International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish)

Fortine Mata[1], Michael Kimwele[2], George Okeyo[3]

[1, 2, 3]Computing Department, Jomo Kenyatta University of Agriculture and Technology

Abstract: ***Data stored in the cloud is increasingly gaining popularity for all users including personal, institutions and business purposes. The data is usually highly protected, encrypted and replicated depending on the security and scalability needs. Despite the advances in technology, the practical usefulness and longevity of cloud storage is limited in today's systems. This paper provides a solution to the problem of securely storing the client's data by maintaining the confidentiality and integrity of the data within the cloud. This paper addresses the problem of ensuring data confidentiality against cloud and against accesses beyond authorized rights. To resolve these issues, we designed a data encryption model that is in charge of storing data in an encrypted format in the cloud. To improve the efficiency of the designed architecture, the service in form of the model designed allows the users to choose the level of security of the data and according to this level different encryption algorithms are used.***

Keywords: Data Storage, Security, Confidentiality, Integrity, Cloud Computing

1. Introduction

Cloud computing [13] is defined as for enabling suitable, on-demand network entrance to a shared pool of configurable calculating resources. Cloud computing everything is delivered as a service,there are three main service models used in the cloud namely:

- Platform as a Service
- Software as a Service
- Infrastructure as a service

a) Security issues

Cloud as a method of providing computing resources has many challenges based on design issues which affect the efficiency, security and performance of the entire system, these challenges could be:

- **Data Storage[17]:** Cloud storage providers manage the data in multiple copies across many independent locations
- **Cloud Confidentiality**: Confidentiality can be defined as the sensitive data not being disclosed to unauthorized process, devices and person. A cloud service provider knows where the user's public or private data is located and who can/cannot access the data.
- **Data Integrity [17]**: Data Integrity is defined as the rightness of data stored in the cloud. The alterations between two updates of a record violate the data integrity.
- **Data Security[17]:** In the traditional file systems data was stored within boundaries, but cloud data is stored outside the boundaries of an organization, say, and third party storage using strong encryption techniques.

To resolve the above listed challenges, cryptography [5] can provide solutions such as reassuring the receiver/recipient that the message received has not been tampered with or altered – this can be defined as **Integrity Checking.** This can be achieved by generating a legitimate source and authentication.

Securing the database can be a means of securing the cloud. This can be achieved using different encryption/decryption algorithms which are classified as follows:

- **Symmetric key**: this refers to encryption methods in which both the sender and receiver share the same key [15]. Examples of such algorithms include:**3DES, DES,BLOWFISH, and AES etc**.
- **Asymmetric key**: this is a public key cryptography that entails using different keys for encryption and decryption [18]; this means that there is a key for private and another different one for public. Therefore, the private key is kept by the receiver and the public is kept by anyone(public)
  Examples of such algorithms includes: **RSA, DSA etc**.
- **Hash Algorithms [14]**: this is where the input data(message) is recreated from the hash value(message digest/digest)
  Examples of such examples include:**MD5, SHA, MD2, MD4, MD6.SHA-256, SHA-512, SHA-1, Whirlpool etc.**

To ensure the security of data in the cloud we propose an effective way with the features of CIA (Confidentiality, Integrity and Authentication). This effective way uses theconcept of combining AES and Blowfish which increases the run time for both encryption and decryption. This means that the total time required for hybrid algorithms will be the addition of both algorithms' run time (processing time).Blowfish requires less time as compared to other algorithms. It also adds the additional processing time thus enhancing the security.

This paper mainly concern with the Introduction of the Cloud Computing, Security Challenges related to the cloud and the basic techniques available for the security and integrity of cloud server.

1st section covers: Introduction of cloud computing and the security challenges related to the cloud.
2nd section covers: Related work(what has been done there before), Criticism (critique what has been there before)

3rd section covers: Model descriptions including the approach used
4th section covers: Experiments and results

4.1 Experiment setup(snapshots)
4.2 Actual Experiments
4.3 Results and Discussion
5th section covers: Conclusion and future work

2. Related Work

Cloud supports large data storage,these results to lots of pressures in the cloud computing which are avoided in the cloud. The main threats in the cloud are confidentiality and data integrity in the cloud data storages. Calce et al introduces the use of a single box for putting everything in the cloud computing model,this only makes it easy for hackers [10] thus lacking **SECURITY.**

Sravan Kumar et al proposed a method of proof by adopting the use of Meta Data. This data is created using randomly selected bits from original file and is appended in an encrypted form to be stored on the cloud, therefore whenever a person wants to check for integrity, he/she throws a challenge by specifying block number and its corresponding Meta Data and finally decrypt's for proof of Correctness [16].

Dalia et al also implemented a mechanism in which integrity is checked at 2 sides by cloud server (for the attacker who's at the inside)and by TPA(for the attacker at the outside) using a digital signature with MD5 [8].

Paresh D. Sharma et al. proposes the use of symmetric key technique using AES algorithm for stored data as well as for the data moving within the cloud or for the outside service provider, then this service provider cannot use these data if it didn't get the key cryptography. So the service provider in the cloud should use the key to get and use their data [11].

Ms.Payal P.Kilor et. Proposed a design to avoid TPA, this checks the integrity of data stored in the cloud at customer's side using security keys [9].

Juels and Kaliski proposed a model Proofs of Retrievability (POR) this guarantees a remotely and reliable integrity of the data without having to retrieve a data file [1].

GeetaSarote introduce threat model to treat privacy problems in the cloud [12].One of the biggest Concerns with cloud storage is the issue of truth authorization of trusted cloud data from the server side, this is not the issue on the designed model.

3. Model Description

The encryption and decryption of data is done by combining both AES and Blowfish algorithms. Combining the two algorithms increases the run time for both encryption/decryption thus increasing the total time required for both processing time.

In our proposed work we compare AES, Blowfish and the combination (AES +Blowfish) based on the performance parameters like: **Throughput, Encryption Time, Cipher text Size** and **Delay**

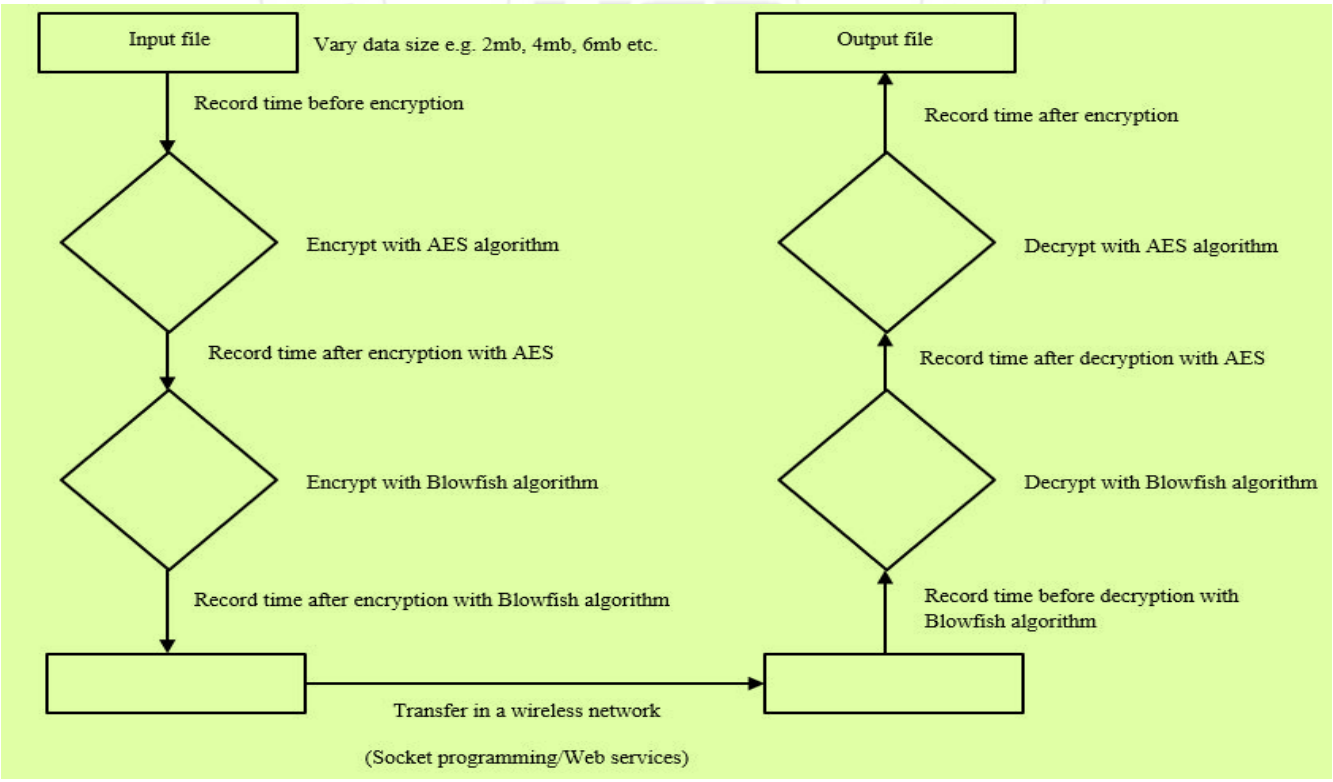

Figure 1: Hybrid AES and Blowfish data encryption and decryption

The named parameters can be calculated as follows:

- **Throughput:** this can be defined as the number of bits transferred per unit time. Its standard units= **bytes per sec**
  Throughput= uploaded file size/delay time
- **Cipher text size:** this refers to the length of encrypted data, its standard units are in **bytes**
  Cipher text size=length of encrypted data
- **Encryption Time:** this is the time taken by the server to encrypt any file or data. Its standard units are in **Nano seconds**.
  Encryption Time =Encryption End Time – Encryption Start Time
- **Delay time:** this is the difference between start time uploading time and end of uploading time. Its standard units are the same as that of Encryption time.
  Delay Time = End uploading time- Start Uploading Time

4. Experiments and Results

4.1 Experiment setup

An application has been designed and implemented in java language on the same network to achieve the functionalities of the client and the server. We have it that the cloud and the server are on the same network so that they can be in apposition to communication; we therefore put them on the same ip address for them to communicate without any hindrances.

This makes the client and the server which are on the same domain be subjected to the same parameters. Based on the experiment we have computed the parameters value for AES, Blowfish and the combination or the hybrid system(AES +Blowfish) for the same file size.

Below is a table with respective tested parameters and the respective values for the said algorithms:

Table 1: Algorithm Parameter values

Algorithms → / Parameters ↓	*AES*	*Blowfish*	*AES + Blowfish*
Encryption Time	1119	3	1123
Delay Time	586	528	63
Cipher Text	0.020195007	0.020175934	0.019347898
Throughput	0.03583618	0.03977273	0.040768746
File size	21kb	21kb	21kb

4.2 Actual Experiments

Server

Figure 2: Main Server Interface

Figure 3: Selecting a file to encrypt using server interface

Figure 4: Server Encryption Output Details

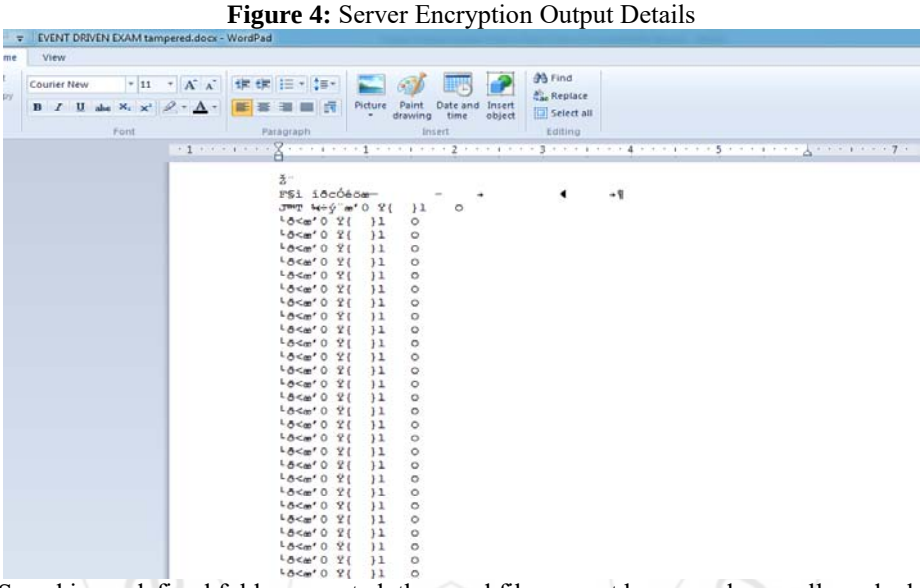

Figure 5: File Saved in predefined folder encypted, the word file can not be opened normally and when opened with wordpad, the below fig show the encypted content

No file preview, indication that it has been encrypted but it retains its original name and extension

Client

Figure 6: Main Client Interface

Figure 7: Client Prompt to enter the IP address of the running server

Figure 8: Client Prompt to choose the file to be decrypted from the server and the default file extension is automatically assigned

Figure 9: Client Decryption Output Details

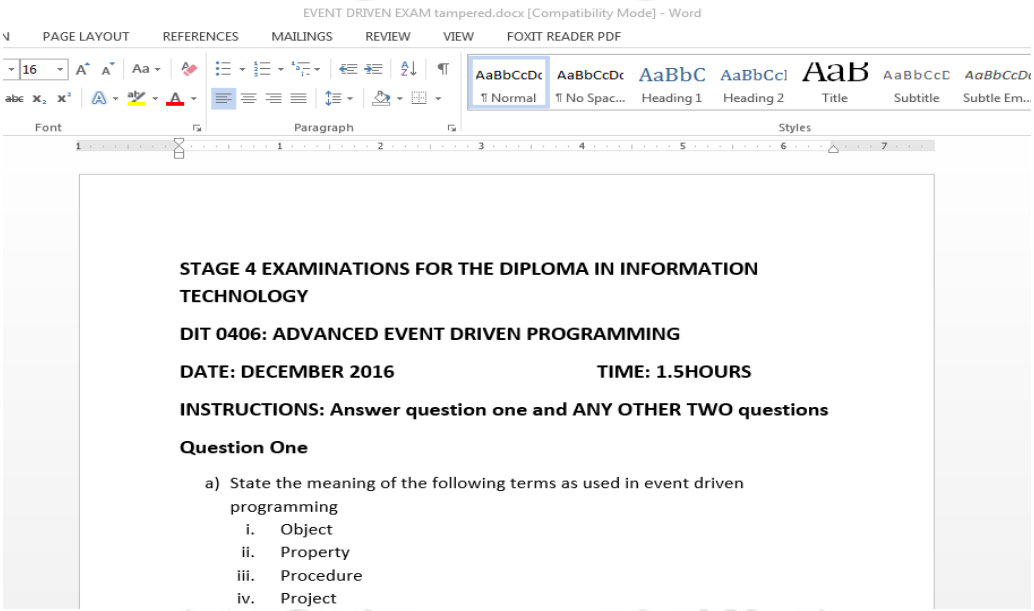

Figure 10: File is decrypted back and is now in a readable format as shown below, can be opened with Ms. Word

4.3 Results and Discussions

Results show that AES is the best algorithm of symmetric encryption technology. AES algorithm is more secure than the Blowfish algorithm but on the other hand Blowfish is more secure than other algorithms. Blowfish runs faster than other symmetric algorithms [2].AES is the symmetrical based encryption standard by NIST [3] [4].

The hybrid algorithm is more secure since it has the characteristics of both algorithms and makes it more vulnerable to threats.

5. Conclusions and Future Work

When the clients store data in the cloud, there's always an issue whether or not cloud service provider stores the data securely. Security as earlier discussed is the main challenge faced while storing data in the cloud, the proposed system provides security for the data stored in the cloud computing model through the help of AES and Blowfish algorithms.

Results show that AES is the best symmetric encryption algorithm, it's more secure than Blowfish though compared to other algorithms Blowfish is by far the best. Blowfish gives the highest throughput as compared to AES.

The hybrid of AES and Blowfish gives the properties of both algorithms thus making the formed hybrid algorithm much stronger to threats. This makes the formed hybrid system secure by increasingly adding the complexity functionalities.

The future scope of this work can be extended by:

- Performing the same experiments using audio and video as well.
- Compression algorithm can be performed for faster encryption.
- Performing the same experiments using some locking techniques for security mechanism.

References

[1] Retrievability for Large Files," In CCS '07: Proceedings ofthe 14th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 584–597.
[2] A.Nadeem and M.Y Javed.,"A PerformanceComparison of Data Encryption Algorithms,"IEEE Information and Communication Technologies, 2005.ICICT 2005.First International Conference, 2006, pp. 84-89.
[3] J.Daeman and V.Rijmen,"AES submission document on Rijndael, Ver2", September 1999.
[4] "Announcing the AdvanceEncryption standard", FIPS Publication, 2001
[5] Gurpreet Kaur And Manish Mahajan (2013), ―Analyzing Data Security for Cloud Computing Using Cryptography Algorithms‖, International Journal of Engineering Research and Application, Vol.-3,782-786.
[6] H. Shacham And B. Waters (Dec.2008), ―Compact Proofs of Retrievability, ‖ In Proceedings. Of Asia Crypt‖08.
[7] Kamak Ebadi, Victor Pena Etc.‖High Performance Implementation and Evaluation of Blowfish Cryptographic Algorithm on Single-Chip Cloud Computer: A Pipelined Approach ‖.
[8] K.Govinda, E.Sathiyamoorthy (2012), ―Data Auditing in Cloud Environment using Message Authentication Code‖, International Conference on Emerging Trends on Advanced Engineering Research (ICETT).
[9] Ms.Payal P.Kilor and Prof. Vijay B.Gadicha (2014) ―Data Integrity Proofs in Document Management System under Cloud with Multiple Storage‖, International Journal of Engineering &Computer Science, and vol.3.
[10] Omer K.Jasim et. al.(2013) ―Efficiency of modern encryption algorithms in cloud computing‖, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 2.
[11] Paresh D.Sharma, Prof. Hitesh Gupta(February 2014) ―An Implementation for Conserving Privacy based on Encryption Process to Secured Cloud Computing Environment‖ IJESRT Sharma, 3(2).
[12] P.Metri and G.Sarote (2013), ―Privacy Issues and Challenges in Cloud Computing‖, International Journal of Advanced Engineering Science and Technologies, vol.no.-5, 1-6.
[13] R.Buyya, C.S.Yeo, S.Venugopal (2009), ―Cloud Computing and emerging IT platforms: vision, hype and reality for delivering computing" as 5th utility, Future Generartion Computer System, 25: 599-616.
[14] Schneier, Bruce. (2014) "Cryptanalysis of MD5 and SHA: Time for a New Standard". Computerworld. Retrieved.
[15] ShivShakti etc. (January-Febuary-2013).‖Encryption using different techniques:A Review international journal in Multidisciplinary and academic research (SSIJMAR) vol.2 No.1 (ISSN 2278-5973).
[16] Sravan Kumar and Ashutosh Saxena (2011), ―Data Integrity Proofs in Cloud Storage", 978-1-4244-8953-4/11/$26.00© IEEE.
[17] S.Subashini and V.Kavitha (2011), ―A Survey on security issues in service delivery models of cloud computing". Journal of Network and Computer Applications 34, 1-11.
[18] Zaigham Mahmood(2011), ―Data Location and Security Issues in Cloud Computing‖, Proceedings of International Conference on Emerging Intelligent Data and Web Technologies.