A Survey: Secure Data Storage Techniques in Cloud Computing

Rakhi Emelaya
Department of Computer Engineering and Application
NITTTR, Bhopal
rakhisports@gmail.com

Dr. Sanjay Agrawal
Department of Computer Engineering and Application
NITTTR, Bhopal
sagrawal@nitttr.ac.in

***Abstract*—** Cloud computing is an era of research where we are looking for a fast and efficient computing solution with dynamic data. Cloud computing provide us a service which is use and pay on demand services, thus the user can have multiple options for data processing system. Many of the techniques to store data using security algorithm have been applied on cloud computing, but still the issue is its giving slow speed compare to server technique. Thus, a secure encryption technique with low computation and early scheme is always required. In this paper, we utilize and uniquely combine the Optimized blowfish homomorphism encryption with SHA-2 for key generation to make encryption more authentic. The proposed solution mentioned by us can give enhancement in security aspects as well as it compute fast data processing.

Keywords:-*AES, blowfish, cloud computing, data security*

*****

I. Introduction

Since the last decade the dependency on use of computer has increased tremendously this has attracted the awareness toward data security. Cloud computing is one such technique. Cloud computing is a technology which can imply on various basic applications such as home utility, medical application and other latest computer trends requirement. Application of the data security service can be deploy in the cloud (a network designed for storing data called datacenter) and then these services are offered to users always, whenever they want to use. The cloud hosted services are delivered to users in pay-per-use, multi-tenancy, scalability, self-operability, on-demand and cost effective manner. Cloud computing has become popular because of the above mentioned services offered to users. All the services offered by servers to users are provided by the Cloud Service Provider (CSP) which is working same as the Internet Service Provider (ISP) in the internet computing. The innovative development in virtualization and distributed computing along with high speed network and low cost attracts the focus of users toward internet services. Internet technology is designed with the new concept of services providing to the users without paying for these services and also stored the data on the local memory.

Cloud architecture comprises of the systems architecture of the software systems involved in the delivery of cloud computing, and this involves multiple cloud components communicating with each other over application programming interfaces, usually web services (Elliptic Curve Cryptography for Securing Cloud Computing Applications, 2013).The basic cloud computing architecture for service providing consist of user or client, a third party auditor and cloud server (Figure 1). In the cloud computing architecture, user is the one who uses the services of cloud. It may be a mobile device or stationary device which request for services to the cloud service provider and then on the basis of user's requests third party auditor, provides demanded services to these users offered by the cloud server. In the cloud computing data is stored in data centers from where data is accessed when or wherever it is required. With the data centers virtual servers are connected in which one or more virtual machines (VM) are situated for computation.

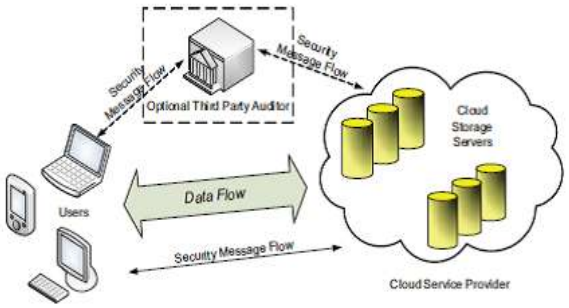

Figure 1:Cloud computing TPA service provisioning architecture [3]

II. LITERATURE REVIEW

Many different cryptographic algorithms have already been proposed and implemented to provide security to the user at the time of communication over the web. But now a days hacking has become a common practice in society to prevent from hacking various cryptographic algorithm is enhanced so that data will be more secure . In this paper we have studied a number of such symmetric key algorithms (RSA,RC4,Blowfish,AES) and select Blowfish among them of them for encryption and further

Enhancement.(A Modified Approach for Symmetric Key Cryptography2012)

2.1 In (2014) payal v. parmar et al main focus is on public key cryptographic algorithms based on homomorphic encryption scheme for preserving security [1]. The case study on various principles and properties of homomorphic encryption is given and then various homomorphic algorithms using asymmetric key systems such as RSA, ElGamal, Paillier algorithms as well a various homomorphic encryption schemes such as BrakerskiGentry-Vaikuntanatha (BGV), Enhanced homomorphic Cryptosystem (EHC), Algebra homomorphic encryption scheme based on updated ElGamal (AHEE), Non-interactive exponential homomorphic encryption scheme (NEHE) are investigated.

2.2 In (2013) Bhabendu Kumar Mohanta and Debasis Gountia say as the data storage challenge continues to grow for insurers and everyone else, one of the obvious solutions is cloud technology[9]. Storing data on remote servers rather than in-house is definitely a money-saver, but in insurance circles, the worry has been that having critical data reside outside the physical and virtual walls of the insurance enterprise is a risky situation. As the IT field is rapidly moving towards Cloud Computing, software industry's focus is shifting from developing applications for PCs to Data Centers and Clouds that enable millions of users to make use of software simultaneously. "Attempting computation on sensitive data stored on shared servers leaves that data exposed in ways that traditional encryption techniques can't protect against," the article notes. "The main problem is that to manipulate the data, it has to be decoded first". Now a new method, called fully homomorphic encryption (FHE) that performs computation with the encrypted data and send to the client and offers a realistic hope that such calculations can be performed securely in the cloud.

2.3 Privacy-Preserving Public Auditing for Secure Cloud Storage.
In (2013) Cong Wang et al Proposed TPA to perform audits for multiple users simultaneously and efficiently they performed batch auditing support where multiple file can be audit without knowledge of data to the TPA and cloud [3]. They have enables an external auditor to audit user's cloud data without learning the data content, multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner, MAC based setup has been performed and hashing algorithm is used to perform auditing while dealing with the data. Author conclude that the homomorphic linear authenticator and random masking is used in this scheme to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process.

2.4 Secure User Data in Cloud Computing Using Encryption Algorithms [10]
In (2013) rachna arora and Anshu Parashar proposed a scheme for cloud security to eliminate the concerns regarding data loss, segregation and privacy while accessing web application on cloud. Algorithms like: RSA, DES, AES, Blowfish have been used and comparative study among them have also been presented to ensure the security of data on cloud. DES, AES, Blowfish are symmetric key algorithms, in which a single key is used for both encryption/decryption of messages whereas DES (Data Encryption Standard) was developed in early 1970s by IBM. Blowfish was designed by Bruce Schneier in 1993, expressly for use in performance constrained environments such as embedded system. AES (Advanced Encryption Standard) was designed by NIST in 2001. RSA is a public key algorithm invented by Rivest, Shamir and Adleman in 1978 and also called as Asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits. The key size of AES algorithm is 128, 192, 256 bits. The key size of Blowfish algorithm is 128-448 bits. The key size of RSA algorithm is 1024 bits. So in this paper the authors have performed various algorithm and compared the results out of all the algorithms.

2.5 Security and Privacy in Cloud Computing[11]
In (2013) Zhifeng Xiao and Yang Xiao studied the security and privacy issues in cloud computing based on an attribute-driven methodology, and the data integrity verification made dealing with encryption algorithm and the audit was performed with the help of hashing algorithm available in order to verify the value generated again while checking the data integrity available with the associated file, here they have worked on different aspects such as user account access approach, availability of data, data changing or integrity verification and the technique should be privacy preserving so that the data should not be leak during the cloud execution.
2.6 Public Auditing for Shared Data with Efficient User Revocation in the Cloud [12]
In (2015) Boyang Wang and Baochun Li proposed privacy-preserving mechanism that supports public auditing on shared data stored in the cloud, they exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. the identity of the

signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire data and conclude two problems in which work can be continue one of them is traceability, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations.

2.7 A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm

Monika Agrawal and Pradeep Mishra(2012) presents a new approach for data encryption based on Blowfish algorithm[4]. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. With this new approach we are implementing a technique to enhance the security level of blowfish algorithm and to further reduce the time for encryption and decryption.

2.8 A Novel Approach to Blowfish Encryption Algorithm

Rajender Kumar and Balwinder Saini in(2014) determine the performance of the Blowfish encryption algorithm is the speed of execution. This speed is directly related to the size of the plaintext file size but it is not affected by varying the key length. Both encryption and decryption analyses where performed for deferent types of data [6].

2.9 A Study of New Trends in Blowfish Algorithm

In (2011) Gurjeevan Singh and et al briefly describes a new method to enhance the security of Blowfish algorithm; this can be possible by replacing the pre-defined XOR operation by new operation '#'[13]. When we are adding additional key and replacing old XOR by new operation '#', Blowfish will provides better results against any type of intrusion and present a fair comparison between the most common four encryption algorithms namely; AES, DES, 3DES and Blowfish in terms of security and power consumption. Experiment results of comparison are carried out over different data types like text, image, audio and video.

2.10 A Survey on Cryptography Algorithms

In (2014) MP Chaudhari and SR Patel conclude that the Blowfish algorithm is faster than other algorithm [7]. It reduces the execution time and provides a better security and it consumes less memory usage compared to any other algorithm. To improve the performance parameter of the Blowfish Algorithm like change in key size to prevent from brust force attack, change the size of plain text and Possible to minimize the key size of blowfish and making round more complexes for improving performance.

2.11 Optimized Blowfish Encryption Technique

In (2014) Christina L and Joe Irudayaraj proposed an optimized Blowfish has been developed[8]. The longer key size is more secure but the encryption time and decryption speed is slow. In order to overcome this problem in Blowfish algorithm reducing of two S-boxes will increase the speed and provide the better security to data. The main advantage of optimized Blowfish is that the execution time is reduced to 0.2 milliseconds and the throughput is increased to 0.24bytes/milliseconds compare than original algorithms. In future, cryptanalysis of optimized Blowfish algorithm will be investigated and this algorithm is tested with other data type such as text file, audio and video.

III. EXISTING SYSTEM

There is various techniques which are used to make data secure and store in the data center. The traditional cryptographic technologies for security, Analyzing existing security algorithms (RSA, AES, BLOWFISH, KP-ABE) by comparing their key size, Server computation time, TPA computation time. Our Proposing enhanced homomorphic data encryption technique based on below analyzed result.

TABLE I. Computation time and key length of different algorithm [10]

Encryption Algorithm	Key Length	Computation time(in ms)
AES	2048	2390
Blowfish	1024	500
RC4	1024	169
RSA-1,2	1024,2048	5199
KB-ABE	2048	346

TABLE II. DIFFERENT HASHING TECHNIQUE RESULT[10]

Hashing Algorithm	Key Length	Rounds
MD5	128	48
SHA-1	160	80
SHA-2	224	64
SHA-3	256	24

Disadvantages:

- Lack of rigorous performance analysis and high communication time with traditional algorithm.
- Small key for the data encryption was used.
- Externally hashing technique needs to compute for verification purpose.

IV. PROPOSED WORK

We proposed an enhanced homomorphic encryption with the Re-encryption technique which is an optimized blowfish scheme where we worked on reducing the S block phase and converted from the 4 S block to 2 S block which works to minimize the speed of the encryption system. Also for the data encryption scheme SHA-256 is used for a large key generation which make our system more secure using a high level key for the data encryption. Here for the purpose of data integrity we are using SHA 256 algorithm. Re-encryption is the solutions for protecting data from brute force attack by allowing the data owner to issue a special key (a `rekey') that can be used by the cloud storage system to re- encrypt cipher texts under a different key or policy without leaking any information about encrypted data.

Advantages

- A fragment technique is introduced to improve performance and reduce extra storage encryption scheme.
- The audit activities are efficiently scheduled in an audit period, and a TPA needs merely access file to perform audit in each activity.

MODULES:

1. Key Generation:
   The algorithm generates a key by using the algorithm manager, and then sends his public key to TPA. secondly, the algorithm use optimized blowfish encryption algorithm for secure cipher text generation.
2. Cipher and Tag Generation:
   The client (data owner) uses the secret key SK to pre-process a file, which consists of a collection of n blocks, generates a set of public verification parameters and index-hash table that are stored in TPA, and transmits the file and some verification tags to CSP.
3. Audit for Dynamic Operations:
   An authorized application, which holds data owner's secret key hsk, can manipulate the outsourced data and update the associated index hash table stored in TPA. The privacy of hsk and the checking algorithm ensure that the storage server cannot cheat the authorized applications and forge the valid audit records.

V. CONCLUSION

In this paper we survey the RSA, RC4, KP-ABE, AES and Blowfish algorithms to enhance the performance and encryption and decryption time. Blowfish algorithm give a better Performance and more security and strongest against any type of intrusion.An optimized Blowfish has been developed the longer key size is more secure but the encryptiontime and decryption speed is slow. In order to overcome this problem in Blowfish algorithm reducing of two S-boxeswill increase the speed and provide the better security to data. The main advantage of optimized algorithm is that the execution time is reduced and data is secure at storage by data auditing.

REFRENCES

[1] PV Parmar, SB Padhar, SN Patel "Survey of Various Homomorphic Encryption algorithms and Schemes" International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014

[2] C. Gupta and I. Sharma, "A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds," in Network of the Future (NOF), 2013 Fourth International Conference on the, 2013.

[3] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." Computers, IEEE Transactions on 62.2 (2013): 362-375.

[4] Agrawal, Monika, and Pradeep Mishra. "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm." International Journal of Engineering and Advanced Technology (IJEAT) 1.6 (2012): 79-83.

[5] Kumar, Rajender, Balwinder Saini, and Satish Kumar. "A Novel Approach to Blowfish Encryption Algorithm." International Journal of Advanced Foundation and Research in Science and Engineering 1.2 (2014).

[6] Chaudhari, Maulik P., and Sanjay R. Patel. "A Survey on Cryptography Algorithms." International Journal 2.3 (2014).

[7] Christina, L., and Joe Irudayaraj VS. "Optimized Blowfish Encryption Technique."

[8] Mohanta, Bhabendu Kumar, and Debasis Gountia. "Fully homomorphic encryption equating to cloud security: An approach." IOSR Journal of Computer Engineering (IOSR-JCE) Volume 9 (2013).

[9] Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms."International Journal of Engineering Research and Applications 3.4 (2013): 1922-1926.

[10] Xiao, Zhifeng, and Yang Xiao. "Security and privacy in cloud computing."Communications Surveys & Tutorials, IEEE 15.2 (2013): 843-859.

[11] Bhaskar, Malaneelam, and G. Umadevi. "Public Auditing For Shared Data With Efficient User Revocation In The Cloud.

[12] Singh, Gurjeevan, Ashwani Kumar, and K. S. Sandha. "A study of new trends in Blowfish algorithm." Internationa 1).

Research and aaplication(2011).

[13] Rana, Deepti, and Shivani Saluja. "A Modified Approach for Symmetric Key Cryptography Using Circles."