A Hybrid Encryption Model with Attribute Based Encryption and Advanced Encryption Standard Techniques

Jaichandran R[a], Shunmuganathan K.L[b], Subapriya V[c], Rahul G[d], Shahal S H[e] and Rahul Raj[f]

A
Department of Computer Science and engineering, Aarupadai Veedu Institute of Technology, Vinayaka Missions Research Foundation (Deemed to be University), Paiyanoor, Tamil Nadu, India

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: The emergence of cloud computing has completely changed the information technology sector, storage of information's and access control. The main challenge in the migration of enterprises is the security to gain data owners confidence. In existing approach, many digital signatures based methodologies are used. In the existing approach, encryption time, security, encryption complexity are the parameters which need more focus. To overcome the existing issue, in this paper we proposed an hybrid architecture invoking attribute based encryption (ABE) for encrypting the key and advanced encryption standard (AES) for file encryption. Thus the proposed methodology provides security, confidentiality and optimizing storage and encryption cost.

Keywords: Security, encryption, attribute based encryption, advanced encryption standard

1. Introduction

Cloud computing is defined as virtualizing the physical hardware environment used for processing and storage. In this software, infrastructure, software platforms can be used by the individuals and enterprises on demand. Thus this provides a greater advantage to the individuals and enterprises in reducing the investment cost, managing cost and maintenance cost. The concept of "Pay as you go" has attracted many cloud developers, enterprises and organizations through which they can pay for their usage alone which provides transparency and gains end user confidentiality. Thus with many significant features like low cost, easy access, pay based on usage of resources, hardware and software availability virtually, support, firewalls paved path for consistent demand and growth for cloud service providers [1].

Every minute millions of data / information's are exchanged between users. Also aside millions of data / information's are stored in the cloud and accessed. Security is the major concern in the existing system. Data access, preserving data owner privacy is very important when you consider several owner and several user case study. The data owner file has to be encrypted before storing into the cloud and the owner can provide the control of access to several users. This being a complex structure, data access can be simplified by using light key management. Existing symmetric key algorithms can be classified into 2 types namely Block cipher and Stream cipher [2]. Cryptography provides encryption and confidentiality of the data owner data. Attribute based Encryption (ABE) has gained more attraction now a days in rendering security and simple access control of data when shared among several users. The access control policy are stored in access tree structure. The shared users can access the data if the policy gets satisfied.

Due to innovation of new technology brining comfortabilty to the users. Data owners can able to upload and access their data from anywhere using cloud computing. For rendering global access, the data owners store their data in the cloud. Recently, attribute based encryption has paid a lot of attention. The main objective of this study is to provide effective security and access control in the cloud environment making intrusion difficult. In ABE the attributes defined by the user plays an important role in conversion of the plain text to the cipher text.

The main goal was to provide security and access control. In this scheme it allows encryption and decryption of data that depends on attributes of users. Policy has been defined here associated with access tree structure. The ciphertext produced will be accessible by user only if the policy is satisfied. ABE policies are associated like a tree model, thus the cipher text is provided if the tree based model is matched.

Cipher text policy attribute based encryption is the enhanced version of ABE addressing security concerns in applications [3]. ABE with access tree structure achieves reduced storage cost and encryption time. Data owner file would be segregated into several subgroups with many layers of access level. Depending on the request only that particular subgroup is provided if the access control policy is met.

In this paper, we are proposing a hybrid model for providing security, confidentiality and optimizing storage and encryption cost through combining AES based file encryption and ABE based key access control.

2. Literature Survey

AES (Advanced Encryption Standard) is the most adaptable encryption algorithm used for file encryption [4]. On emergence of AES, Many encryption algorithms like DES, 3DES are been replaced. Many banks still now uses AES encryption algorithm. AES is a symmetric block cipher invoking many rounds of encryption. AES has several block ciphers like AES-128, AES-192 and AES-256. AES has several rounds of encryption such as 10, 12 and 14 rounds. Thus the input plain text is converted into cipher text after execution of sequence of rounds. AES based block cipher is secure but takes greater transmission time when compared with the stream cipher based encryption algorithms.

Attribute Based Encryption (ABE) [5] was introduced during the year 2005 in order to address the access control and security. ABE was introduced to address the key generation and easy access of public or private keys by the respective data owners. In the traditional approach, several private keys has to be noted or remembered by the data owner for each and every file, which is difficult and a challenging one. Also generation of secret or private keys for several files at a time is complex and time consuming process. ABE addresses this challenge in which user known attributes are used to perform encryption and decryption processes [6]. The cipher text generated in ABE majorly based on the user attributes such as age, school, pet name, school name etc. The cipher text would be transformed back to plain text when the defined attribute exactly matches during the decryption process. The major disadvantage which needs attention with regard to ABE is that the data owner has to utilize public key which is complex when implemented in real scenarios arising security concerns.

Our survey states AES is more adaptable for encryption has it provides more security [7]. Data transmission time is high and addition to it generating private keys and encrypting it will consume more time. Hence a hybrid based structure can be used where AES is used for encryption and ABE is used for generating the key to access the file. ABE uses asymmetric key which would be append with the AES based encrypted file. During the attribute definition, the data owner can provide access to other users to access the file.

3. Methodology

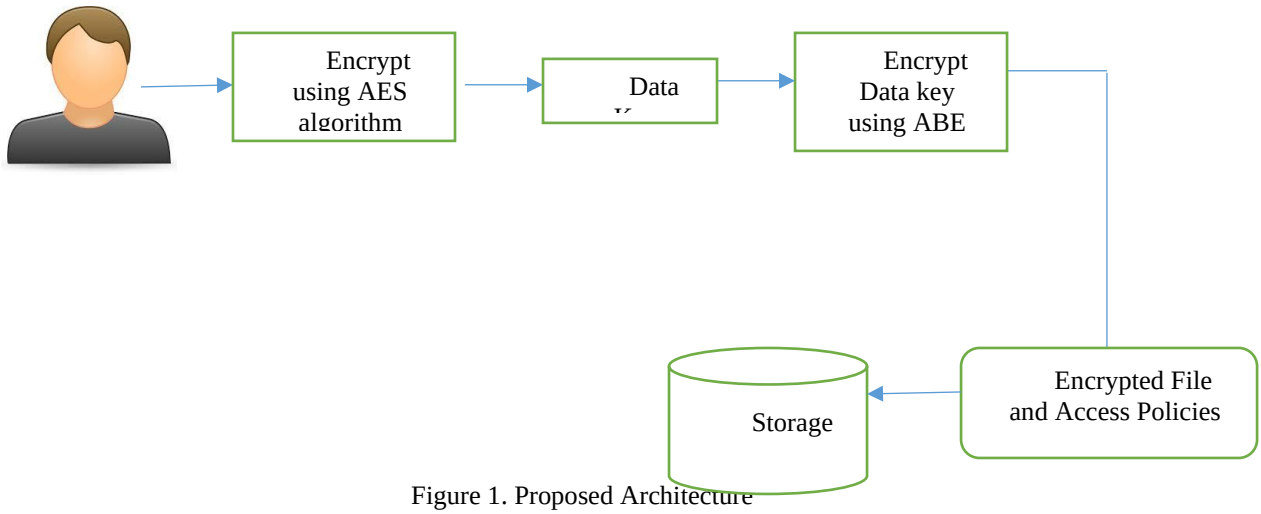

Figure 1. Proposed Architecture

Our paper proposed a hybrid security model for cloud users combining both AES and ABE encryption algorithms. For data owner file, data encryption we have proposed AES algorithm and data access authorization and key generation, we have proposed ABE encryption algorithm [8].

In ABE algorithm, attributes is the important components. In our proposed methodology to reduce the storage cost and encryption time, we have introduced the storage representation of the access control policy for a specific file in a tree based structure. To explain the tree structure in the ABE, the tree has different numbers of level. The top of the tree node is termed as the root node and the following level nodes are defined as the leaf nodes.

4. Results

Table 1: Comparison of Encryption Time

Number of attributes	ABE (1KB) m/s	AES (5KB) m/s
2	7	13
5	9	17
7	12	21

Table 2: Comparison of Decryption Time

Number of attributes	ABE (1KB) m/s	AES (5KB) m/s
2	0.71	1.75
5	1.15	3.1
7	1.75	3.5

5. Conclusion

Thus in this paper, the proposed methodology introduced was a hybrid encryption scheme invoking AES for file encryption and ABE for key generation and access control. In this system KP based ABE is used to append along with the encrypted file to manage efficiency. Integration of KP based ABE supports fine grained access control over the input data. The data owner can decide whether the users have access over the data by authentication the selected attributes. Thus our proposed work provides high security for the data transmission using AES based block cipher and reduces the key management complexity using KP based ABE algorithm and addresses each file based access control mechanism.

References

1. Lai, J., Deng, R. H., Guan, C., &Weng, J. (2013). Attribute-based encryption with verifiable outsourced decryption. IEEE Transactions on information forensics and security, 8(8), 1343-1354.
2. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE transactions on parallel and distributed systems, 24(1), 131-143.
3. Rakesh Venkat Battu*, Mangalagowri R, Authenticated Cloud Data Service Using Attribute Based Encryption, Journal of Chemical and Pharmaceutical Sciences, 2017.
4. Sneha Chandrashekhar Parit1, Dr. Rashmi Rachh2, Ciphertext Policy Attribute Based Encryption, IRJET, 2017
5. Garg, S., Gentry, C., Halevi, S., Sahai, A., & Waters, B. (2013). Attribute-based encryption for circuits from multilinear maps. In Advances in Cryptology–CRYPTO 2013 (pp. 479-499). Springer Berlin Heidelberg.
6. Gorbunov, S., Vaikuntanathan, V., & Wee, H. (2015). Attribute-based encryption for circuits. Journal of the ACM (JACM), 62(6), 45.
7. Hohenberger, S., & Waters, B. (2013). Attribute-based encryption with fast decryption. In Public-Key Cryptography–PKC 2013 (pp. 162-179). Springer Berlin Heidelberg.
8. Raja, S. Kanaga Suba, and T. Jebarajan. "Reliable and secured data transmission in wireless body area networks (WBAN)." European Journal of Scientific Research 82, no. 2 (2012): 173-184.
9. Lewko, A., & Waters, B. (2012). New proof methods for attribute-based encryption: Achieving full security through selective techniques. In Advances in Cryptology–CRYPTO 2012 (pp. 180-198). Springer Berlin Heidelberg.
10. Murugan, S., Jeyalaksshmi, S., Mahalakshmi, B., Suseendran, G., Jabeen, T.N. and Manikandan, R., 2020. Comparison of ACO and PSO algorithm using energy consumption and load balancing in emerging MANET and VANET infrastructure. *Journal of Critical Reviews*, *7*(9), p.2020.
11. Sampathkumar, A., Murugan, S., Sivaram, M., Sharma, V., Venkatachalam, K. and Kalimuthu, M., 2020. Advanced Energy Management System for Smart City Application Using the IoT. In *Internet of Things in Smart Technologies for Sustainable Urban Development* (pp. 185-194). Springer, Cham.
12. Sampathkumar, A., Murugan, S., Rastogi, R., Mishra, M.K., Malathy, S. and Manikandan, R., 2020. Energy Efficient ACPI and JEHDO Mechanism for IoT Device Energy Management in Healthcare. In *Internet of Things in Smart Technologies for Sustainable Urban Development* (pp. 131-140). Springer, Cham.