International Journal of Engineering & Technology, 7 (2.20) (2018) 150-152

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Data security and storage in cloud using hybrid algorithms

L. Archana [1] *, K. P. K. Devan [2], P. Harikumar [2]

[1] PG Student, Easwari Engineering College, Chennai, Tamilnadu, India
[2] Associate Professor, Easwari Engineering College, Chennai, Tamilnadu, India
**Corresponding author E-mail: archana.cse@gmail.com*

Abstract

Cloud Computing has already grabbed its roots in many industries. It has become a fascinating choice for small budget organizations, as On-demand resources are available on pay as you use basis. However, security of data being stored at cloud servers is still a big question for organizations in today's digital era where information is money. Large organizations are reluctant to switch to cloud services since they have threat of their data being manipulated. Cloud service provider's claim of providing robust security mechanism being maintained by third party, but still there are many reported incidents of security breach in cloud environment in past few years. Thus, there is need for ro-bust security mechanism to be adopted by cloud service providers in order for excelling cloud computing. Since there are n number of data's in cloud, Storage of those data are to be placed with high rank of Significance. In Existing system, no efficient hybrid algorithms are used there by security and storage is compromised to significant ratio. We propose AES and Fully Homomorphic algorithm to encrypt the data, thereby file size get is compressed thereby increasing Data security and stack pile.

Keywords: *Advanced Encryption Standard; Data Encryption Standard; Fully Homomorphic Encryption.*

1. Introduction

Cloud computing is a paradigm, a model to facilitate prevalent access to pools of configurable resources (such as computer networks, servers, storage, applications and services).Overall consistency and efficiency can be ensured by cloud, that allows various owners and users with varying capabilities to store and process datasets via privately possessed cloud or third party authentication.

The Service Models in cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). A different kind of Cloud includes Private cloud, Public cloud and Hybrid cloud. Security is now becoming a major concern. Data can be gathered through tapping wires, planting bugs in output devices, shifting through trash receptacles, monitoring electro-magnetic radiation, bribing key employees, inferring data point from other values, stealing, buying, bribing etc.

There are various threats to data's especially while transferring them from one center to the other. Data are being stored in cloud as it provides seamless file transfer, an edge, an easy backup. Recently, there is an increase in outsourcing of files for the above stated reason.

1.1. Motivation

Various hybrid algorithms are being in use. Among various cryptographic algorithms, Advanced Encrypted Standard (AES), a symmetric key block cipher and Homomorphic algorithms played a major role in motivating this paper.

Data Encryption Standard had various disadvantages. In S-box 4th iteration, the last three output bits can be derived in the same way as the first output bit by complementing some of the inputs. Any two bits of inputs randomly chosen to an S-box array can create the same output. Also it is possible to obtain same output in a single round by changing bits in only three neighboring S-boxes. Major disadvantage is the generation of weak keys which are subject to brute force attack, man in the middle attack. To overcome these weaknesses Advanced Encryption Standard is being designed.

AES is a non-fiestal cipher that encrypts and decrypts data block of 128 bits. The key size can be 128 bits, 192 bits or 256 bits depending on the rounds (rounds may be 10, 12 or 14). This paper deals with total 10 rounds and 128 bits key size. Various rounds involves substitution, unlike DES substitution is done for each byte, Second only one table is used for transformation of every byte, which means two bytes are the same. Each round has the following steps. Sub bytes, shift rows, mix column, add round key.

Key expansion algorithms in AES – 128 bits, the words are generated in group 4. The cipher key creates the first four words (w0 to w3). If i mod 4 not equal to zero, wi←(wi-1)+(wi-4), otherwise wi←t+(wi-4). This helps in providing additional storage space.AES has no serious weakness unlike DES. The key expansion routine can be implemented without storing a single table. AES without any doubt is secure against brute force attack If we can break DES in t seconds, we need (two^72*t) seconds to break AES. Homomorphic algorithm allows us to perform computations on the cipher text. It is comparatively secure and provides additional storage to the text data files.

2. Related works

2.1. Advanced encryption standard

The Saakinaah Ali Pitchey, Wail Abdo Ali, Farida Ridzuan and Madihah Mohmad sandi [12], [4] suggests introducing a support pattern for a cloud storage system where security and privacy is at the maximum concern. In proposed system they have tried to pro-

vide security for the files stored in USB, in which data may get lost if the USB device is lost. They have used waterfall model to design a system correctly and apply AES and RSA algorithm to provide security. However, the major concern is, it does not detect the correct USB that would contain the keys for encryption and decryption.RSA can be cracked in spite of its complexity. Better algorithm can be used.

Ali Azougaghe, Zaidkartit, Mustapha Hedabou, Mostafa Belkasmi,, Mohammed El Marakki [6], share their concept of inter-cloud data sharing using AES and Elgamal Cryptographic algorithm in proposed system to protect data from unauthorized users. AES performs well in wide variety of networks and produces high performance. It is much faster and not susceptible to many attacks. Elgamal algorithm is used to provide additional security but DoS attack is still being under research.

Deepak Singh and Harsh K Varma [13], [8], in order to overcome the difficulty of privacy, authentication and integrity between user and CSP, they have adapted a new framework using AES, SHA-1 for security. Though AES and SHA-1 are both efficient that provides integrity and confidentiality, brute-force attack remains a major concern.

Babitha.M.P and KR Ramesh Babu [2], [10] addresses different data security and privacy protection issues in cloud where provider is not a trusted one. They have used AES algorithm and SMS message alert mechanism if in case of security breach. They have divided the file into blocks and transferred them to cloud by encrypting data using AES algorithm in proposed system offering authentication, authorization and confidentiality. In addition, a comparison on AES, DES and RSA is made and AES is found to be more secure than the rest. Time delay in computation increases as the file size is increased hence this is under consideration.

Amjad Alsirami, Peter Bodorick, Srinivas Sampalli [11], [12] have proposed a combination of encryption algorithms and distribution system to improve confidentiality. Pope et al says he has used AES - CBC algorithm for encryption and proxy server helps to retrieve the information via queries. Detailed study on Delays with many predicates AND,OR,WHERE can be done as future enhancement on fragmented data's as Analytical method can't be used to measure the data.

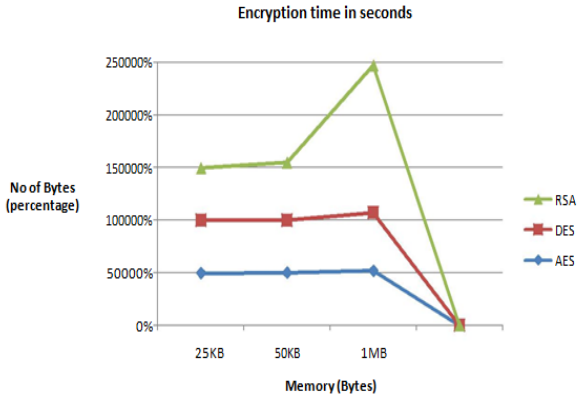

Fig. 1: Comparative Execution Times (in Seconds) of Encryption Algorithms in ECB Mode on a P-II 266 Mhz Machine [5].

Lizhi Xiong, Zhenquan xu proposes re-encryption technique, for providing security. A piece of data is encrypted twice using different keys and final cipher text is progressive elliptic curve algorithm is used in this paper. Usage of single algorithm twice causes complexity in key usage. Hence different algorithms can be used. Data backup, error detection, and data recovery, privacy, integrity and availability are ensured. In spite of this collision attack still remains.

2.2. Homomorphic encryption

All various researches have been made on fully homomorphic algorithms over integers. A "public key compression technique" [1] has been used. Gentry (2009), proposed a bootstrapping method that had limitations on multiplication of cipher texts and contained noise. If the size of noise breaks the threshold, exact time for decryption is impossible.

Gentry and Halevi (2011) suggested to use next lattice based dimension depending on key sizes. For lattice dimension of 512 and key size of 17mb, the time taken for key generation is 2.5 sec and the time taken for recryption was 6 sec.

Dijk, Gentry, Halevi, Vaikunthan [9] proposed somewhat homomorphic technique, which also included the above stated disadvantages. This public key compression method reduced key size 900 times with set of medium parameters. Based on Public Key Compression technique and CRT, efficient somewhat homomorphic scheme was proposed. It focused on reduction of public key size and cipher text size. The Public key size reduction observed was $O(\lambda^{10})$ to $O(\lambda^{7.5})$ and cipher text size decreased from $O(\lambda^{5})$ to $O(n\lambda^{5/n})$.Since both scheme has same secret key size decryption was also similar. On comparing DGHV and BV- BGV technique, a realization was made on multiplication of cipher texts where noise level is increased.

3. Proposed systems

This paper mainly focuses on providing storage and security to the Text Data files. The procedure is as follows:

1) User registers himself with the cloud service provider and requests the needed file.
2) The cloud service provider verifies with the Owner about the authorization and then the owner uploads the file to the cloud service provider using Advanced Encrypted Standard (AES) algorithm. Private Key is generated at the same time, which is obtained by the user in the end for decryption.
3) The cloud service provider splits the AES encrypted file into three different files, applies Fully Homomorphic Encryption and reduces the file in turn and stores as a different cluster in the same data centre.
4) The cloud service provider also sets timer. Within the allocated time, the user must download the file. If time elapses, the user cannot download the file from the cluster and they will be automatically deleted from the cluster. Therefore, if the user wants to download the file he must send the request again.
5) The user gets the private key from the Data Owner, Decrypts and obtains the requested text data file securely from the cloud.

In the Gentry scheme, bootstrapping proved unfeasible in practice due to a massive overhead in both computation and memory cost. For example

Cipher text c1 = Encrypted text (m1) and cipher text c2 = Encrypted text (m2) where m1 and m2 are the two plain texts.

- M1+m2 = Decryption of cipher texts(c1+c2)
- M1*m2=Decryption of cipher texts (c1*c2)

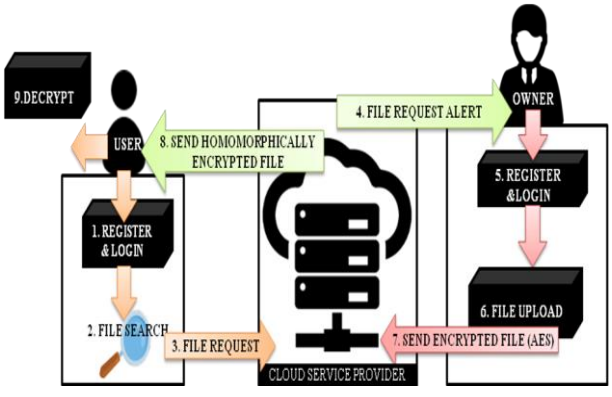

Fig. 2: System Architecture.

This is said to be homomorphic addition and multiplication. Homomorphism is computation that takes place in an n Algebraic group. The scheme homomorphic for both addition and multiplication is called fully homomorphic.BGV method is adapted along with modulus switching and double crt technique more amount of storage space is reduced.

3.1. Brakerski gentry vaikuntanathan homomorphic encryption scheme

Brakerski, Gentry and Vaikunthan suggested this technique.

3.2. Encryption and decryption

Encrypt (plaintext m, public key pu): Cipher text c
Decrypt (plaintext m, private key pr): plaintext m

3.3. Level shifting operation

Rescale (ciphertext C): Cipher text C'
Switch key (Augumented Ciphertext c): Cipher text C'

3.4. Homomorphic operation encryption

Add (c1+c2) =a1, Add (c3+c4) =a2,
Mul (a1, a2) =b1, compute xi= (b1 mod k)
Decryption:
Inverse result

4. Results

A qualitative performance analysis have been made and presented here. This paper deals with the message size and storage space occupied by those messages using AES algorithm as well as FHE method and time taken to download those files. Novelty in our approach is usage of minimal algorithms and providing efficient security and storage in cloud environment. User downloads the file within 0.99 sec provided guaranteed 5G network.

Table 1: Result Analysis (Fast 5g Network)

Results Obtained			
Initial File Size	Aes	Fhe(Bgv)	Download Time
100kb	123kb	30kb	0hr:0min:1sec
200kb	245kb	54kb	0hr:0min:1sec
500kb	613kb	132kb	0hr:0min:2sec
1000kb	1054kb	S258kb	0hr:0min:2sec

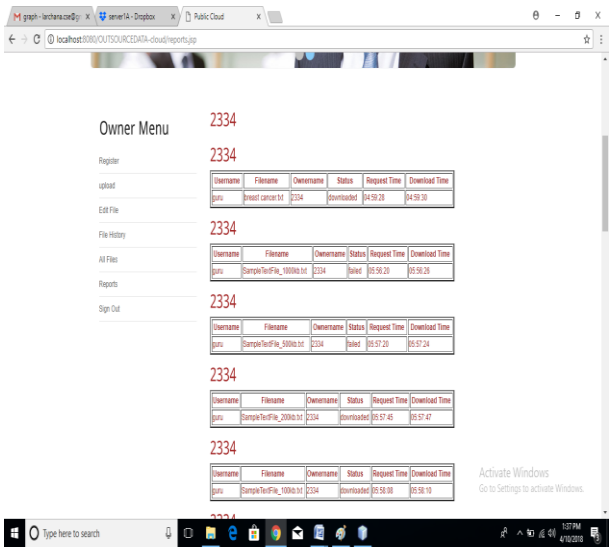

Fig. 3: Screen Showing the Output.

5. Conclusion

In this paper deals with various hybrid algorithms which is more secure against man in the middle attack, DoS attack, brute force attack and random attack. It also reduces storage space comparatively as shown from the above figure. In future, an adaption of other version of AES - 192 bits or AES - 252 bits and various other Homomorphic computational combinations can be inferred in order to be even more efficient. Network speed and many other security threats can also be taken under consideration.

References

[1] Alexandr N. Gerasimov, Anna V. Epishkina, Konstantin G. Kogos,"Research of Homomorphic Encryption Algorithms over Integers", 978-1-5090-4865-6/17/$31.00 IEEE, (2017).
[2] Dr. A. M. Gonosai and L.M. Raval, "Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network", International Journal of Computer Trends and Technology, Vol 11(1), pp. 7-12, May 2014.
[3] J.Viega,"Cloud Computing and the Common Man", Journal Computer Vol 42(8), pp. 106-108, August 2009.
[4] K.Yang and J.Xiaohva, "Security for Cloud Storage Systems", Springer Brief in Computer Science, 2014.
[5] L.Archana and Mr.K.P.K.Devan,"A Survey on Various Cryptographic Algorithms" International Journal of Recent Engineering Research and Development (IJRERD) ISSN: 2455-8761, Volume 02 – Issue 12,| December 2017, PP. 01-04.
[6] L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol 2,Issue 8,August 2013.
[7] P.Mell, Grance," The NIST definition of Cloud Computing", NIST Special Publication, pp. 800-145, Sep 2011.
[8] P.Rewagad and Y.Pawar," Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies, 2013.
[9] Peng Zhang , Xiaoqiang Sun, Ting Wang, Sizhu Gu, Jianping Yu, Weixin Xie, "An Accelerated Fully Homomorphic Encryption Scheme Over The Integers", Proceedings of CCIS2016, pp. 419-423.
[10] Prerna Mahajan,Abhishek Sachdena,"A study of Encryption Algorithms AES,DES and RSA for Security",Global Journal of Computer Science and Technology Network web and Security,vol.13,Issue 15,Vol 1,2013.
[11] R.A.Popa, C.M.S.Redfield, N.Zeldovich al,H.Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing", pp. 85-100, 2012.
[12] T .Chou, "Security Threats on Cloud Computing Vulnerabilities", International Journal of Computer Science and Information Technology, Vol 5(3), pp .79-88, 2013.
[13] Y. Pawar, P. Rewagad and N. Lodha, "Comparative Analysis of PAVD Security System with Security Mechanism of Differenr Cloud Storage Services",2014 Fourth International Conference on Communication Systems and Network Technologies, 2014.