International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

Secured Data Migration using AES Algorithm and Authentication Techniques in Cloud Environment

R. Amrutha[1], P. Perumal[2], S. Balaganesh[3], D. Ishwarya[4]

[1,3,4]Student, Dept. of Computer Science and Engg., Sri Ramakrishna Engineering College, Coimbatore, India

[2]Professor, Dept. of Computer Science and Engg., Sri Ramakrishna Engineering College, Coimbatore, India

Abstract**: Cloud computing service is valuable in various segment of human activities and it has been a future information technology design for organizations, education sectors and other commercial sectors. Cloud storage services allows clients to put away data and enjoy the high quality on-demand cloud applications without the stress of constant management of their own software, hardware and data. It moves data maintained by cloud service provider on the cloud storage servers which prevent too much burden on users such as control of the physical data possession. Although the welfares of cloud services are more, but there are new threats related to data safety due to physical possession of outsourced information. Users are putting away their sensitive data and since they have no more control over the services or their stored information, there is need to implement strong security strategies that will prevent unauthorized access to the system functionalities and user's information. To address data security threats while in cloud storage, strong authentication scheme and data encryption scheme was introduced in this paper by fragmentation of file and Advanced Encryption Standard (AES) algorithm for the encryption of users' data contents before putting into storage and Authentication scheme for valid user verification and protection of unauthorized access to all units of system functionalities.**

Keywords**: cloud storage, Advanced Encryption Standard and Authentication Scheme, Fragmentation.**

1. Introduction

Cloud computing is emerging as a key computing platform for sharing resources that include infrastructure, software, applications, and business processes. Gartner predicts by 2015, 10% of overall IT security enterprise capabilities will be delivered in the cloud, with focus on messaging, web security and remote vulnerability assessment. Other focus areas will include data-loss prevention, encryption, and authentication, as technologies aimed to support cloud computing mature. The notion behind cloud computing is that work done on the client side can be moved to some unseen cluster of resources over the internet. Cloud Service Provider (CSP) maintains database and applications for the users on a remote server and provide independence of accessing them from any place through a network. There are three major cloud service categories: software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS).

Cloud computing is the broader concept of infrastructure convergence. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability, and less maintenance to meet business demands. For example, we can manage and store all smartphones or tablets apps at one location i.e. cloud. So we do not require any memory space at our end. This also gives the security of data and applications in case device is damaged or lost. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. Security goals of data cover three points namely: Availability, Confidentiality, and Integrity. Cryptography, in modern days is considered grouping of three types of algorithms. They are Symmetric algorithms used the same (secret key) key for encryption and decryption.

The same key messages are used for encrypted by the sender and decrypted by the receiver. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), IDEA Twofish, Ron's Code (RCn), and Triple DES, Blowfish etc. Asymmetric algorithms use different keys. One key (public) is used for encryption and other (private key) is used for decryption. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm(DSA) etc.

Fig. 1. General Structure of Cloud Computing

2. Literature review

In order to make the data secure in cloud environment researches proposed many systems.

[1] This paper addresses different data security and privacy protection issues in a cloud computing environment and proposes a method for providing different security services like

authentication, authorization and confidentiality along with monitoring in delay. 128-bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. In this proposed approach data is encrypted using AES and then uploaded on a cloud. The proposed model uses Short Message Service (SMS) alert mechanism for avoiding unauthorized access to user data.

[2] To address data security threats while in cloud storage, strong authentication scheme and data encryption scheme was introduced in this paper using Advanced Encryption Standard (AES) algorithm for the encryption of users data contents before putting into storage and Authentication scheme for valid user verification and protection of unauthorized access to all units of system functionalities.

[3] This paper propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, they present construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

[4] The purpose of this work is to secure the Multi-cloud using secret sharing algorithm. This objective is achieved using Shamir's secret sharing algorithm. This secret sharing scheme has a good foundation that provides an excellent platform for proofs and applications. Also the disadvantages of single cloud and advantages of multi cloud were addressed in this paper.

3. System model

A. *Problem definition*

With the tremendous growth of sensitive information on cloud, cloud security is getting more important than even before. To ensure that the data is secure is more important, than just migrating the data to cloud servers.

1) *Introduction to Proposed System*

The first authentication scheme consists of valid username and password. Second authentication scheme is to ensure that only authenticated users are allowed to access the private cloud. Each authenticated user is given the secret key and the storage location for those keys are in safe location. Even if hackers or malicious attackers eavesdrops or hacked the database and get access to username and password, that will not grant them access to the system. Based on system design, new users can fill request form and submit, service provider will verify new user before grant or deny access. Advanced Encryption Standard (AES) algorithm serve as scheme for data encryption which is the most secured algorithm as of now. This system provides additional security by fragmenting the file into two parts and encrypting each file with AES two times. The two encrypted files are stored in two different private cloud servers. The system is divided into two functionalities, cloud service provider and cloud users.

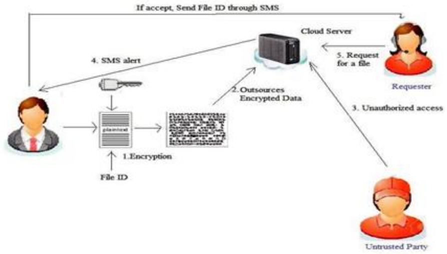

Fig. 2. Architectural diagram of proposed system

2) *Module description*

The overall proposed system is divided into three modules: Module 1: User authentication and database connectivity. The authenticated user accounts are registered by the admin in order to prevent the unauthorized users to signup and the database is created in order to store the valid credentials of the authenticated users. Database is connected to the system and the details of the users are stored.

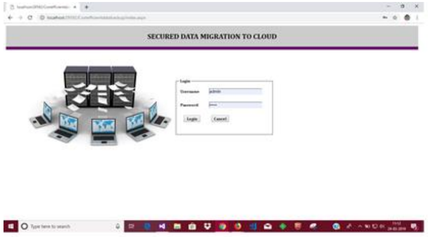

Fig. 3. User authentication and database connectivity

Module 2: Fragmentation of the file and double AES encryption. The file to be uploaded is fragmented into two subfiles. Each sub file is encrypted twice using AES algorithm with two different complex keys. The two encrypted files are generated. The two encrypted files are uploaded in the system and are decrypted to generate the original file.

Fig. 4. Encryption result

Module 3: Setting up of private cloud server and connecting the server Private clouds are set up using Tonido software and the valid URL for the cloud servers are collected. The users are redirected to the cloud to upload the two encrypted files to two different private cloud servers. The encrypted files are downloaded at the other end by valid users. The encrypted files are uploaded to the system to generate the original file.

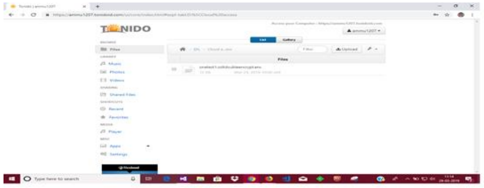

Fig. 5. Setting up of private cloud server and connecting the server

3) *Implementing AES Algorithm*

AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. We propose AES with 128-bit key length. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical. 16-byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule.

For encryption, each round consists of the following four steps:

- SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).
- Shift Rows – a transposition step where each row of the state is shifted cyclically a certain number of times
- Mix Columns – a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- Add Round Key – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

4) *Why AES?*

- AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP's.
- Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
- This algorithm has speedy key setup time and good key agility.
- It requires less memory for implementation, making it suitable for restricted-space environments.
- The structure has good potential for benefiting from instruction-level parallelism.
- There are no serious weak keys in AES.
- It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits).
- Statistical analysis of the cipher text has not been possible even after using huge number of test cases.
- No differential and linear cryptanalysis attacks have been yet proved on AES.

5) *Authentication Scheme*

The authentication scheme used in the proposed system design and implementation is categorized in to two as described above. Each user has username and password, both are saved in same database, to avoid possibility of unauthorized access to the database, each user has cloud access key, this help to strength authentication scheme. The secret key is in separate and save space with username and password. Despite user login with valid username and password, that doesn't grant access to the system functionality, secret key must be valid.

6) *Fragmentation*

The file to be uploaded is divided into two subfiles each containing first and last half of the data on the file. Each fragmented file is encrypted two times with AES algorithm and uses two different keys for each encryption. The two fragmented files are uploaded in two different private cloud servers, such that even if the hackers attack one server they would still only get one part of the file and not the another part.

7) *Comparing AES with Other Algorithms*

The fact that the cipher and its inverse use different components practically eliminates the possibility for weak and semi-weak keys in AES, which is an existing drawback of DES. Also, nonlinearity of the key expansion practically eliminates the possibility of equivalent keys in AES. A performance comparison amongst AES, DES and Triple DES for different microcontrollers shows that AES has a computer cost of the same order as required for Triple DES [9]. Another performance evaluation reveals that AES has an advantage over algorithms-3DES, DES and RC2 in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption as well as decryption. Also in the case of changing data type such as image instead of text, it has been found that AES has advantage over RC2, RC6 and Blowfish in terms of time consumption.

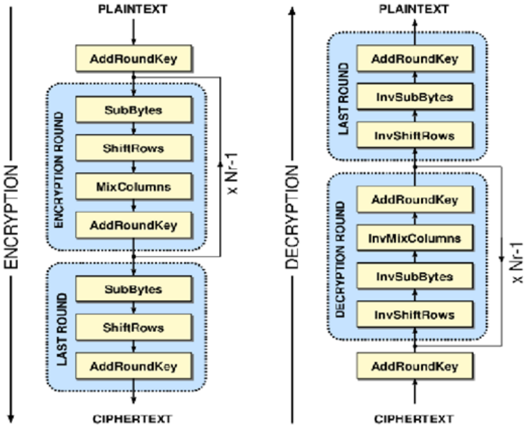

Fig. 6. AES Encryption and Decryption

4. Result

The experimental result of the proposed system provides enhanced security level over AES algorithm by fragmenting and encrypting/decrypting the file twice with AES algorithm.

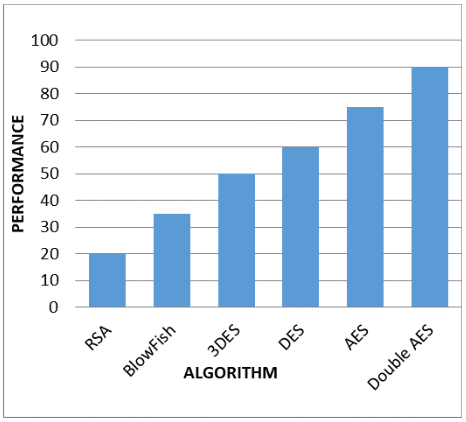

Fig. 7. Performance Comparison of Algorithm

5. Conclusion

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. AES encryption is the fastest method that has the flexibility and scalability and it is easily implemented. On the other hand, the required memory for AES algorithm is less than the Blowfish algorithm. AES algorithm has a very high security level because the 128, 192 or 256-bit key are used in this algorithm Additional functionalities for futures work includes Auto verification of users' encrypted data while in transit over internet to ensure that it doesn't contain any harmful data. Provide means of secured communication between cloud clients while monitoring their activities and protection of network layers.

References

[1] Babitha M.P. and K. R. R. Babu, "Secure cloud storage using AES encryption," International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, pp. 859-864,2016.

[2] Mohamed Ismail, Badamasi Yusuf, Ensuring Data Storage in Cloud Computing with Advanced Encryption Standard (AES) and Authentications Scheme (AS), International Journal of Information System and Engineering, Vol. 4 (No.1), April, 2016.

[3] T. Jun-Feng, Z. Jia-Yao and D. Rui-Zhong, "Date Hierarchical Storage Strategy for Data Disaster Recovery," in *IEEE Access*, vol. 6, pp. 45606-45616, 2018.

[4] Taek -Young Youn, Ku - Young Chang, Kyung -Hyune Rhee, Sang uk Shin, Efficient Client - Side Deduplication of Encrypted Data with Public Auditing in Cloud Storage, vol no:6, pp. 26578-26587,2018.

[5] Amit Banerjee, Mahamudul Hasan, MD.Auhidur Rahman, Rajesh Chapagain, CLOAK: A Stream Cipher Based Encryption Protocol for Mobile Cloud Computing, vol no: 5,pp:17678-17691,2017.

[6] Bin Feng, Xinzhu MA, Cheng Guo, Hui Shi, Zhang Fu, Tie Qiu, An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing., vol. 4, pp. 7988-7910, 2016.

[7] Ying-Si Zhao, Qing-An Zeng, Secure and Efficient Product Information Retrieval in Cloud Computing, vol no:6, pp:14747-14754 ,2018.

[8] Jianghong Wei, Wenfen Liu, and Xuexian Hu, Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption, IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1136-1148, 2018.

[9] BojanSuzic, Andreas Reiter, Florian Reimair, Daniele Venturi, Baldur Kubo, Secure Data Sharing and Processing in Heterogeneous Clouds, Procedia Computer Science, vol. 68, pp. 116 – 126, 2015.

[10] M. Muhil, U. Hemanth Krishna, R. Kishore Kumar, E. A. Mary Anita, Securing Multi-Cloud using Secret Sharing Algorithm, 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), Procedia Computer Science, vol no. 50, pp: 421 – 426, 2015.

[11] P. Mell, Grance, "The NIST definition of cloud computing", Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication, pp.800-145; Sep.2011.

[12] Hyun-Suk Yu, Yvette E. Gelogo, K J Kim, "Securing Data Storage in Cloud Computing", J. of Security Engineering, pp. 252-259,2012.

[13] C.W. Hsu, C.W. Wang, Shiuhpyng Shieh, "Reliability and Security of Large Scale Data Storage in Cloud Computing", part of the Reliability Society Annual Technical Report, 2010.

[14] Qian Wang, Cong Wang, Jin Li, Kui Ren, Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", IEEE Systems Journal, Vol.9, No.1, August2015.

[15] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Ensuring data storage security in Cloud Computing", IEEE 17th International Workshop on Quality of Service (IWQoS), pp. 1 -9,2009.

[16] Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol. 13, no. 15, Vol. 1, 2013.

[17] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[18] Wentao Liu, "Research on cloud computing security problem and strategy", IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp.1216-1219.