interact and share their file system with secure manner.

## REFERENCES

[1]. Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE2014, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing"

[2]. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering 2012.

[3]. Boyang Wang, Baochun Li, Hui Li," Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," IEEE TRANSACTIONS ON Cloud Computing, VOL. 2, NO. 01, March 2014.

[4]. "The Notorious Nine - Cloud Computing Top Threats in 2013," https://downloads.cloudsecurityalliance.org/initiatives/top_threats

[5]. "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, VOL. X, NO. X, XXXX 2014, accepted.

[6]. Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou, "A Hybrid Cloud Approach for Secure Authorized Deduplication", IEEE Transactions on Parallel and Distributed Systems, 2014.

[7]. Lluis Pamies-Juarez, Pedro Garc__a-L_opez, Marc S_anchez-Artigas, Blas Herrera, "Towards the Design of Optimal Data Redundancy Schemes for Heterogeneous Cloud Storage Infrastructures" ," Computer Networks, Vol.55, 1100-1113, 2011.

[8]. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering 2012.

[9]. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73,2012.

[10]. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li," Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"Proc. IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011 .

[11]. D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from theWeil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), pp. 514-532.

[12]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[13]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.