FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

Secure and Reliable Data sharing scheme using Attribute-based Encryption with weighted attribute-based Encryption in Cloud Environment

Chandrajeet Yadav[1], Vikash Yadav[2] and Jasvant Kumar[3]

[1]*CSE Department, Maharishi University of Information Technology, Lucknow, India*
[2]*Department of Technical Education, Uttar Pradesh, India*
[3]*Institute of Engineering and Technology, Lucknow, India*
***Corresponding Author:** Vikash Yadav; Email: vikas.yadav.cs@gmail.com

ABSTRACT: The field of data management has been reformed by the Cloud computing technologies which offered valuable establishments and amended the storage restrictions barriers for its users. In large enterprises the cloud has been extensively used for implementation due to its benefits. There are still lot of security threats for the data in the cloud. The data owners suffer from its privacy issues which are considered as one of the major concerns. Data privacy can be secured by employing some of the existing methods such as Attribute-based Encryption (ABE). Yet, the security issues are prevailing largely over the cloud. In this research a secured data access control is proposed using the Advanced Encryption Standard (AES) combined with a weighted attribute-based Encryption (AES-WABE). To encrypt the data, the access control policies are used and weight is assigned according to its significance of each attribute. The outsourced data is stored by the cloud service provider and the attribute authority based on the weight that updates the attributes. To minimize the computational overload the data file is accessed by the receiver corresponding to its weight. The proposed procedure provides resistance for collusion, multiple user security with control of fine-grained access based on protection, reliability and efficiency. On concerning the data collaboration and confidentiality, the performance rating is done related with the Cipher-text Policy–Attribute-based Encryption (CP-ABE) and the hybrid attribute-based encryption (HABE) scheme, access control flexibility, limited decryption, full delegation, verification and partial signing.

Keywords: Cloud Security, Access Control, Attribute-Based Encryption, Advanced Standard Encryption, Encryption of Data, Privacy Cloud Computing

ARTICLE INFORMATION
Author(s): Chandrajeet Yadav, Vikash Yadav and Jasvant Kumar
Received: July 22, 2021; **Accepted**: Sep 20, 2021; **Published**: Sep 30, 2021;
e-ISSN: 2347-470X;
Paper Id: IJEER-090305;
Citation: doi.org/10.37391/IJEER.090305
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-9/ijeer-090305.html

1. INTRODUCTION

Enormous amount of data can be handled by the storage of cloud which is considered as a magnificent service having effective techniques. Personal and business data's can be stored using this facility, due to this factor lot of enterprises, establishments and individual users also use it.

The data is uploaded in the cloud by the cloud data provider which is later used by the user, with the help of server of the cloud. The multi-regional, multi-domain and extensive data sharing can be recognized by the cloud storage. The benefits of cloud storage are required resources, on needed storage, economical, maintenance is effortless and managing the storage of the user's [1, 2]. Even though, there are lot of advantages in the cloud storage service, the main issue in it is the security. Different geographically distributed data centers has access to the stored information in the cloud hence, in database of the cloud the data of the user will not be under the user's control. The cloud user faces privacy and data confidentiality problems while using cloud computing [3].

Due to the complications on using this [4, 5], the cloud-based data resources can be accessed only by the authorized users. To deal with this the data before uploading to the cloud infrastructure should be encrypted, but this approach bounds the sharing and further processing of data [6]. Normally, the encrypted data from the cloud storage is downloaded by the data owner in order to re-encrypt them to share the data. Moreover, the cloud users at some cases act themselves as the content providers. The data is broadcasted by them on the cloud servers so as to share and to access those contents the fine-grained data access control is used. [7-10]. In addition, the contents of data should be confidentially retained by the CSP should against the users of the cloud [11].

Encryption is a spontaneous way to safeguard the data [12, 13]. The essential utilizations of data are blocked by the old-style encryption techniques. To obtain the required data a data user decrypts and downloads all cipher texts from the cloud server. Apparently, this approach will be led to computation overhead and unfeasible communication in the cloud computing environment. An inspiration was gained from the author Vipul Goyal et al. [14] who proposed a full-blown key-policy attribute-based encryption scheme (KP-ABE). A wide range of access structures is allowed by this method and achieves a flexible and fine-grained data access control using the attribute-based encryption scheme. In this paper, every data's user key is associated with a specific tree-access

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

configuration assisting the threshold gates. Using the user key, the message can be from the final ciphertext if attributes of cipher text satisfies key's access structure. The Rivest–Shamir–Adleman (RSA) algorithm connected with the digital signature has been examined to the cloud data for purpose of security which approves the digital message. The attribute-based signature (ABS) and group signature is joined to guarantee the consumer anonymity since the attribute authorities are safeguarded by the private key.

In order to remove the constraints and to protect sensitive data the cloud protects the personal data in the cloud silently. Using the fine grained-access control the data encrypted by the owner of data will be deployed to the cloud. At the time of collision, the leakage of information might occur between the user and the cloud, and by using the safety data sheet (SDS) leakage of data can be stopped. And the data is protected from vulnerability by employing the similarity index and to support the query of the neighbor's and the m-index is encrypted. The private key of the signer's is divided into dual types using policy attribute-based signature (KP-ABS) based on the key. Other users cannot access the signature.

In this study, besides the data protection stored in the cloud an Advanced Encryption Standard (AES) is crossed with the algorithm of (AES-WABE) weighted attribute-based encryption. For the purpose of encryption WABE is related with the AES. In AES algorithm Encryption, decryption and Key generation are confirmed.

The contribution of this study is mentioned below:

• A new data collaboration approach is presented in cloud computing in which effective key management is done by a symmetric encryption algorithm which minimizes the computational overhead.
• For the outsourced encryption and decryption, a verification method is provided. The user notices the faulty results returned by the cloud with the support of the verification algorithm. Hence any device can be used by the user to access the data anywhere and anytime. The ABE used in the user side makes the computational cost very low.
• The performance analysis of the proposed scheme demonstrates that it is largely needed and superior in security of data.

The remaining part of the paper is designed in the following way:

After the introduction section, *Section 2* discusses the related works based on secured data privacy and access control methods in the field of cloud computing. *Section 3* briefs about the Hierarchical Attribute-Based Encryption. *Section 4* explains the proposed architecture in depth. The experimental evaluation of our project is described in the *section 5*. In *section 6* the conclusion of the paper and future work is discussed.

2. LITERATURE SURVEY

In the past, several researchers introduced lot of security frameworks by the integration of digital signature, decryption, encryption, secured data storage schemes and access control algorithms confirming secured data communications. Among them, a discretionary and efficient access control model was proposed by Elisa et al. [15] in which the temporal intervals are used for validation. For providing new access the author also designed an automatic rule-based derivation for the next users. While comparing with some of the existing schemes this proposed method was better.

For developing a secure database, the authors Moni and Avishai [16] proposed a novel signature distribution with access control approach using quorum systems. A quorum system is one which has filled-in intersection among each of two sets. The quorum is used by many applications in the distributed system. In this study there are access server which is extremely secured and a compromised data server. The quorum enabled access server performs the operations such as revoking and granting of authorization. The digital signature can be shared among the users in this system due to the confidentiality property of this system. The original ABE scheme is the indefinite model of identity-based encryption (IBE) which was planned by the authors Waters and Sahai [17]. The application of ABE schemes blocked due to the lack of expression and error tolerance is the main goal in IBE.

The key-policy attribute-based encryption (KP-ABE) was proposed by the author Goyal et al. [18] which is considered as a better attribute-based encryption cryptosystem and this system deals with the limitations of the IBE scheme. The author Bethencourt et al. [19] intended encrypting (CP-ABE) cipher text-policy attribute by merging the cipher texts with the access policy. On developing the ABE scheme, a chain of ABE schemes is proposed and such schemes are divided into KP-ABE and CP-ABE schemes. There will be an additive increase in the number of attributes in normal ABE scheme with accordance with the dimension of secret keys and cipher texts. A huge volume of computation, communication and storage are required by these schemes. And the decryption and encryption time is also non negligible.

Therefore, secret keys and constant-size cipher texts along with ABE scheme has been focused and have been proposed. The constant size cipher text was authenticated by some of them (e.g. [20–25]) and the features of constant size secret keys were attained by the other schemes. A sensitive CPABE scheme was presented based on [26, 27] with constant size for both secret keys and cipher texts. In the settings of attribute based cryptographic, the authors Liang et al [28] applied the PRE and generated a re-encryption key by presenting a Ciphertext Policy Attribute Proxy Re-encryption (CP-ABPRE). Author Kawai [29] proposed a malleable CP-ABE proxy re-encoding approach by joining the adaptive CP-ABE together with the method of encryption. Deploying the generated key of re-encryption to cloud server the cost of computation at client side is decreased. To deal with the outsourcing model of re-encoding key generation a first attempt was made in the PRE setting by the authors. The

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

author's in [30] for outsourcing the data presented the L-PRE approach which supports the lightweight access control. The re-encryption task is offloaded by this L-PRE using the proxy. The re-encryption key size based on the assigned expiry period was designed as small. Hence, for every re-encryption the key used for re-encryption has not to be changed compulsorily. The re-encryption cost is minimized by this scheme when compared to other PRE methods. The author Li et al. [31] suggested a framework of novel patient-centric to access the data and to store personal records information.

Each patient personal health record (PHR) files are of encrypted form which achieves scalable and clear data, by ABE techniques the data will be contrasted with respect to the hiring out of data security. By the multiple security domains, the key management complexity is degraded due to the division of PHR system. The break glass and access policies enable the scalability, security and efficiency. A thorough survey was presented by the authors Subashini and Kavitha [32] about the security problems of every models in service delivery models with the pros and limitations in cloud computing.

3. ATTRIBUTE-BASED ON HIERARCHICAL ENCRYPTION

By combining the features of the hierarchical identity-based encryption (HIBE) and the ciphertext-policy-attribute-based encryption (CP-ABE) hierarchical attribute-based encryption (HABE) can be developed. This approach has scalability and supports fine-grained access control moreover yields the entrustment among the attribute authorities. This approach signifies the hierarchical structure of the establishment when compared with other conventional methods, moreover this scheme suits for an outsourcing organization.

CP-ABE: This approach is a reversed form of the KP-ABE scheme which makes the user to clarify the access strategy upon the entire attributes with the intention of the data consumer to decrypt the cipher text. As a result, the data access control and confidentiality can be assured. The steps involved in this process is stated below

(1) *Encrypt (PK, Sa, m)*: This stage outputs a cipher text CT by fetching the inputs PK, the descriptive attribute Sa and a message m.

(2) *Decrypt (CT, SK)*: In this stage the input is CT, which contains the (S)K user's secret key and the access tree (T) merged with Sa, message m is the output. When Sa satisfies T this stage is fulfilled.

(3) *Setup ()*: Only unstated security parameter is approved in this stage. The public key PK and the Master key MK are created at this step.

(4) *Keygen (MK, AS)*: In this step the inputs considered are the non-monotonic access structure AS and MK and provides the output as the attribute secret key SK. The cipher text is combined with CP-ABE's access image until the pack of detailed attributes makes an interpretation for decryption process as shown above. The decryption key and the cipher text is changed with the influence of KP-ABE. Moreover, this system, along with a threshold value provides the monotonic access form for appropriate attributes. The CP-ABE approach is effectual in respect of enforcing the access control of the encrypted data than the approach of KP-ABE. The bounds of CP-ABE are that it fails Figure 1: The Proposed Framework (AES-WABE) to fulfil the efficiency and flexible properties of the provisions in their access control.

HIBE: This approach is the prolongation of IBE. The primitive ID (PID) of public keys is used by a private key generator (PKG) that delivers the private key and referred as 1-HIBE. This approach has heavy key handling which is an imitation of this scheme. A 2-HIBE approach is used to deal with this, it has a root PKG and a domain PKG. The domain PKG generates the domain secret and creates the secret key which is achieved from the root of private key generator. The cryptosystem comprises of authority of a root certificate that allows the certificates of hierarchy. Besides, HABE degrades the support for multi-valued tasks and cannot capably aid the compound attributes. A novel AES-WABE method is presented in this study to deal with this drawback.

4. METHODOLOGY PROPOSED

By the proposed AES-WABE approach a protective and efficient data association is reached. A unique access is used to deal both the secret and public keys by the existing ABE methods. In specific situation the attributes the consumers manage the attributes from multiple authorization of the attributes and the data holders shares the data of the consumers and it is controlled by the different authority. To deal with this problem several attribute-based multi authority access control structures are proposed. To provide secure data, in this study the weighing of attributes is given by the AES. Five basic modules are considered in this system: (a) a cloud server for storing the data (b); the data holder, who uses an access control policy for data encoding and uploads it to the cloud; (c) A weight attribute authority (WAA) based authorization, this validates and updates the users attributes; (d) the Central Authority (CA), grants a global user identifier and consumer public key for every consumers to WAA; and (e) the data users, as shown in *Figure 1*. The weighted attributed authority is combined with the AES which is presented in the *Figure 1*.

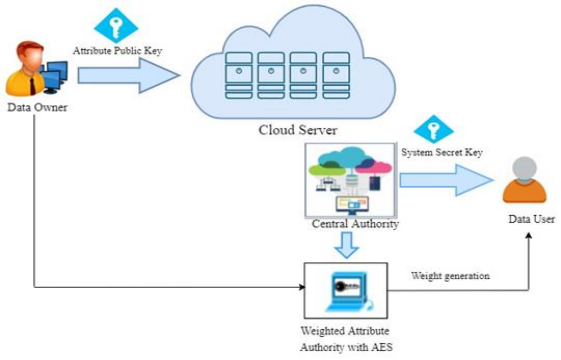

Figure 1: The Proposed Framework (AES-WABE)

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

The AES used in the proposed approach generates the keys randomly by encrypting and decrypting the data. Moreover, for security purposes an image-matching technique is employed. Later, a weight value is generated by the system for the users based on its attributes. This scheme is reliable and secure; while comparing with the conventional methods this approach is suitable for applications in real-time. Proposed encryption considers multi authority security, collusion resistance along with fine-grained access control. Two phases are available in the proposed method and that includes the system phase, algorithm phase. In the phase of algorithm, the system-level operations are defined with the AES algorithm. In conflict, the foremost operations for example, User Annulment, System Setup, admitting New User, Creation of New File, File Access and Deletion are described in the system level.

4.1 DSTATCOM Allocation and Voltage Profile AES Encryption

AES [33] is the alliance of permutation and substitution which is according to the substitution-permutation network and it has high efficiency in the hardware and software. This system does not use a Feistel network unlike its predecessor DES, AES. AES is a form of Rijndael which has a key size of 128, 192, or 256 bits and a fixed block size of 128 bits, and illustrated in *Figure 2*.

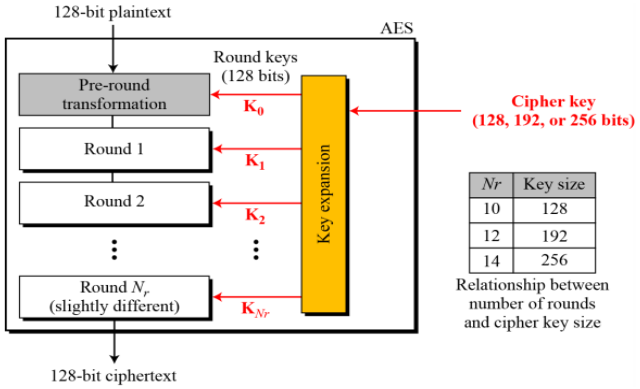

Figure 2: AES Encryption process

For an AES cipher the key size used states the number of replications of transformation rounds that convert the input, i.e. the plaintext, into the final output, i.e. the cipher text. The following are the number of cycles of repetition:

- 14 cycles for 256-bit keys repetition
- 12 cycles for 192-bit keys repetition.
- 10 cycles for 128-bit keys repetition

There are certain processing steps for each round, each has four similar but dissimilar stages.

To transform the cipher text into a plaintext a pair of reverse rounds is implemented using the similar key of encryption. Four types of transformations are used by AES to provide security they are mentioned below.

- *Permutation*: This stage does is a transposition in which each row of the state is shifted to a certain number of steps.
- *Substitution*: In this particular stage based on the lookup table each byte is replaced with another.
- *Mixing*: This stage functions on the state columns, in each column four bytes are combined.
- *Key-Adding*: At this stage, the state unites the partial key an in every round a sub key is obtained from the main key by using the schedule of Rijndael's key; the sub key size is similar to that of the state. On combining the bytes of the state with the sub key it uses the bitwise XOR operator. The AES Encryption/ Decryption algorithm is mentioned below.

Algorithm for Encryption of AES

```
Cipher ((byte out [4*Nb]), (word
W [Nb*(Nr+1)]), (byte in [4*Nb]))
Start
        Byte condition ([ Nb,4])
        condition = in
        AddingRoundKey ((w [0, Nb-1]), condition)
        For round = 1 from step 1 to Nr–1
                (condition) Shift Rows
                (condition) Sub Bytes
                (condition)Mix Columns
                (condition)Adding RoundKey ,
                W (([(round+1)*Nb-1]), (round*Nb))
        End for
        (condition)Shift Rows
        (condition)Sub Bytes
        AddingRoundKey ((w, condition [Nr*Nb),
        (Nr+1)*Nb-1]))
        condition = Out
Quit
```

Algorithm for Decryption of AES

```
InverseCipher ((byte out [4*Nb]), (word
W [Nb*(Nr+1)]),(byte in [4*Nb]))
Start
        Byte condition [ Nb,4]
        In= condition
        AddingRoundKey ((w [Nr*Nb),
        (Nr+1)*Nb-1]))
        For round = Nr-1 step -1 down to 1
                (condition) InverseShiftRows
                 (condition)Adding RoundKey ((W [round*
        Nb), (condition), ((round+1)*Nb-1]))
                (condition)InverseMixColumns
        End for
        InverseShiftRows (condition)
        InverseSubBytes (condition)
        AddingRoundKey ((condition), (w [0, Nb-1]))
        Out = condition
Quit
```

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

4.2. Process in System Level
This process is defined below:

(1) System Setup: The algorithm for global setup is processed by the challenger to attain the global public parameters. A security parameter is chosen by the data holder which yields the secret key SK by giving a request message to the interface of the phase setup of the algorithm.

The Central authority (CA) receives every SK component that is cyphered by the data holder and encrypted module once it is sent.

Despite, the holder's signature is authenticated by the CA. Moreover, if it's correct the CA uses the systems public and master key which provides secret and public keys for a new consumer. The attributes weight is determined by the WAA in the organization domain.

(2) Key Generation: CA allots an uncommon user ID while the system is connected with the new user.

Conversely, the consumer of the attribute set is cyphered and sends it to the WAA. The consumer's signature is authenticated by the attribute authority.

If it is true, WAA creates the weight for the new consumer and the equivalent attribute secret keys. Next, the WAA and CA, separately, transfer the attribute secret key and the consumer's system secret key to the new consumer.

Ongoing with the setup of the central authority and the relating keys algorithm the challenger prevails and issues the hackers public keys.

(3) Encryption: Prior posting the data file by the data holder, for encoding the data an uncommon ID is used to log in and employing for symmetric data file key of encryption. For respective data files and users, the "weighted threshold access structure" (W) is defined by the data holder and the usage of W data is encrypted as shown in *Figure 3*.

This section presents and discusses the simulation results for optimal DSTATCOM position and size, power loss reduction, and enhancement of voltage profile. Cost-benefit analysis and evaluation of the results obtained are also presented.

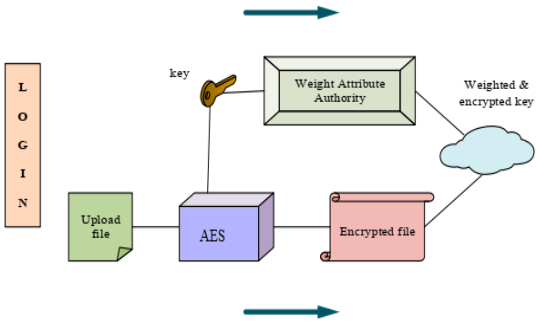

Figure 3: Process of encryption on the owner side data

(4) Decryption: The data is downloaded by the consumer from the cloud, and then decrypted the information using the decryption algorithm. Suppose the attributed secret key of the data consumer is approved, then the system grants different weights as per their level.

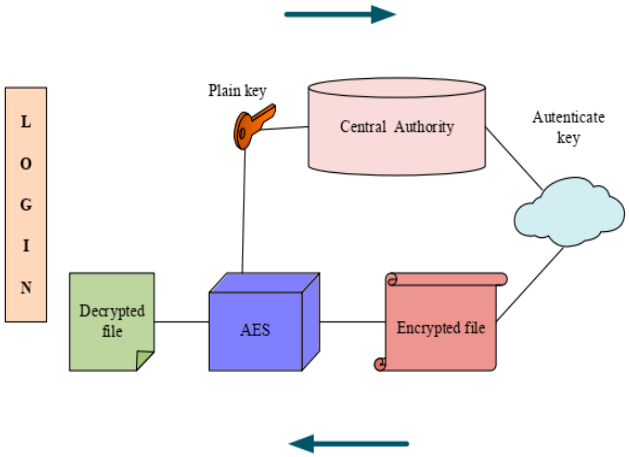

Figure 4: Decryption process of the data user side

Then, with respect to W the user decrypts the respective data file. If the user is invalidated the user fails for data file decryption, as shown in *Figure 4*.

5. RESULTS AND ANALYSIS OF THE EXPERIMENT

The experiment results and analysis for performance evaluation is present in this section. This work is done using the language Java with 8GB RAM (Random access memory) and Intel core i3 processor. The cost of computation is calculated for encryption and decryption. Even though these systems achieve the access control of encrypted data in the cloud network it provides security of data. The existing methods CP-ABE [34] and HABE [35] are compared with the data collaboration schemes of the proposed approach. The proposed approach attains full delegation and partial signing with less workload (WAA and data user) and in a large-scale consumer this achieves the lightweight key management. The AES approach employed in this study encrypts and decrypts many input files of dissimilar sizes (in kB) and also does weight generation and Key generation. Mainly for security function this AES algorithm. This algorithm does the encryption and decryption process with very less execution time. Table 1 illustrates the final results of the approach of proposed system.

Table 1. Experimental outcomes of throughput, encryption/decryption and execution time for AES-WABE

Input data	Size of the File (GB)	Encryption Time	Decryption Time	Throughput
I_1	1	120	115	0.00850
I_2	2	235	226	0.00870
I_3	3	344	600	0.00876

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

Time of Encryption: The time of Encryption is stated as the required time for data encryption. It is used to validate the system speed and to assess the throughput of an encryption approach. The encryption time is the time required to create ciphertext from plaintext. *Figure 5* illustrates the encryption time.

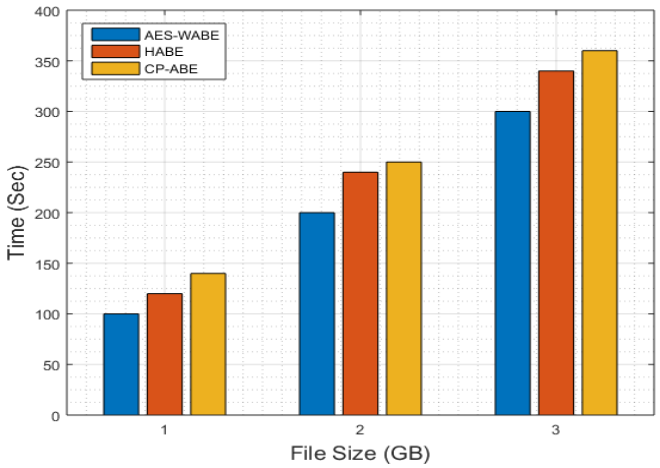

Figure 5: The Encryption time of the proposed compared with the existing

Decryption time: The decryption is the converse process of encryption process. The time taken to yield a plaintext from a cipher text is termed as the decryption time. *Figure 6* illustrates the decryption time of the proposed compared with the conventional methods.

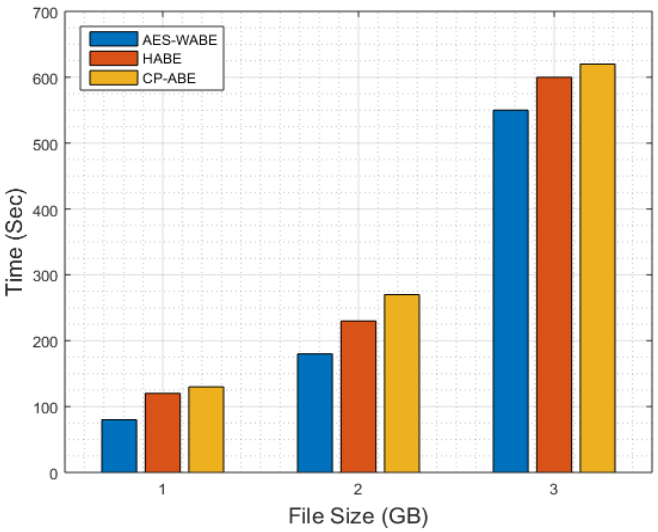

Figure 6: The decryption time of the proposed method compared with the existing methods

Throughput: Throughput is defined as the ratio of the file of data which is encrypted based on the encryption time. The proposed approach achieves high throughput as per the *Figure7*.

$$Throughput = \frac{\text{Size of the file (Kb)}}{\text{Encryption Time}} \quad (1)$$

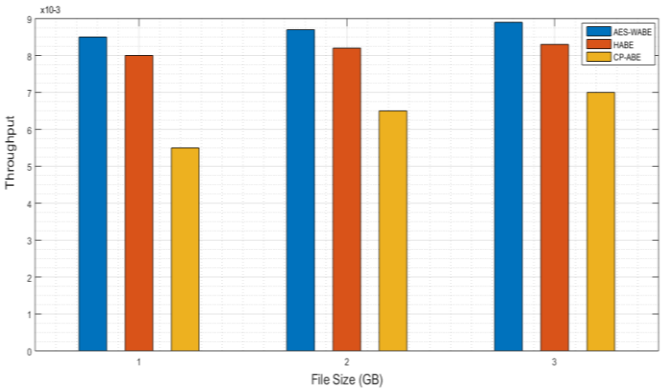

Figure 7: Throughput Comparison of CPABE, HABE and AES-WABE

Secret key analysis Rate: In *Figure 8*, an analysis of the overhead storage and the cost of computation of secret key is done and plotted. The total number of weighted attributes and the storage overhead or time cost is represented in the X and Y axis.

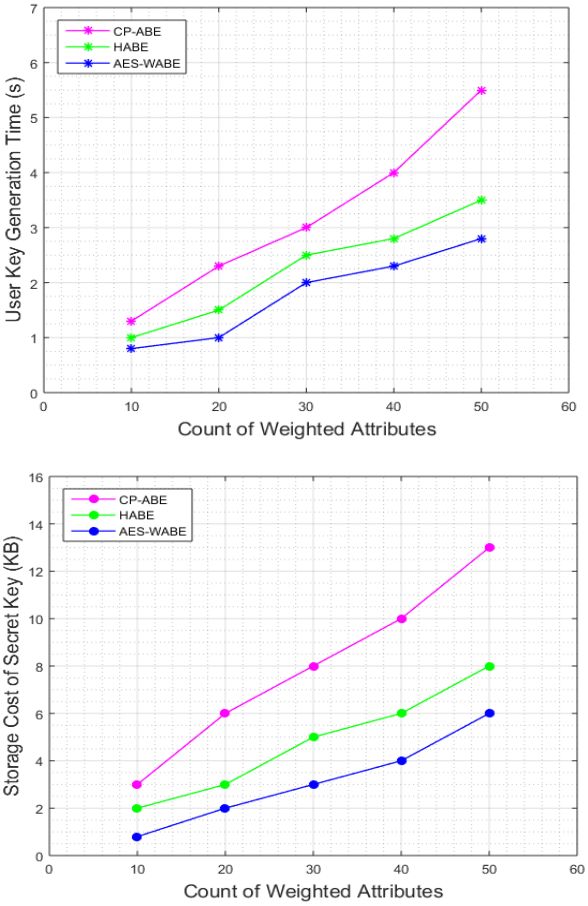

Figure 8: Cost generation of User secret key: 1, and cost analysis of time 2 storage analysis.

Cipher text analysis cost: *Figure 9* illustrates the cost of computation and storage elevation of data encryption. X and Y axis denotes the number of weighted attributes and the time cost or storage overhead of data encryption.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

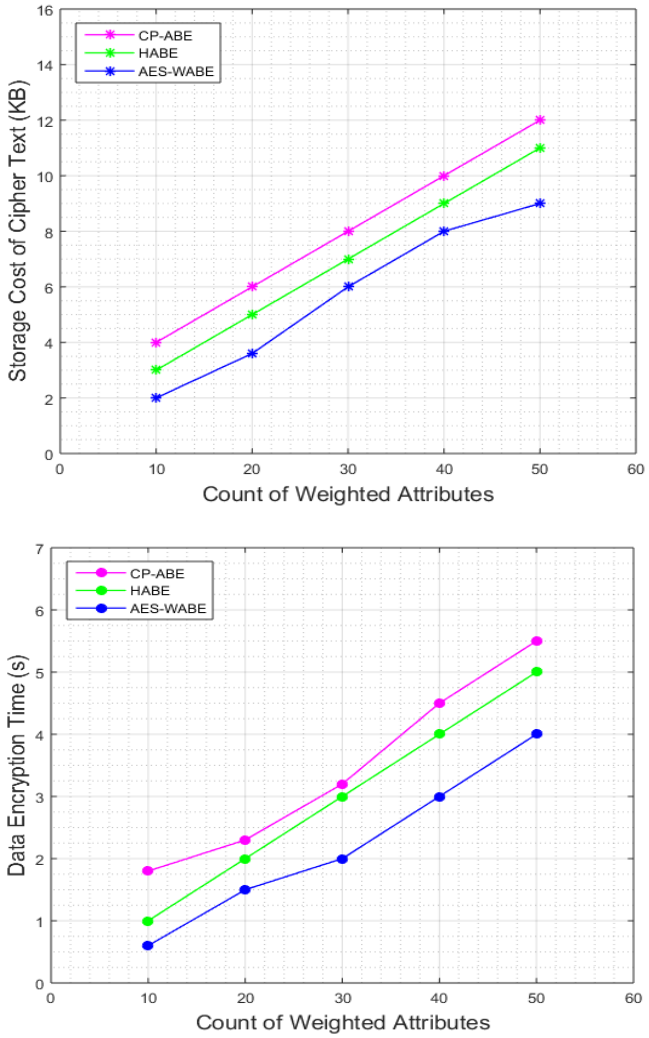

Figure 9: Cipher text cost. (a) Analysis of Storage cost; (b) Analysis of Time cost

5.1. Security Analysis

The proposed AES-WABE technique encrypts shared data. The protective features of the proposed scheme are analysed as follows:

5.1.1 Fine-Grained Access control

This scheme provides flexible differential access policies for individual data. The AES-WABE scheme is used to implement this kind of access control. In the encryption phase of the proposed scheme, a flexible and expressive access policy is enforced by the data owner and to encrypt the data the symmetric key is used. The defined access policy in tree undergoes with the access critical operations, i.e. AND and OR gate, which represents any preferred access conditions.

5.1.2 Data confidentiality

Access policy is used for encryption, which guarantees data confidentiality against the users which fulfil the access policy without maintaining the attributes set. In a ciphertext, the access policy cannot be satisfied by the set of attributes during the decryption phase, the value A = e (h, h)gt cannot be recovered to attain the anticipated value of the global key (GK). Thus, the user decrypts cipher text with reasonable attributes that satisfy the policy of accessing. CK is a random symmetric key which encrypts the data, it is secured by AES-WABE. Since the AES-WABE and the symmetric encryption scheme are secure, the outsourced data's confidentiality is assured against illicit users.

6. CONCLUSION AND FUTURE SUGGESTION

User authentication and Data security in the environment of the cloud are the challenging issues. In this study an access control scheme is proposed which is very efficient and scalable. This study employs an AES Hybridised weight attribute-based encryption mechanism which provides data security. To transmit data securely AES does the encryption and decryption process. When a request is made by the authenticated user, the consumer based on its weight receives the corresponding files in an encrypted format. The generated key with the AES algorithm is used to decrypt the data by the data consumer. The experimental outcomes reveal that the proposed approach is proficient based on efficiency and reliability. In future this work can be extended by providing protection-saving property and quality-based encryption and re-encryption. These are the aspects wherein one can employ miscellaneous methods to achieve information-sharing.

REFERENCES

[1] Zhou, Junwei, Hui Duan, Kaitai Liang, Qiao Yan, Fei Chen, F. Richard Yu, Jieming Wu, and Jianyong Chen. "Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation." The Computer Journal 60, no. 8 (2017): 1210-1222.

[2] Balusamy, Balamurugan, P. Venkata Krishna, GS Tamizh Arasi, and Victor Chang. "A Secured Access Control Technique for Cloud Computing Environment Using Attribute Based Hierarchical Structure and Token Granting System." IJ Network Security 19, no. 4 (2017): 559-572.

[3] Namasudra, Suyel, Pinki Roy, Pandi Vijayakumar, Sivaraman Audithan, and Balamurugan Balusamy. "Time efficient secure DNA based access control model for cloud computing environment." Future Generation Computer Systems 73 (2017): 90-105.

[4] Namasudra, Suyel, Rupak Chakraborty, Abhishek Majumder, and Nageswara Rao Moparthi. "Securing Multimedia by Using DNA-Based Encryption in the Cloud Computing Environment." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 16, no. 3s (2020): 1-19.

[5] Wadhwa, Amit, and Vinod Kumar Gupta. "Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud." International Journal of Applied Engineering Research 12, no. 24 (2017): 15715-15722.

[6] Chandrajeet Yadav, Vikash Yadav et al, "AES-Light Weight CP–ABE Based Privacy Protection Framework with Effective Access Control Mechanism in Cloud Framework", Design

Engineering, Rogers Media Publishing Ltd., ISSN 0011-9342, Vol. 2021, No. 6, pp. 2321-2336, June 2021.

[7] Shen, Rui, and Xuejun Zhu. "The Research on Multi-Authority Based Weighted Attribute Encryption Algorithm in the Cloud Computing Environment." In 4th International Conference on Computer, Mechatronics, Control and Electronic Engineering. Atlantis Press, 2015.

[8] Wang, Shulan, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, and Weixin Xie. "Attribute-based data sharing scheme revisited in cloud computing." IEEE Transactions on Information Forensics and Security 11, no. 8 (2016): 1661-1673.

[9] Zhang, Wenfeng, and Shiqi Jin. "Research and Application of Data Privacy Protection Technology in Cloud Computing Environment Based on Attribute Encryption." In 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), pp. 994-996. IEEE, 2020.

[10] Qian, He, Song Jing, Xu Hong, and Wang Yong. "HABEm: Hierarchical Attribute Based Encryption with Multi-Authority for the Mobile Cloud Service." In 2020 IEEE/CIC International Conference on Communications in China (ICCC), pp. 524-529. IEEE, 2020.

[11] Chaudhry, Shehzad Ashraf, Hosam Alhakami, Abdullah Baz, and Fadi Al-Turjman. "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure." IEEE Access 8 (2020): 101235-101243.

[12] Muthurajkumar, Sannasy, Muthuswamy Vijayalakshmi, and Arputharaj Kannan. "Secured data storage and retrieval algorithm using map reduce techniques and chaining encryption in cloud databases." Wireless Personal Communications 96, no. 4 (2017): 5621-5633.

[13] Alam, Masoom, Naina Emmanuel, Tanveer Khan, Yang Xiang, and Houcine Hassan. "Garbled role-based access control in the cloud." Journal of Ambient Intelligence and Humanized Computing 9, no. 4 (2018): 1153-1166.

[14] Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encryption data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.

[15] Bertino, Elisa, Claudio Bettini, Elena Ferrari, and Pierangela Samarati. "A temporal access control mechanism for database systems." IEEE Transactions on knowledge and data engineering 8, no. 1 (1996): 67-80.

[16] Naor, Moni, and Avishai Wool. "Access control and signatures via quorum secret sharing." IEEE Transactions on Parallel and Distributed Systems 9, no. 9 (1998): 909-922.

[17] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In Annual international conference on the theory and applications of cryptographic techniques, pp. 457-473. Springer, Berlin, Heidelberg, 2005.

[18] Mayur Rahul, Vikash Yadav et al, "A Survey on State-of-the-art of Cloud Computing, its Challenges and Solutions", International Conference on "Recent Trends in Communication & Electronics (ICCE-2020), Ghaziabad, November 28-29, 2020.

[19] Bethencourt J, Sahai A, Waters B (2007) Ciphertext-policy attribute-based encryption. In: IEEE symposium on security and privacy, 2007. SP'07. IEEE, pp 321–334

[20] Chen C, Chen J, Lim HW, Zhang Z, Feng D, Ling S, Wang H (2013) Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In: CT-RSA. Springer, pp 50–67

[21] Doshi N, Jinwala DC (2014) Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption. Secur Commun Netw 7(11):1988–2002.

[22] Emura K, Miyaji A, Nomura A, Omote K, Soshi M (2009) A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: ISPEC, vol 9. Springer, pp 13–23.

[23] Herranz J, Laguillaumie F, Ràfols C (2010) Constant size ciphertexts in threshold attribute-based encryption. Public Key Cryptogr PKC 2010:19–34

[24] Zhang Y, Zheng D, Chen X, Li J, Li H (2014) Computationally efficient ciphertext-policy attributebased encryption with constant-size ciphertexts. In: International conference on provable security. Springer, pp 259–273

[25] Zhou Z, Huang D (2010) On efficient ciphertext-policy attribute based encryption and broadcast encryption. In: Proceedings of the 17th ACM conference on computer and communications security. ACM, pp 753–755

[26] Guo F, Mu Y, Susilo W, Wong DS, Varadharajan V (2014) CP-ABE with constant-size keys for lightweight devices. IEEE Trans Inf Forensics Secur 9(5):763–771

[27] Odelu V, Das AK, Rao YS, Kumari S, Khan MK, Choo KKR (2017) Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. Comput Stand Interfaces 54:3–9

[28] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, ''An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing,'' in Proc. Eur. Symp. Res. Comput. Secur. (EROSICS), Wroclaw, Poland, 2014, pp. 257–272

[29] Y. Kawai, ''Outsourcing the re-encryption key generation: Flexible ciphertext-policy attribute-based proxy re-encryption,'' in Proc. Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), vol. 9065. Cham, Switzerland: Springer, 2015, pp. 301–315

[30] S. Fugkeaw and H. Sato, ''Embedding lightweight proxy re-encryption for efficient attribute revocation in cloud computing,'' J. High Perform. Computer Network, vol. 9, no. 4, pp. 299–309, 2016

[31] Li, Ming, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption." IEEE transactions on parallel and distributed systems 24, no. 1 (2012): 131-143.

[32] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34, no. 1 (2011): 1-11.

[33] Jain, Raj. "Advanced encryption standard (AES)." Washington University in Saint Louis, St. Louis (2017).

[34] Sun, Guo-Zi, D. O. N. G. Yu, and L. I. Yun. "CP-ABE based data access control for cloud storage." Journal on Communications 32, no. 7 (2011): 146.

[35] Huang, Qinlong, Yixian Yang, and Mansuo Shen. "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing." Future Generation Computer

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 9, Issue 3 | Pages 48-56 | e-ISSN: 2347-470X

Systems 72 (2017): 239-249.