Indian Journal of Science and Technology, *Vol 8(19), DOI: 10.17485/ijst/2015/v8i19/72272, August 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

EnBloAES: A Unified Framework to Preserve Confidentiality of Data in Public Cloud Storage

R. Kalaichelvi[1*] and L. Arockiam[2]

[1]Department of Computer Science, Karpagam University, Coimbatore - 641021, Tamil Nadu, India; kalai_hasan@yahoo.com
[2]Department of Computer Science, St. Joseph's College, Tiruchirappalli - 620002,Tamil Nadu, India; larockiam@yahoo.co.in

Abstract

Objective: Cloud storage reduces the cost of IT infrastructure for businesses by sharing resources through internet. However, data stored on cloud has security issues and vulnerable to attacks by malicious hackers. The main objective of this paper is to propose a framework to address issues and attacks which compromise the confidentiality of outsourced data. **Methods:** The significant factor to ensure data security is confidentiality. Data partitioning, shuffling and encryption techniques are taken in this study to preserve confidentiality. Specifically blowfish and AES encryption techniques are modified to have better performance in terms of encryption time, decryption time, overall processing time, throughput and the degree of security. **Findings:** In the proposed framework, the data is split into multiple chunks and the chunks of data are shuffled. Then the shuffled chunks are encrypted using a hybrid technique which comprises of Enhanced Blowfish (EnBlo) and Enhanced Advanced Encryption Standard (EnAES) in order to provide data confidentiality. It further proposes an efficient retrieval scheme by appropriate decryption and a system to rearrange data chunks in order to get the original data at the client side. **Conclusion:** This research concludes, the EnBloAES provides extensive data security and adept at retrieval scheme by incorporating data confidentiality.

Keywords: Cloud Storage, Confidentiality, Data Outsourcing, Data Partition, Encryption, Shuffling

1. Introduction

Cloud computing is an omnipresent network which offers services such as large pool of virtual resources, storage, platforms, applications and dynamic computational power. The common cloud services are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). This model is referred as the SPI model. Cloud can be deployed as a public, private, hybrid or a community cloud[1].

Main entities involved in outsourcing of data on cloud computing are Data Owner (DO), Cloud Service Provider (CSP) and the Data User (DU). This study is an extension to R. Kalaichelvi et al[2] in which it was proved that the proposed approach EnBlo has better efficiency in speed and throughput than the existing blowfish algorithm with the simulation results. In this paper, EnBlo is integrated with other mechanisms in order to guarantee safe cloud storage in terms of preserving data confidentiality.

2. Data Outsourcing

Cloud Computing is a subtly alluring paradigm to individuals and business enterprises. The significant powers of cloud computing such as scalability, elasticity, reliability and pay-as-you-go make the cloud paradigm offer services at a reduced cost. The vital factor of cloud computing "pay-as-you-go" drives the industrial world to

*Author for correspondence

migrate to cloud environment as it significantly reduces the capital expenditure and operational expenditure. As a result, small start-up companies and large enterprises widely adopt data outsourcing. Data outsourcing delegates data storage, maintenance of data consistency, data management and data security. Cloud Service Providers (CSP) control and allocate the resources to store data.

Data outsourcing security is in its juvenescent period as far as reaching its goals are concerned. When the data is outsourced to off-premises vendors, the relationship between the data owners and their data is disconnected. Consequently, data owners lose control on their own data when it is outsourced to third party vendors. As a result, the sensitive data of enterprises may be potentially exposed to risks and security vulnerabilities. Figure 1 depicts the data outsourcing to the cloud by enterprises.

3. Issues Arise in Adoption of Data Outsourcing

Despite all the benefits and enormous growth of cloud computing, it may not provide a high degree of security to the data. Security concerns and challenges that are related to outsourcing storage should be considered as a prime and significant factor to be dealt with carefully. Protection of cloud data ensures confidentiality of stored data on the cloud. Cloud data may be snooped by any inside or outside attackers. Though the data owners rely on the CSPs to store their huge amount of data, as the data is administered by the cloud administers, there are possibilities that malevolent attackers at cloud providers may snoop or leak the stored data on cloud. The other barrier to adopt cloud computing is outside attackers. The outsiders could be the public or people involved in the business who have access to cloud storage. These attackers can view or alter cloud data. As a result, the confidentiality and integrity[3] of data are compromised by malicious cloud employees or any other third parties.

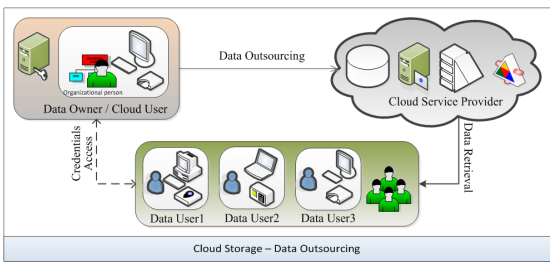

Figure 1. Data outsourcing to cloud by enterprises.

Due to the ever growing significance of cloud computing, individuals and many organizations in the business world are migrating to cloud computing. The adoption of cloud technology is escalating day by day as it has high availability, elasticity and simplicity features. It offers storage and other high-performance computing resources to the cloud users at a fairly low price. Cloud computing revolutionizes the business market through online services. Outsourcing storage is the main attraction in migrating to the cloud. Despite the enormous growth in cloud technology, it lacks security measures in service availability, data confidentiality, data integrity and many other aspects. When data is outsourced, the users lose their control on the data. Moreover, the multi-tenancy features of cloud computing leads to serious risks in data security by other organizations which are connected to the CSP. There are a lot of possibilities in disclosure of sensitive data to unauthorized people who may be the administrators and other personnel in the cloud as well as other organizations' personnel. This scenario can compromise the confidentiality of sensitive data. Consequently, the prime security intimidation on the cloud is data security. This section illustrates the related research works of cloud data security in terms of ensuring data confidentiality.

Nathalie Baracaldo et al[4] proposed a framework for the cloud storage which ensures data confidentiality. The framework referred as Trusted Decrypter (TD) has 2 modules namely, Critical module and Coordinator module. Security related tasks are managed in the critical module and non-security related tasks are administered by coordinator module. TD covers data de-duplication, off-boarding and compression functions. They projected many data reduction algorithms in their architecture. The proposed architecture TD ensures no outflow of data to either outside malicious attackers or inside attackers such as administrators in the cloud or any other tenants who are connected to the cloud providers. Aikaterinal et al[5] investigated cryptography issues in cloud computing and summarized some of the cryptographic algorithms related to computation outsourcing and secure data storage such as Oblivious RAM (ORAM), Fully Homomorphic Encryption and Searchable Symmetric Algorithm, Functional Encryption, Proof of Retrievability and Provable Data Possession schemes. The researchers also proposed a framework for cloud computing security with a list of security goals to different attack models such as Curious CSP, Lazy CSP AND Byzantine CSP. In Krishna et al[6] illustrated a new approach called Silverline to improve

data confidentiality on the cloud. The Silverline framework functions are: 1. Determining outfitted data for encryption. 2. Allocating strong encryption keys to different datasets with less complexity of data management. 3. Providing secure data access to users. The evaluation of Silverline technique is performed on 3 real-world applications namely Astro Space, Use BB and Comendar. Eyad Saleh et al[7] proposed a prototype HPI Secure. It enhances the security of cloud data. The prototype stores the encrypted data on cloud without any compromise of functionality. The researchers claim that HPI Secure successfully encrypts the data before it is stored on the cloud. And the decryption is done at the user side.

Hussain Aljafer et al[8] presented a survey of strong encryption schemes such as Fully Homomorphic Encryption (FHE), Hierarchical Attribute Based Encryption (HABE) and Advanced Encryption Standard (AES). They also implemented the schemes in a framework and did a comparative study to evaluate the performance of the schemes. The experimental results show that all the schemes ensure data confidentiality. They concluded that AES is much faster than other schemes for small files and suits small enterprises, whilst for larger files FHE and HABE give better performance than AES algorithm. Trang Hoang et al[9] proposed the Advanced Encryption Standard algorithm based on Field Programmable Gate Array as a platform. They analysed the FPGA-based AES with other designs to evaluate the performance of their implementation. The simulation results are highlighted in terms of achieving low complexity architecture. Subsequently, Atul M. Borkar et al[10] proposed AES implementation on Field Programmable Gate Array (FPGA). The researchers used Very High Speed Integrated Circuit Hardware Description Language (VHDL) code in their model in order to reduce the hardware consumption. The simulation results depicted the encryption and decryption performance. Chi-Feng Lu et al[11] discussed the security efficiency of AES compared to other algorithms. They also implemented the AES algorithm in the smart card. The researchers used chip operating system as the AES implementation architecture. They simulated AES embedded COS design without a coprocessor. Concurrently, they accomplished another design called Cipher System On Demand (CSOD) with multiple algorithms. Performance results were presented and AES embedded design was compared with the CSOD design. They concluded that the performance of AES embedded design is better than CSOD design. But in case of flexibility and elasticity aspects, CSOD is as good as AES embedded design.

Mandal et al[12] discussed the role of cryptography in information security system. Also, the parameters which affect the performance of the system were pointed out in their research. They implemented Data Encryption Standard (DES) and Advanced Encryption Standard (AES) in MATLAB. They illustrated the avalanche effect with various parameters in their simulation results. Consequently, Dewangan et al[13] discussed cryptography technique against malicious attacks and the computing resources CPU time, memory and computation time. They analysed the avalanche effect in Advanced Encryption Standard (AES) using MATLAB software. With their simulation results, they concluded that AES has good security level. In[14,15] the researchers performed the experimental analysis of symmetric algorithms: DES, AES and Blow fish. From the simulated result, they concluded that in the case of performance, blow fish is the efficient algorithm and AES is superior in terms of security. Mallaiah et al[16] analyzed the performance of Format Preserving Encryption (FIPS 74-8). They briefed the overhead of FIPS-74-8. The testing is done on 1000 credit card numbers with DES, 3DES, Blow fish and AES. Though FIPS-74-8 is using DES block cipher, the researchers observed that Blow fish or AES gives better results in preserving the format of numeric data.

4. Motivation

Data outsourcing, also known as database as a service[17], offers remarkable cost savings[18], higher availability and other benefits to the cloud users. Nevertheless, the confidentiality of cloud data should be taken into account when data is outsourced. The aforementioned related literature mainly confers the encryption technique which maintains data confidentiality. Encryption is one of the key techniques to protect data. But, existing encryption techniques are not adequate for cloud data security. Consequently, this paper aims to achieve data security which covers confidentiality of cloud data with the following objectives:

- Defining a novel, concrete framework of cloud storage in order to achieve confidentiality of data.
- Applying data partition, data shuffling and a hybrid encryption technique to ensure higher security, before the data is outsourced.
- Maintaining metadata of data partition, data shuffling and hybrid encryption technique.
- Ensuring cloud-stored data can be accessed only by authorized data users or data owners.

5. EnBloAES: Framework for Secure and Robust Cloud Storage

In this modern era, a wide range of individuals and business enterprises use the hi-tech trend cloud computing. One of the most profitable, essential services provided by cloud computing is cloud storage. It allows individuals and organizations to move their sensitive data from their local computers to cloud environment. However, providing security to sensitive data is the greatest challenging issue faced by DOs due to unauthorized access of data by malicious attackers and snoopers in the cloud environment.

This section describes our proposed novel framework EnBloAES which gives solution to the issues faced by DOs. The proposed framework EnBloAES to preserve confidentiality of cloud data is shown in Figure 2.

The EnBloAES uses three mechanisms: data partition, shuffling and two encryption techniques - EnBlo and EnAES to protect data. The proposed framework maintains confidentiality of data stored on the cloud. The first mechanism in the proposed model is partitioning big volume of data into multiple chunks. Secondly, to provide security, these chunks are shuffled in order to change the order of the generated chunks before they get encrypted in shuffling mechanism. In metadata creation, the hash function is used and they are maintained safely at the DOs side. Hash function offers two roles to the proposed system:

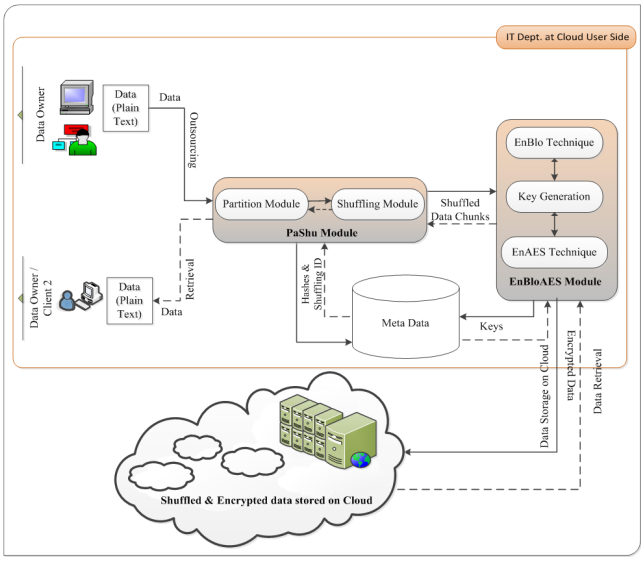

Figure 2. EnBloAES with PaShu - proposed framework to preserve confidentiality of cloud data.

1. It maintains the integrity of data. 2. The indices generated using hash function is used to retrieve the data back in the original form at the client side. The first and the second mechanisms together are known as PaShu module. It serves as a base layer of security and it happens at the DOs side. Subsequently, the shuffled chunks are encrypted by a hybrid technique which comprises of EnBlo and EnAES in order to provide data confidentiality. After these mechanisms are applied to the data, the shuffled and encrypted data chunks are transferred to the cloud. When DU needs to access the cloud-stored data, the transaction takes place at the client side to access the shuffled and encrypted data. After the transaction between the DO and the DU, the DU will be identified if he is the authorized user. Then the identified authorized user can fetch the data from the cloud with his genuine credentials. At the client side, the proposed model further proposes an efficient retrieval scheme by appropriate decryption methods and a system to rearrange and merge the data chunks in order to get the original data. By incorporating data confidentiality, EnBloAES provides a substantial data security and profi-cient retrieval scheme.

5.1 PaShu Module: Partition and Shuffling

5.1.1 Data Partition

To split a file into a number of chunks, an identifier or key to identify each chunk is generated first. These identifiers are used later when the chunks are required to be joined at the receiver side. An index table will be generated with the details of 1. Indices of all chunks which point the specific byte or the first byte of chunks presented in the original file. 2. Names of the chunk files and the name of the original file. 3. File size of the original file. 4. File size of chunks arrive from the original file[19,20].

Henceforth the splitting algorithm generates 2 parts when the chunks are created from the original file:

- Metadata which contains above-mentioned information.
- Data or content from the original file.

5.1.1.1 Following are the Steps Involved in Data Partition

- Input the original file to be split.
- Specify the folder to store the chunks and names of the chunks.
- Input the number of partitions to be done on the file.

5.1.1.2 Metadata Creation

Creating an array as indices (hashes) for the chunks using the hash function which uses the following details. Hash IDs are created using Java's hash Code () method.

- Set boolean value for identifying the first chunk and the last chunk of the file.
- Let: 0 for first chunk and 1 for last chunk.
- Get the size and name of the original file.
- Set the position and the size of the chunks. //Get the position of a chunk from its name.

5.1.2 Shuffling Data Chunks

The generated data chunks file orders are shuffled by shuffling algorithm. The shuffling ID and the original indices of the data chunks are stored to rearrange them later. With the shuffling ID, the files are renamed using: old Name. rename To (new Name) method of file class.

The following Steps explain the shuffling of data chunks.

For i = 1 to number of data chunks {
    k = random integer
Swap a[k] and a[i]}

5.2 EnBloAES Framework

After the PaShu module, the shuffled chunks are encrypted by Encryption module. Encryption module is a hybrid technique which comprises of Enhanced Blow fish (EnBlo) and Enhanced Advanced Encryption Standard (EnAES) in order to provide data confidentiality. Figure 3 illustrates the detailed version of EnBloAES hybrid encryption module.

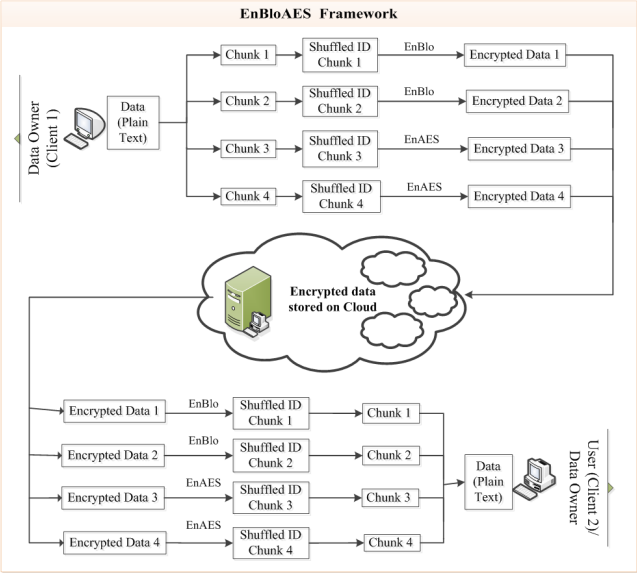

Figure 3. Detailed version of EnBloAES hybrid encryption module.

5.3 EnBlo Technique

EnBlo uses the R. Kalaichelvi et al[2] proposed Mod Blow encryption technique. The paper discusses the superior nature of the blow fish algorithm. The proposed EnBlo technique considers two factors: modified F function and initialization vector in order to achieve better results in performance in terms of encryption time, decryption time and throughput. The key generation module generates the keys needed to perform the encryption. Key generation and management are dealt by other third party vendors or at the DOs side.

5.4 EnAES Technique

EnAES technique in EnBloAES hybrid model is a novel technique. EnAES uses AES-128 structure. It accepts 128 bit block array i.e 16 bytes array. AES involves 4 stages with 10 iterations for encryption and decryption namely, Sub Bytes, Shift Rows, Mix Columns and Add Round Key. EnAES algorithm is proposed with changes in 2 stages: Sub Bytes and Mix Columns stages for achieving better performance. AES-128 key length is 128 bits. Theoretically 2^{128} permutation of 128 bit key can crack the AES algorithm. The heart of cryptography is finite fields. The most important and powerful stages in AES are Sub Bytes and Mix Column stages as they use multiplicative inverse in GF (2^8). The degree of the security is improved in Modified Sub Bytes stage, whereas the encryption time, decryption time and the throughput are improved in Modified Mix Column stage.

In AES, the lookup table S-Box is static but has non-linearity properties. S-box is built by multiplicative inverse function and invertible affine transformation to evade any attacks. Each input byte of state matrix is replaced by the values in S-box in the Sub Bytes stage. Here, to improve the security of AES algorithm, the only non-linearity element S-box is strengthened. The proposed S-box of AES algorithm is dynamic[21,22]. It is a key-dependent, dynamic lookup table. The complexity of Sub Bytes stage will be increased so that the algebraic attacks will be impossible. In our proposed model, a key schedule algorithm can be used to generate 16 bytes array key. In the first round of encryption, the 16 byte array is XORed with each byte of

S-box row-wise. From the second round onwards, the key array is left shifted one byte and the new array with shift is XORed with the S-box. And hence every round the S-box values are unique. S-box is constructed as follows:

For round = 1
{
i = 0;
for j = 0 to 16 bytes
i = s[j] ⊗ NK[j]
swap (s[j], s[i])}
for round = 2 to 9{
for j = 0 to 16 bytes
Left circular shift NK[j]
for j = 0 to 16 bytes
i = s[j] ⊗ NK[j]
Swap (s[j], s[i])
}

The stage which takes significant time for encryption and decryption is Mix Columns. Mix Columns has circular left shift of polynomial $03x^3 + 01x^2 + 01x + 02$ using arithmetic GF (2^8). The sum of products of two matrices: polynomial with left shift matrix and the state matrix are used to get elements of the state matrix as the output of this stage. When the degree of the result of the product of 2 elements is greater than 7, the mod operation with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$is used to get the final result. Since this stage comprises of shift, multiplication, XOR and the mod operation, the consumption time for encryption is high. Moreover, the inverse matrix uses the invertible polynomial $0Bx^3 + 0Dx^2 + 09x + 0E$. The computations of Inv Mix Columns are complicated, since the coefficients of Inv Mix Column are 0B, 0D, 09, 0E. Hence the time taken for computation becomes significantly high in decryption process[23, 24]

The proposed model is constructed to reduce the processing time extensively. The Mix Column stage uses multiplicative inverse in GF (2^8) with a degree eight, irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, so that it takes considerably high processing time. Consequently, the proposed model uses the addition in Galois Field. The property of addition in GF (2^8) is plain and straightforward. In addition, in GF (2^8), the same power terms can be combined irrelevant of their coefficients. The addition can be performed with a simple XOR operation. Moreover, when the addition operation involves the Mix Column stage, the inverse operation is not needed in the decryption process. Avoiding the large coefficients of Inv Mix Column 0B, 0D, 09, 0E in decryption, with the same XOR operation, the process of Inv Mix Column consumes comparatively very less time, but it does the same substitution process with high degree of confusion property.

5.5 EnBloAES Implementation Screens

Figure 4 is the interface screen of EnBlo technique where the comparisons of blowfish and EnBlo techniques performance are shown. Figure 5 is the interface screen of EnAES technique where the comparisons of AES and EnAES techniques performance are shown. The time consumption of encryption, decryption and the whole process time are compared for both the scenarios in Figure 4 and Figure 5. Figure 6 shows the GUI screen of EnBloAES framework. The user inputs the number of chunks to be split from the original file. The shuffled, encrypted chunks with their new file names and IDs are displayed in the frame 1. These shuffled, encrypted and indexed data chunks are stored in one or more clouds for security reason. The frame 2 depicts the ordered and decrypted chunks after retrieval from the cloud providers at the DUs or DOs side. And the frame 3 shows the original file retrieved from the chunks with the parameters of split time, shuffling time, indexing time, encryption time and decryption time and overall processing time.

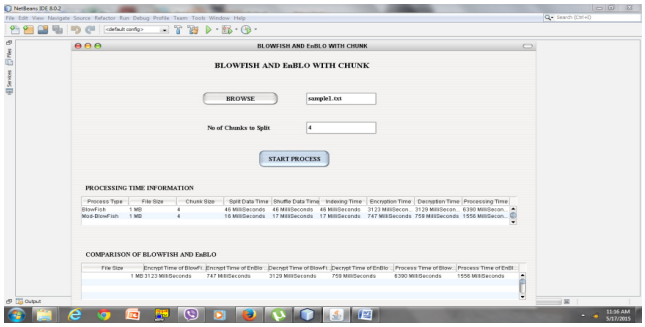

Figure 4. Interface screen of EnBlo technique.

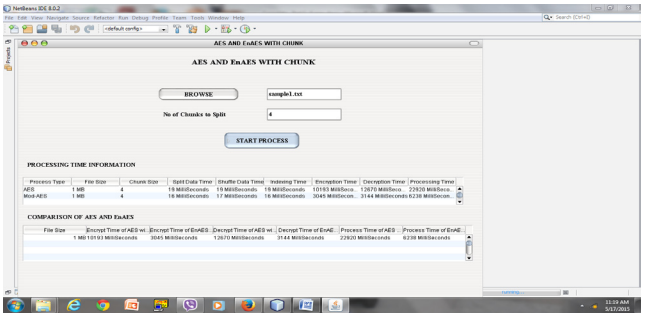

Figure 5. Interface screen of EnAES technique.

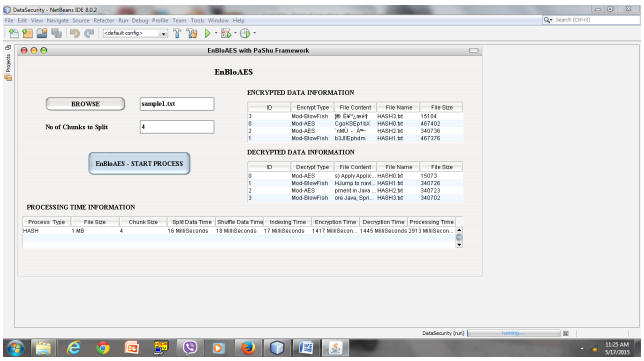

Figure 6. GUI screen of EnBloAES with PaShu framework.

6. Conclusion

This paper aimed to make DOs empowered by the novel, concrete framework EnBloAES. The PaShu module of the EnBloAES partitions and shuffles the data before the encryption takes place. PaShu module is followed by the EnBloAES module where encryption takes place to provide data confidentiality. These operations are performed at the DOs' side before data is uploaded to the cloud. In addition, the proposed EnBloAES framework provides efficient data retrieval scheme to the genuine DUs or DOs. By incorporating data confidentiality. EnBloAES provides substantial data security and proficient retrieval scheme. In conclusion, the EnBloAES will definitely make the entire world adopt cloud usage quickly.

7. References

1. Kalaichelvi R, Arockiam L. Research challenges and security issues in cloud computing. International Journal of Computational Intelligence and Information Security. 2012 Mar; 3(3): 42–8.
2. Kalaichelvi R, Arockiam L. Security enhancement of cloud data storage using modified blow fish algorithm. IJAER. 2015 Feb; 10(2): 3685–700.
3. Lee J-Y. A study on data integrity and consistency guarantee in cloud storage for collaboration. Indian Journal of Science and Technology. 2015 Apr; 8(S7): 674–8.
4. Baracaldo N, Androulaki E, Glider J, Sorniotti A. Reconciling end-to-end confidentiality and data reduction in cloud storage. CCSW'14, ACM Workshop on Cloud Computing Security; New York, USA. 2014 Nov. p. 21–32.
5. Latsiou A, Rizomiliotis P. The rainy season of cryptography. Panhellenic Conference on Informatics, ACM (PCI'2014); Greece. 2014 Oct. p. 1–6.
6. Krishna PN, Kruegel C, Zhao BY. Silverline: toward data confidentiality in storage-intensive cloud applications. Symposium on Cloud Computing SOCC'11, ACM; Portugal. 2011 Oct 10.
7. Saleh E, Meinel C. HPI Secure: towards data confidentiality in cloud applications. IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid); Delft. 2013 May 13-16. p. 605–9.
8. Aljafer H, Alodib M, Abdelmounaam. An experimental evaluation of data confidentiality measures on the cloud. Management of Computational and Collective Intelligence in Digital EcoSystems, MEDES 14, ACM; Saudi Arabia. 2014 Sep. p. 117–24.
9. Hoang T, Nguyen VL. An efficient FPG Aimplementation of the advanced encryption standard algorithm. IEEE Computing and Communication Technologies, Research, Innovation and Vision for the Future (RIVF); Ho Chi Minh City. 2012 Mar. p. 1–4.
10. Borkar AM, K shirsagar RV, Vyawahare MV. FPGA implementation of AE Salgorithm. IEEE International Conference on Electronics Computer Technology (ICECT); Kanyakumari. 2011 Apr 8-10. p. 401–5.
11. Lu C-F, Kao Y-S, Chiang H-L, Yang C-H. Fast implementation of AES cryptographic algorithms in smart cards. IEEE Annual International Carnahan Conference on Security Technology; 2003 Oct 14-16. p. 573–9.
12. Mandal AK, Parakash C, Tiwari A. Performance evaluation of cryptographic algorithms: DES and AES. IEEE Conference on Electrical, Electronics and Computer Science (SCEECS); Bhopal. 2012 Mar 1-2. p. 1–5.
13. Dewangan CP, Agrawal S, Mandal AK, Tiwari A. Study of avalanche effect in AES using binary codes. IEEE Conference on Advanced Communication Control and Computing Technologies (ICACCCT); Ramanathapuram. 2012 Aug 23-25.p. 183–7.
14. Verma OP, Agarwal R, Dafouti D, Tyagi S. Performance analysis of data encryption algorithms. IEEE Information and Communication Technologies on Electronics Computer Technology ICECT; Kanyakumari. 2011 Apr 8-10.p. 399–403.
15. Ramesh A, Suruliandi A. Performance analysis of encryption algorithms for Information Security. IEEEI CCPCT 2013 International Conference; Nagercoil. 2013 Mar 20-21. p. 840–4.
16. Mallaiah K, Ramachandram S, Gorantala S. Performance analysis of Format Preserving Encryption (FIPS PUBS 74-8) over block ciphers for numeric data. IEEE International Conference on Computer and Communication Technology (ICCCT); Allahabad. 2013 Sep. p. 193–8.
17. Damiani E, De Capitani di Vimercati S, Foresti S, Jajodia S, Paraboschi S, Samarati P. Metadata management in outsourced encrypted databases. Proceedings of the

2nd VLDB Workshop on Secure Data Management: Lecture Notes in Computer Science; Trondheim, Norway: Springer-Verlag; 2005 Sep. p. 1–17.
18. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr; 6(4): 4396–401.
19. File Splitter. 2014; Available from: http://forum.codecall.net/topic/69665-file-splitter-part-1-of-2-parts
20. Bu Y, Howe B, Balazinska M, Ernst M. Loop H: Efficient iterative data processing on large clusters. Proceedings of the VLDB Endowment, ACM. 2010 Sep; 3(1-2):285–96.
21. Abd-ElGhafar, Rohiem A, Diaa A, Mohammed F. Generation of AES dependent S-Boxes using RC4 algorithm. Aerospace Sciences and Aviation Technology; Cairo, Egypt. 2009 May 26-28. p. 1–9.
22. Enhancement of confidentiality using cryptographic 2015 Jan. Available from: http://shodhganga.inflibnet.ac.in/handle/10603/5051?mode=simple&submit_simple=Show+simple+item+record
23. Hernandez OJ, Sodon T, Adel M, Kupp N. A low cost Advanced Encryption Standard (AES) co-processor implentation. JCS and T. 2008 Apr; 8(1):8–14.
24. Venkaiah VC, Srinathan K, Bruhadeshwar B. Variations to S-box and mixcolumn transformations of AES. Technical Report. Deemed University; 2006 Feb.