

# Improvement in Cloud Storage Auditing with Verifiable Outsourcing of Secure Key

**M.Tech.Scholar Tanuj Sharma**

Department of CSE  
SAMCET, Bhopal  
Madhya Pradesh, India  
Sharmatanuj048@gmail.com

**Asst.Prof. Lakhan Singh**

Department of CSE  
SAMCET, Bhopal  
Madhya Pradesh, India  
sisodiya.lakhan53@gmail.com

**Asst.Prof. Ankur Taneja**

Department of CSE  
SAMCET, Bhopal  
Madhya Pradesh, India  
ankurtaneja5@gmail.com

**Abstract** – Presentation Cloud registering is a current mechanical advancement in the processing field in which for the most part centered around outlining of administrations which can be given to the clients in the same route as the fundamental utilities like nourishment, water, gas, power, and communication. Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. In Existing system, there are following associate problems which are worked on our proposed work AES-256 is quite common and easily available for hacker activity in case it desire to break. Highly indexed data structure is not taken in the Existing system. In this paper we are using a stander SHA-2 algorithm for message key generation and for data encryption used optimized Bluefish algorithm after the completed of these process we also find the proxy server in cloud system. For simulation we used cloudsims a java based simulator.

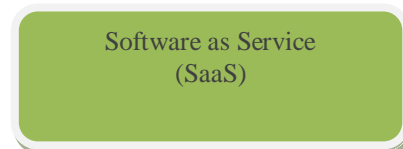
**Keywords** – cloud computing, cloud security, security issues etc.

## I. INTRODUCTION

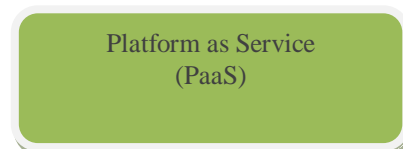
Cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its uses and providers. CLOUD computing, as a new technology paradigm with promising further, is becoming more and more popular nowadays.

It can provide users with unlimited computing resource. Enterprises and people can outsource time-consuming computation workloads to cloud without spending the extra capital on deploying and maintaining hardware and software. In recent years, outsourcing computation has attracted much attention and been researched widely. It has been considered in many applications including scientific computations.

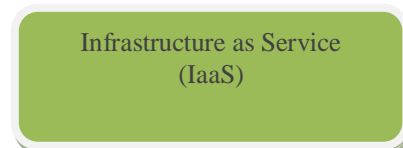
However, it needs to satisfy several new requirements to achieve this goal. Firstly, the real client's secret keys for cloud storage auditing should not be known by the authorized party who performs outsourcing computation for key updates. Otherwise, it will bring the new security threat. So the authorized party should only hold an encrypted version of the user's secret key for cloud storage auditing. Secondly, because the authorized party performing outsourcing computation only knows the encrypted secret keys, key updates should be completed under the encrypted state.



SaaS:- Consumer Can Run Application in cloud



PaaS:- Consumer gets an open platform/Solution



IaaS:- Network, Processing Storage

FIG. 1 Cloud Service Models.

## II. PROBLEM STATEMENT

- In Existing system, there are following associate problems which are worked on our proposed work :
- AES-256 is quite common and easily available for hacker activity in case it desire to break.
- Existing accessing and storage scheme is slow in terms of computation time and process.
- Thus it exhibit high cost while storage of data, providing its availability to access.
- The existing algorithm use model which is still extension is required for proper loose coupling.
- Previous approach having limitation of accessing data from large structure of dataset.
- Highly indexed data structure is not taken in the base paper, which further need analysis of high end access.

### III. PROPOSED WORK

- The proposed work can be done in accordance of working with security and storage over the various available components.
- A product information outsourcing and searching system model including the data owner, cloud server and data users is designed.
- Two index structures supporting efficient product retrieval are constructed. Moreover, corresponding search algorithms are also proposed.
- Cloud storage auditing protocol with secure outsourcing of key updates is composed by Eight algorithms (SSetup, EUpdate, VESK, DESK, AuthGen, Proof- Gen, Proof Verify and Check ProxyTPA).

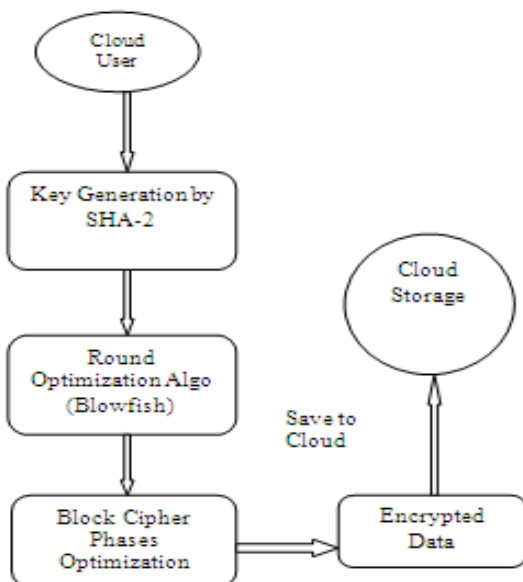


Fig.2 Working Architecture of algorithms for encryption.

#### 1. Key Generation by Sha-2

SHA-2 contains the key length of 256 piece which isn't flimsy with the animal power assault framework which is the key principle purpose of the hashing plan, likewise the MAC security gave if there should arise an occurrence of encryption where the most elevated number of security is being changed.

Our proposed work means to give a high-security blend approach while managing the cloud security approach, as the general strategy either work with the security encryption or hashing information check system.[4]

#### 2. Blowfish Algorithm For Data Encryption

The first step in the algorithm is to break the original key into a set of sub keys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit sub keys, while each S-box contains 256 entries.

This algorithm is divided into two parts.

- Key-expansion.
- Data Encryption.

#### 3. Optimization Blowfish Algorithm

Our proposed strategy is working same as Blowfish calculation working, yet there is few points we have changed get the best outcomes.

- Encryption Key size expanded.
- Reduce the Block (Phases.)

The only change is S-boxes in the F-function. The Feistel structure of Blowfish algorithm is not changed but the structure of F-function is modified. The original Blowfish algorithm F-function has four S-boxes but the optimized Blowfish F-function has two S-boxes.

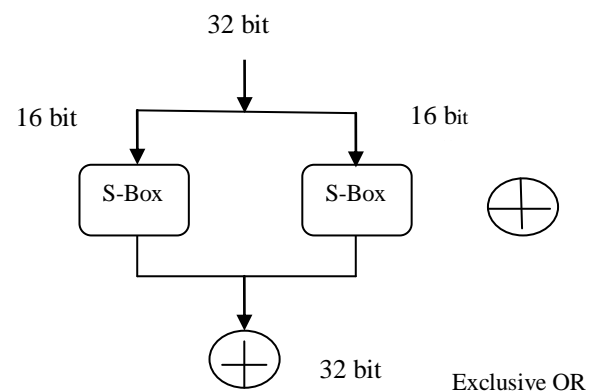


Fig.3 S-boxes break in Two Parts.

#### 4. Pseudo-Code of Algorithm

##### 4.1 Pseudo-code of F-Function with four S-Boxes (S0, S1, S2 and S3)

Step 1: Divide xL into four eight-bit quarters: a, b, c, and d  
Step 2:  $F(xL) = ((S_0, a + S_1, b \text{ mod } 232) \wedge S_2, c) + S_3, d \text{ mod } 232$

##### 4.2 The Pseudo-code of optimized F function with two S-boxes

Step 1: Divide xL into two sixteen-bit quarters: a, and b.  
Step 2:  $F(xR) = (S_0, a \wedge S_1, b)$

### 4.3 Pseudo-code of Encryption

- Step 1: Divide the 64 bit input data into two 32-bit halves (left and right): xL and xR
- Step 2: for i=0 to16  
 xL XORed with P[i].  
 Find F(xL)  
 F(xL) is XORed with xR.  
 Interchange xL and xR.
- Step 3: Interchange xL and xR.
- Step 4 : xR is XORed with P[16].
- Step 5: xL is XORed with P[17].
- Step 6: Finally combine xL and xR.

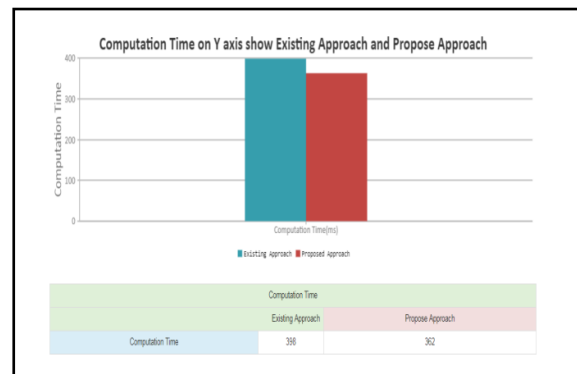


Fig.5 Decryption Vs Time.

## IV.RESULT ANALYSIS

1. **Encryption Time (Second)** by used our approach the encryption time is reduced

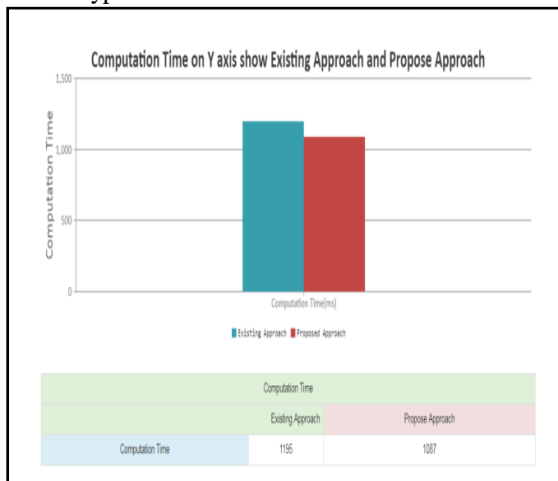


Fig.3 Encryption Vs Time.

2. **Throughput** by used our approach the over all system Throughput increase.

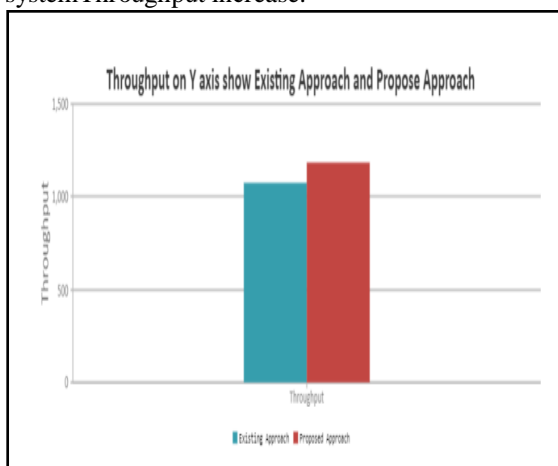


Fig. 4 Throughput Vs Time.

3. **Decryption Time** by used our approach the overall system Decryption time decrease.

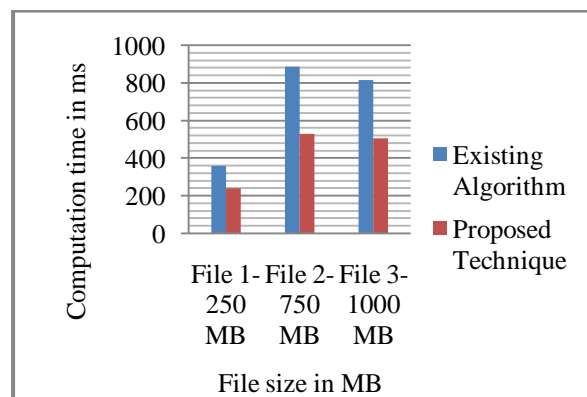


Fig.6 Computation Time Vs File Size.

A Comparison analysis of the result obtained from the existing technique is made with our Technique. Our technique obtained better minimizing computing time while comparing with the existing compressive sensing, accessing approach. A Computation cost and other major analysis shows the efficiency of our technique

## V.CONCLUSION

Cloud computing by itself is in evolving stage security implications in it are not complete. It is evident that even the leading cloud providers such as Amazon, Google etc are facing many security challenges and are yet to stabilize. Achieving complete solution for are facing many security challenge With this level of issues in cloud computing decisions to adopt cloud computing in an organization could be made only based on the benefits to risk ratio. By checking a proxy server we will find out the fault in encryption. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the client end and the cloud server end. Main goal of cloud computing is securely store and transmit the data in cloud. As per analysis the proposed work compute the low time at TPA side as well as server side to process the data store at server side as well as manage and proof generation.

## REFERENCES

- [1]. M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. ESpartford, "Secure outsourcing of scientific computations," Trends in Software Engineering, vol. 54, pp. 215-272
- [2]. Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2010.
- [3]. Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An access control model for cloud computing", Elsevier journal of information security and applications, 2014.
- [4]. C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou Toward secure and dependable storage services in cloud computing IEEE Trans. Services Comput., 5 (2) (2012), pp. 220-232
- [5]. Duncan, Adrian, Sadie Creese, and Michael Goldsmith. "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
- [6]. Pearson S. and A. Benameur: Security and trust issues arising from cloud computing. IEEE Second International Conference on Cloud Computing Technology and Science, CloudCom, pp. 693-702, 2010
- [7]. [10]. M. M. Hassan, K. Lin, X. Yue, and J. Wan, "A multimedia healthcare data sharing approach through cloud-based body area network," Future Generation Computer Systems, vol. 66, pp. 48-58, 2017
- [8]. M. S. Hossain and G. Muhammad, "Healthcare big data voice pathology assessment framework," IEEE Access, vol. 4, pp. 7806-7815, 2016.
- [9]. P. G. J. Leelipushpam and J. Sharmila, "Live vm migration techniques in cloud environment : A survey," in Information Communication Technologies (ICT), 2013 IEEE Conference on, April 2013, pp. 408-413.
- [10]. U. Varshney, Pervasive Computing and Healthcare. Boston, MA: Springer US, 2009, pp. 39-62
- [11]. A. Khan, M. Othman, S. Madani, and S. Khan, "A survey of mobile cloud computing application models," Communications Surveys Tutorials, IEEE, vol. 16, no. 1, pp. 393-413, First 2014.
- [12]. 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.
- [13]. Po-Wen Chi ; Chin-Laung Lei " Audit-Free Cloud Storage via Deniable Attribute-Based Encryption Sign In or Purchase" IEEE Transactions on Cloud Computing ( Volume: 6, Issue: 2, April-June 1 2018 ).
- [14]. Luo Yuchuan ; Fu Shaojing ; Xu Ming ; Wang Dongsheng " Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage Sign In or Purchase" China Communications ( Volume: 11, Issue: 11, Nov 2014).