Highly Optimized Encryption Technique for Auditing Cloud Data through Trusted Auditor

N. M. Sawant
Department of Computer Science and Engineering
SKN Sinhagad, Pandharpur, Maharashtra, India

V. V. Pottigar
Department of Computer Science and Engineering
SKN Sinhagad, Pandharpur, Maharashtra, India

N. S. Mane
Department of Computer Science and Engineering
SKN Sinhagad, Pandharpur, Maharashtra, India

U. D. Bagal
Department of Computer Science and Engineering
SKN Sinhagad, Pandharpur, Maharashtra, India

Abstract- Cloud storage security is one of the challenges in cloud computing. As data user stores data on cloud server, loses control of the data. Cloud provider may see or change user's data. To avoid this we have to audit the data using trusted auditor. But storing plain data is not a proper way to store data, because both cloud provider and trusted auditor may see the data. To overcome this problem we are using encryption technique for the data. And auditor can provide the audit of user's data without decrypting it depending upon tags assigned to the data. Cryptography is playing an important role in cloud storage security. Many authors are coming with different cryptographic techniques to provide data security for the cloud data. Security to the cloud data can be provided by using RSA, DES, AES and Blowfish etc. But each technique has its own advantages and disadvantage. RSA is an asymmetric key algorithm which requires two keys for encryption and decryption. DES, AES and Blowfish are symmetric key algorithms, out of that Blowfish is faster and most secure encryption algorithms.

Keywords – Encryption, tags, auditor, cloud provider, blowfish, AES, DES

I. INTRODUCTION

Cloud computing is nothing but, storing and accessing data and programs over the Internet instead from your own hard disk. It is like utility service which we are using in our day to day life such as water, electricity, LPG connection, etc. It means that we are paying for the service as per our requirements. Same is happens in cloud computing, suppose we don't have enough data storage then we can take data storage from the cloud on rent. Similarly, if we want to use any software by avoiding purchasing license of that you can go for the Cloud. Depending upon which service you are using there are following types of services in cloud computing.

1) Software as a Service (SaaS)
2) Platform as a Service(PaaS)
3) Infrastructure as a Service(IaaS)

Software as a service, in this type cloud service cloud provider gives access to the both resource and applications. User of this service doesn't need to have physical copy of the software on his/her device to be installed. User don't need to have license of the software and also no need to upgrade the software, it is responsibility of cloud service provider. Platform as a service is one of the services of the cloud. This is the one higher level that software

as a service. In this cloud provider provides components of cloud to the user for the development and also provide platform to operate the application over internet. Infrastructure as a service provides infrastructure to the user. User controls and manages the system in terms of operating systems applications, storage and network connectivity but thing is that user cannot control the cloud infrastructure.

Providing security for the data stored on cloud is important issue in cloud computing [1] [2] [3] [4] [5] [6]. As data user stores his/her data on cloud server and lose control of data. Cloud service provider may see or modify that data as it is having total control of data. To avoid this, data user may encrypt the data and store on the cloud, but this scenario can't guarantee that stored data can't be handled or modified by the cloud service provider. Now, here question comes that which encryption technique is used to provide strong security for the data. There are many encryption algorithms, each of them having its positive and negative points. Encryption algorithms broadly categorized into two parts Asymmetric key algorithm such as RSA and symmetric key algorithm such as AES, DES & Blowfish etc. Asymmetric key algorithm requires two keys, public key for encryption and private key for decryption. On other hand symmetric key algorithm requires only one key for data encryption and decryption. Following section explains various encryption algorithms.

II. TRUSTED AUDITOR AND DATA TAGGING

Third party auditing is one of the best techniques for auditing the cloud data. Because either data user or cloud provider doing auditing is not proper, both of them may blame one other. For that in this paper we have used trusted auditor. Trusted auditor can convince to both data user and cloud provider as it managed by the government.

Data user divides data into number of blocks and after that blocks are encrypted by using blowfish algorithm (discussed in next section). Later one unique id (tag) will assigned to each block. Tags are sent to the trusted auditor. And data blocks are stored on cloud server. If data blocks are downloaded by the cloud provider then tag of that data block is changed. Now if data user wants to check data then, request for that is sent to the trusted auditor. Trusted auditor request new data tags from the cloud provider and compare the old tag and new data tags. And if there is change in tags then auditor submits the report to the data user.

Tags are assigned to each data block by using GUID algorithm which internally uses pseudorandom generator. Now a day's GUID is provided as predefined class in C# .net.

III. ENCRYPTION ALGORITHMS

Data Encryption Standard (DES)

DES is a block cipher algorithm. It uses 56-bits key for the encryption. This key looks like 64-bits, but 1-bit from every octet is used as parity bit, hence actual key size 56-bits. DES takes 64-bits size block as input and performs substitution and permutation on that block, which is after Ex-OR with input. This process is repeated for 16 times with the help of sub keys. As this algorithm uses 16 rounds, it makes it secure. [10] [11] [12]. Decryption is done in reverse order with the same key. As this is a symmetric key algorithm. We already mentioned above, symmetric key algorithm have same key for encryption and decryption. We know that key size of this algorithm is 56-bits which give space of 256 =7.2058 X 10^{16} elements. It means attacker will obtain plain text after 2^{56} trials on an average. If key for encryption is not used strong enough then it becomes easy work for the attacker. And also suppose all sub keys are same then after 16^{th} round we get plaintext as it is which is not expected. There are many weaknesses in the DES algorithm because that this algorithm is insecure.

Advanced Encryption Standard (AES)

AES is a block cipher algorithm. It uses encryption key and several rounds for encryption. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size (Fig. 3). This algorithm can be implemented on various platforms, especially on small devices [white paper]. There are various operations in AES that repeat after every round that are as follows: ADD ROUND KEY, BYTESUB, SHIFT ROW, and MIX COLUMN is enhances the security of algorithm [Review paper]. This algorithm requires high processing power as compared to DES, 3DES and blowfish. Brute force attack is the only known attack against the AES. AES is been observed very effective for live video streaming

Blowfish

Blowfish algorithm is designed by Bruce Schneier in 1993. Block size of blowfish algorithm is 64 bit and it has variable length key size from 32 to 448 bit. It has 16 round Fiestel ciphers and it uses large key dependent on 4 s-boxes. General structure of Blowfish algorithm is shown in [12].

Following factors are considered while designing Blowfish block cipher encryption algorithm.

Fast: Blowfish is fast algorithm [14] as it encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.

Compact: It requires less memory for execution.
Simple: It simple because it uses addition, XOR, lookup table with 32-bit operands.
Secure: This is one of the secure algorithms as it has key length is variable having range of 32 to 448 bits. 128 bits key length is default. It is suitable for applications where the key does not change often.

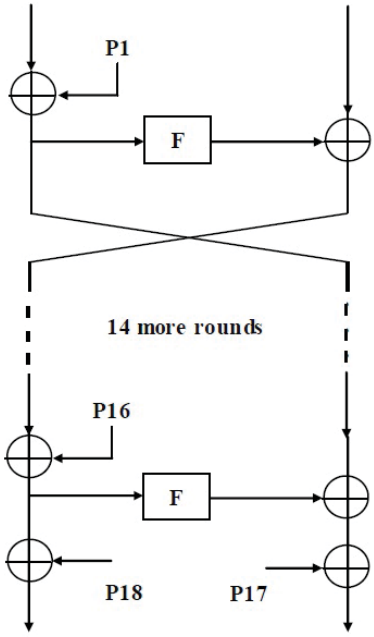


Figure 1 General structure of Blowfish algorithm

IV. BLOWFISH ALGORITHM

In 1993 Bruce Schneier designed Blowfish as a fast, free alternative to existing encryption algorithms. It is slowly getting acceptance as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish is a block cipher that encrypts data in 64 bit blocks. The algorithm consists of two parts, a key-expansion part and a data-encryption part. First part i.e. key expansion converts a variable-length key of at most 56 bytes into several sub-key arrays of 4168 bytes. Blowfish has 16 rounds. Every round consists of a permutation and substitution which is key dependent and key and data dependent respectively. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

This algorithm has two parts.

a. Key-expansion
b. Data Encryption

- a. Key-expansion:

It will convert a key several sub key arrays (P array) giving 4168 bytes. Blowfish uses large number of sub keys. These keys are generated earlier to any data encryption or decryption.
The p-array consists of 18, 32-bit sub keys:
P1, P2……., P18
Four 32-bit S-Boxes consist of 256 entries each:

S1, 0, S1, 1 ……. S1, 255

S2, 0, S2, 1…….. S2 255

S3, 0, S3, 1…….. S3, 255

S4, 0, S4, 1.....S4, 255

The sub keys are calculated using the Blowfish algorithm:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

3. Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.

6. Replace P3 and P4 with the output of step (5).

7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

In total, 521 iterations are required to generate all required sub keys. Applications can store the sub keys rather than execute this derivation process multiple times.

b. Data Encryption:

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round [12].

Algorithm: Blowfish Encryption

Divide x into two 32-bit halves: xL, xR

For i = 1to 16:

xL = XL XOR Pi

xR = F(XL) XOR xR

Swap XL and xR

Swap XL and xR (Undo the last swap.)

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR

The function F is as follows:

For XL, into four 8-bit a, b, c and d.
F (XL) = ((S1, a + S2, b mod 232) XOR S3, c) + S4, c mod 232.

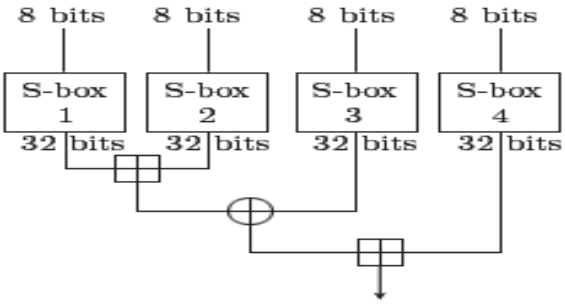


Figure 2 Four S- box representation of Blowfish algorithm

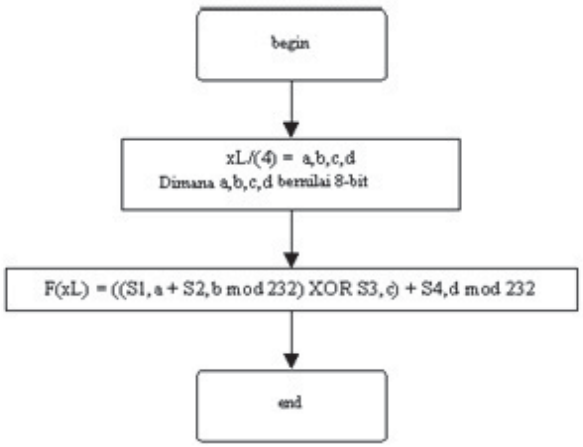


Figure 3 Block diagram of function used in Blowfish algorithm.

V. PROPOSED SYSTEM

Our proposed system consists of following entities.

1. Data user – who stores data on cloud.
2. Cloud provider – who stores data.
3. Trusted auditor – who audit data of the user and give result to user.

We have developed the highly secure data storage cloud system. We are auditing the data stored on cloud server by the user [7] [8] [9]. As user stores data on the cloud, data user loses the control of the data. Now whole

control of data is with cloud provider. Blowfish cryptographic algorithm is used to provide data security. But to keep track of our data we are using auditor. If cloud provider downloads user's data, auditor will tell to the data user, that his/ her data has been viewed or security of the data has been compromised by cloud provider.

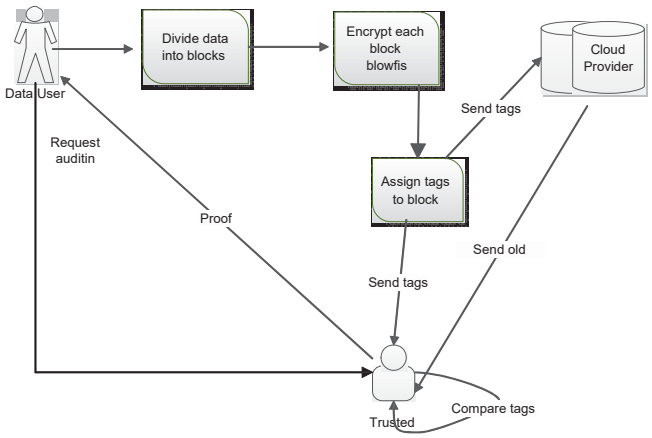


Figure 4 General structure of proposed system.

Data user, before storing his data on cloud, divides data into number of blocks. After that, each data block gets encrypted using blowfish algorithm. And, that each encrypted data blocks have assigned a tag. After assigning the tags to data block, all data blocks are stored on the cloud server.

One of the challenges in data security is to assign tags to the data blocks. We have assigned tags to blocks by using one predefined class in C# .net called 'GUID'. GUID class generates the unique hash value every time you are calling to it. That unique value we are using as a tag for the data block. If cloud provider downloads the data block stored by the data user, tag of that data block gets changed. That changed tag for the particular data block will be reflected to the auditor. Now, task of auditor becomes easy as it has to just check whether tag of the file block is changed or not. If tag of data block gets changed, auditor will submit the report to the data user.

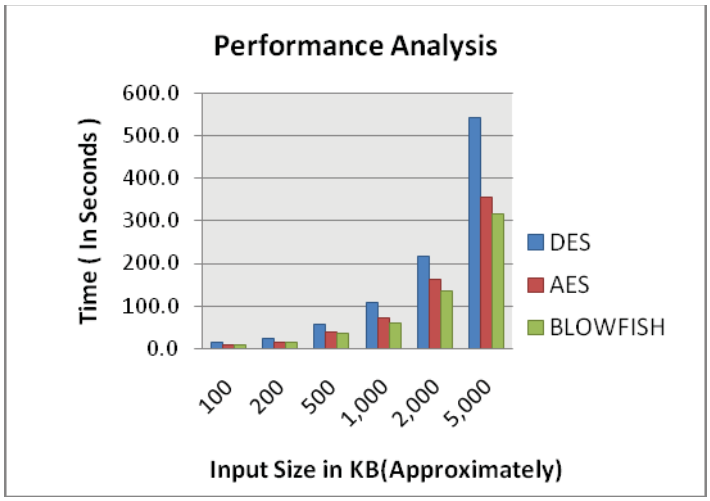
VI. Experiment and Result

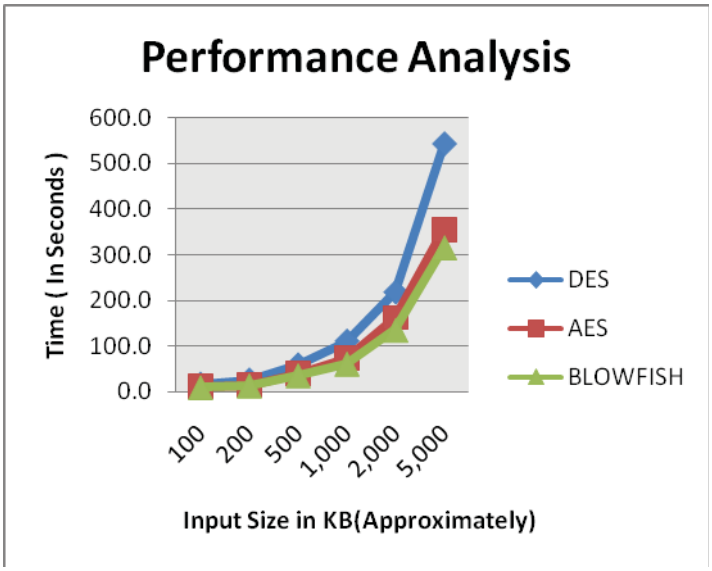
We have compared our system with existing system which uses AES and RSA combined for the encryption []. In our system we have used Blowfish algorithm for the encryption of the data. Our system gives better result to upload the data on the cloud. Table 1 shows result analysis.

Table 1 Comparative analysis different encryption algorithm.

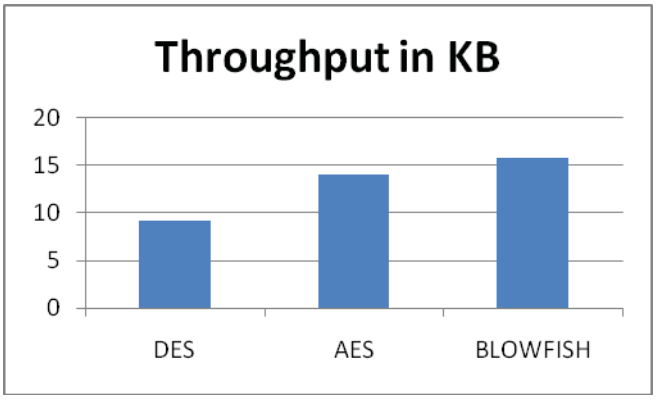
SIZE OF FILE(KB)	DES	AES	BLOWFISH
100	16.1	10.3	9.4
200	25.0	14.2	13.6
500	58.2	38.2	35.6
1,000	110.0	72.2	61.2
2,000	217.3	161.9	135.2
5,000	542.3	355.9	315.7

We have tested our system on different input file size and according to that we have generated result.





Following graph shows result analysis of different encryption algorithm in terms throughput. By observing graph we can say that Blowfish algorithm gives maximum throughput as compared to other algorithm i.e. AES and DES.



VII.CONCLUSION

We have designed system to provide the high security for the data storage on the cloud by using blowfish algorithm for encryption of the data. Blowfish is faster that DES and AES. Our system requires less time to upload data on the cloud as compared to other systems which are using DES and AES. Also we are auditing the user's data with the help of trusted auditor. Trusted auditor uses tagging concept to verify the security of the data. Auditor compares old tag and new tag of the data block. If both old and new tags are not matching it submit report to the user about security of the data block.

REFERENCES

[1] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J.Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, P. Ning, S.D.C. di Vimercati, and P.F. Syverson, eds., pp. 598-609, 2007.

[2] C.C. Erway, A. Ku¨pc¸u¨, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security, E. Al-Shaer, S. Jha, and A.D. Keromytis, eds., pp. 213-222, 2009.

[3] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010. W.-K. Chen, *Linear Networks and Systems*, Belmont, CA: Wadsworth, 1993, pp. 123-135.

[5] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.R. A. Scholtz, "The Spread Spectrum Concept," in *Multiple Access*, N. Abramson, Ed. Piscataway, NJ: IEEE Press, 1993, ch. 3, pp. 121-123.

[6] Kan Yang and Xiaohua Jia "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" IEEE transactions on parallel and distributed systems, vol. 24, no. 9, September 2013.M. B. Kasmani, "A Socio-linguistic Study of Vowel Harmony in Persian (Different Age Groups Use of Vowel Harmony Perspective," *International Proceedings of Economics Development and Research*, ed. Chen Dan, pp. 359-366, vol. 26, 2011.

[7] Anuradha Appasaheb Jagadale, Shilpa Gite "Privacy Preserving Auditing Protocol Using Cryptography for Cloud Storage Systems" IJSR Volume 3 Issue 12, December 2014.

[8] M. Ravi kumar and E . Madhusudhana Reddy "Auditing Framework Service for Efficient Secure Data Storage in Multi- cloud" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1181-1183.

[9] B. Sunitha, 2 K. Suresh Babu "Auditing Protocol for Secured Data Storage in Cloud" IJCSEC- International Journal of Computer Science and Engineering Communications. Vol.3, Issue 3, 2015, Page.1013-1020, ISSN: 2347–8586

[10] Dr. Prerna Mahajan α & Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security" Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350**.**

[11] Anuj Kumar, Sapna sinha & Rahul Chaudhari "A Comparative Analysis of Encryption Algorithms for Better utilization" International Journal of Computer Applications (0975 – 8887) Volume 71– No.14, May *2013*

[12] Ms. Arati Appaso Pujari, Mrs. Sunita Sunil Shinde "Cryptography and encryption algorithms for information security" International Journal of Advance Engineering and Research Development ISSN (Print): 2348-6406 ISSN (Online): 2348-4470 2014.

[13] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011

[14] N. M. Sawant, V. V. Pottigar, N. S. Mane, "A Survey on Auditing Technique used for preserving privacy of data stored on cloud " International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.