OPEN ACCESS
Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

RSA CP-ABE with Access Tree Structure for Secure Revocable Scheme for Building Trust Model

Rajashekar M. B[1*], S. Meenakshi Sundaram[2]

[1,2]Department of Computer Science & Engineering, GSSS Institute of Engineering & Technology for Women, Affiliated to VTU, Belagavi, Karnataka, India

DOI: 10.36348/sjet.2022.v07i04.001 | **Received:** 27.02.2022 | **Accepted:** 02.04.2022 | **Published:** 10.04.2022

***Corresponding author:** Rajashekar M. B
Department of Computer Science & Engineering, GSSS Institute of Engineering & Technology for Women, Affiliated to VTU, Belagavi, Karnataka, India

Abstract

Attribute-Based Encryption (ABE) can provide a technique of fine-grained control. The suggested Enhanced CP-ABE technique includes the use of a proxy to securely communicate the key to users. The Rivest Shamir Adleman (RSA) Algorithm secures outsourced big data in the cloud by allowing public key encryption to safeguard data transported across an unsecured network like the internet. During decryption, the proposed RSA CP-ABE with Access tree structure for Secure Revocable scheme for Building Trust model successfully identifies the users who decrypt the cipher messages. For Third Party auditing, the Dynamic Attribute Tree approach is proposed to encrypt data based on its attribute. The attributes, together with data and keys, are stored in a tree structure, which aids in improving the dynamic update of data in the cloud. Bilinear mapping is used by the Dynamic Attribute Tree approach to validate the integrity of the data without having to retrieve it from the cloud. The experimental results reveal that for a 256-bit key length, the proposed Scheme achieves encryption and decryption times of 1638 ms and 1102 ms, respectively.

Keywords: Attribute-based encryption, Cipher text policy-based attribute encryption, Cloud computing, Rivest Shamir Adleman, Security.

1. INTRODUCTION

Cloud computing is widely used to advance technology and science in a variety of disciplines. Cloud computing estimates a wider scale of complex data and provides internet users with strong tools [1]. Because cloud computing is scaling, a considerable quantity of sensitive and personal data is stored in the cloud, which makes consumers more concerned about the security of their data in the cloud. Low-cost and pay-as-you-go features are among the benefits of cloud storage [2]. Huge amounts of data are being outsourced to the cloud in order to keep corporate and personal data safe. The cloud is publically accessible, untrustworthy, and outsourced data should not be released by the cloud service provider without the data owners' permission [3]. Data privacy and security are critical concerns, and no user wants to transmit papers containing sensitive information that isn't guaranteed to be secure [4]. The cloud's generality will inadvertently jeopardize the secrecy of outsourced data as well as the privacy of cloud users. The issues that arise are allowing unauthorized users access to data that has been outsourced to the cloud at any time and from any location [5]. The solution is to encrypt the data prior to uploading it to the cloud. As a result, the method reduces additional data processing and sharing because data owners must download encrypted data from the cloud and decrypt it before sharing [6]. Attribute-based encryption (ABE) is a type of encryption that combines access control with encryption features. It has piqued the interest of many researchers. The ABE is a sort of public-key encryption that allows for flexible access control over encrypted documents [7]. The ABE technique is used in a variety of applications and is the foundation for establishing "one too many" file sharing and fine graining, whereas older systems only give "one to one" encryption [8].

The size of cipher texts increases linearly in the cipher text policy attribute based encryption (CP-ABE) scheme, as the amount of attributes in the access structure improves the interaction of overheads in the receiver. Furthermore, during the decryption process, the number of pairing operations is proportional to the

number of attributes, increasing the receiver's computing expenses. When it comes to practical implementations of the ABE approach, when bandwidth and processing resources are limited, the limits of practical applications of the ABE approach are particularly important [9]. Access control, trust, and encryption are all used in diverse research methodologies for privacy protection. However, existing cloud security approaches for accessing outsourced huge data are dispersed and non-systematic. As a result, an effective solution for facilitating cloud data privacy security is necessary [10]. To solve such issues, the proposed enhanced CP-ABE with RSA algorithm is implemented, for providing security to outsourced big data in the cloud. The ABE is applied to fine grained control of encryption and enhanced cipher text policy is applied with ABE for privilege control of revocable process. The tree structure is applied to store the tag and encrypted data to provide efficient control in the enhanced CP-ABE with RSA. The tree structure applied in CP-ABE with RSA method helps to improve the efficiency of the encryption, decryption and access control.

2. LITERATURE SURVEY

M. Chase and S.S.M. Chow proposed a distributed KP-ABE strategy for solving the key escrow problem in a multi-authority system in 2009. All (disjoint) attribute authorities participate in the key generation procedure in a dispersed manner in this approach, therefore they can't pool their data and link various attribute sets belonging to the same user. The performance degradation associated with this type of fully distributed system is one downside. Because there is no centralized authority holding master secret information, every attribute authorities in the system should communicate with each other to generate a user's secret key. This adds overhead to the system setup and any rekeying phases, and requires each user to keep additional auxiliary key components in addition to the attributes keys, where N is the number of authorities in the system [2]. In the identity-based literature, S.S.M. Chow presented an anonymous private key generation protocol in 2009, which allows the KGC to issue a private key to an authorized user without knowing the identities of the other users. When we treat an attribute as an identity in this design, it appears that this anonymous private key generation technique works fine in ABE systems. However, it was discovered that this could not be used to ABE systems for two key reasons. First, users' identities are no longer public in Chow's protocol, at least not to the KGC, because the KGC can produce Otherwise, users' secret keys will be exposed. Second, because the most important security flaw in ABE is user participation [3]. In the CP-ABE and KP-ABE contexts, Bettencourt, V. Kumar, and Boldyreva suggested the first key revocation procedures in 2008. These implementations enable attribute key revocation by encrypting the message to the attribute set with its validation time. These attribute-revocable ABE schemes face a security degradation risk in terms of backward and forward secrecy. To revoke the attribute, they use a timed rekeying technique, which is performed by setting expiration duration on each attribute. It is usual in ABE systems for attribute group membership to change often. A new user may then access the data until it is encrypted with the newly updated attribute keys via periodic rekeying, a new user may be able to access the previous data encrypted before his joining (backward secrecy). A revoked user, on the other hand, would still have access.

3. PROPOSED METHODOLOGY

Dynamic auditing is used in this study to improve auditing performance by using the attribute tree encryption method. To effectively handle the data, the attributes are kept in a tree structure together with the data and key. The RSA scheme is used to increase the security of the data.

3.1 Stamp Scheme

A. Preliminary Considerations

1) Location Granularity Levels: We assume that each location has granularity levels, which can be represented the finest location granularity and represents the coarsest location granularity. Location granularity level will be referred to as location level in the following paragraphs. If we know the location we assume that obtaining a higher location level is simple. It is expected that the semantic representation of location levels is consistent throughout the system.

2) Cryptographic Building Blocks: To secure the secrecy of proves, STAMP employs the concept of commitments. This scheme allows you to commit to a message while keeping it secret from the rest of the world, with the option of later revealing the committed value. After a message has been committed, it cannot be modified. A message commitment is represented by, where is a nonce that is used to randomize the commitment so that it cannot be reconstructed by the recipient, and the commitment may be confirmed later when the sender reveals both and. A variety of commitment tactics are available. have been devised and are widely utilized. A specific commitment plan is not required in our system. Any perfect binding and computational concealment approach can be employed. Based on one-way hashing were employed in our implementation. Commitment schemes and one-way hash functions have similar binding and concealing properties.

3.2 Protocol

STP evidence creation and STP claim and verification are the two main parts of our system. When a prover collects STP proofs from his or her co-located mobile devices, we refer to this as a STP proof collection event.

Setup, user key generation, data encryption, data decryption, and revocation are the five steps of the

proposed and upgraded CP-ABE with RSA system. The suggested upgraded CP-ABE with RSA algorithm technique is secure against cloud-based outsourced huge data, as detailed briefly in this section. Data owners, users of data, trusted authority, cloud server, and server proxy are among the five performers in the proposed upgraded CP-ABE technique. Data owner: Before data is uploaded, the data owner is a trusted performer who oversees data encryption and data privacy. According to the stated access policy, the data owner forwards and shares the outsourced information received from users. To identify unauthorized access, data owners specify a threshold access limit for data that is outsourced. Data users: Data users can only retrieve the plaintext from the obtained cipher text if the attributes match the access policies and trusted entities. Authority that can be trusted: The master-secret key (MSK), the user-secret key (US), the public key (PK), and the user identity (UID) number are all created by TA. Before forwarding the secret key, the TA verifies that the data consumers are authentic people and observes the proofs.

Cloud server: CS has a bigger storage capacity, allowing owners to keep information and make it accessible to non-revocable users. The cloud server also manages the server proxy. Proxy server (PS): In a cloud environment, the PS is the entity that is dedicated to an organization. The proxy server will complete the task appropriately and obtain the plain content.

3.2 The RSA algorithm

Input two prime numbers such as e, f and e ≠ f, e, f > 3
Output the components of public key $\{e, N\}$
The components of private key $\{d, M\}$

Procedure

$N \leftarrow$ e × f × (e − 1) × (f − 1) $M \leftarrow$ e × f
The random integers are selected r, e > 2 r < f
Compute private key generation $\emptyset$ value of N $\emptyset(N) \leftarrow$ (e−1)×(f−1)×(e−2 r)×(f−2 r) 2 r
Select a random number e, such that $1 < e < \emptyset(N)$ and gcd $(e, \emptyset(N)) = 1$
Calculates the random number d in such a way that $d * e = 1 * (\emptyset(N))$
The RSA algorithm for encryption
Input
The plain text message, P < The public key component :{e, N}
Output
The cipher text, C Procedure The cipher text,
$C \leftarrow P\ e\ mod\ N$
The RSA algorithm for decryption
Input
The cipher text message, C
The private key components: $\{d, M\}$
Output Decrypted plain text, M
Procedure $P \leftarrow C\ d\ mod$ N

3.3 Attribute Tree Encryption

Parties set P 1,P 2,...,P n make up Attribute Based Encryption (ABE). Monotonic is a set of A2P 1,P 2,...,P n if for B,C it is true that if BA and BC are true, then CA is true. MAS2P 1,P 2,...,P n / are non-empty subsets of P 1,P 2,...,P n of monotonic collection MAS in Monotonic access structure. From the full set 2P 1,P 2,...,P n, two sub-sets are created: allowed sets (belonging to MAS) and non-authorized sets. The MAS is made up of a set of approved attributes that are used to define parties. In this study, monotone access structures are used.

In Attribute-Based Encryption, bilinear mappings are used. G 1 and G 2 are two cyclic multiplicative prime order p groups. The G 1 generator is represented by the letter g. The bilinear map is indicated by the letters e, e:G 1G 2. This is made up of the properties listed below. 1) Have e (ua, vb)=e(u, v)ab for all u,v G 1 and a,bZ p, 2) e(g,g)1. Encryption, Decryption, Key Generation, and Setup are the four algorithms that make up an ABE method for encryption and decryption.

Setup: During the setup step, a prime number p is chosen at random. The trust centre chooses a random number t 1,...,t n,y from the Z q finite field. In this phase, the master key MK=(t 1,...,t n,y) is created.

User qualities are used as input for private key generation, and the algorithm produces the user's private key. A trusted party generates each user's private key. A trusted party chooses a random polynomial q(x), such as q(0)=y. The private key is described in Equation (1).

$$D = \left\{ D_i = g^{\frac{q(i)}{t_i}} \right\}_{\forall_{i \in A_U}} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Master key MK is public key in such equation (2).

$$PK = (T_1 = g^{t_1}, \ldots, T_n = g^{t_n}, Y = e(g,g)^{y}) \ldots\ldots (2)$$

Encryption: Some input values are used in algorithm such as randomly selected number, a set of attributes, public key, and plain-text message. Users with a set of attributes are able to decrypt the data and encrypted message is an output.

Message to encrypt is denoted as $M \in G_2$, a set of attributes are denoted as A_{CT}, and a random number is denoted as $s \in Z_q$. Equation (3) process is applied to encrypt message.

$$CT = (A_{ct}, E = MY^s = e(g,g)^{ys}, \{E_t = g^{t_i s}\}_{\forall_{i \in A_U}}) \ldots.. (3)$$

Decryption: Cipher text, private key, and attributes A_U user set are inputs of the decryption algorithm. If $|A_U \cap A_{CT}| \geq d$, choses d attributes from $i \in A_U \cap A_{CT}$ to process values $e(g,g)^{q(i)s}$, $Y^s = e(g,g)^{q(0)s} = e(g,g)^{ys}$. Decrypted message is $M = E/Y^s$.

Access Trees are constructed for selected access structure based on identified private key. Tree each node is built as threshold gate and attributes are used for leaves.

4. EXPERIMENTAL AND RESULTS

The encryption, decryption, and execution times acquired by the suggested RSA CP-ABE with Access tree structure for Secure Revocable scheme technique, which is employed to provide security against selected plain text and collision attacks of users in the cloud, are summarised in Table 1. It displays the amount of time (in milliseconds) required to complete the task, taking into account the amount of data.

Table 1: The comparison of encryption time with existing methods for different key lengths

Key Length	AES	Collaborative	Hash tree	RSA CP-ABE with Access tree structure
8	27241	0	0	21070
16	19158	483	452	14994
32	9920	495	482	7795
64	4972	526	503	4436
128	2742	545	517	2544
256	1748	1937	1843	1638

Table 1 shows the Encryption time in milliseconds for the proposed RSA CP-ABE with Access tree structure for Secure Revocable scheme method The simulation used is with number of blocks in the X axis and the verification times in the Y axis. For the 100 blocks of data that had been considered is in blocks of 10.T he Encryption time of proposed method has taken 1638ms compared The Encryption times of hash tree and collaborative method methods are 1843 ms and 1937 ms respectively. We observe that in Encryption time performance of the proposed method gives 12.1% efficiency for the hash tree and 18.2% efficiency for hash tree method. The key handling is carried out based on the tree structure and performs the dynamic update to encrypt and decrypt the data.

Table 2: The comparison of decryption time with existing methods for different key length

Key Length	AES	Collaborative	Hash tree	RSA CP-ABE with Access tree structure
8	24747	0	0	20299
16	17873	256	243	14382
32	9042	267	252	7394
64	4593	283	257	3813
128	2265	291	264	2019
256	1175	1275	1375	1102

Table 2 shows the decryption time in milliseconds for the proposed RSA CP-ABE with Access tree structure for Secure Revocable scheme method The simulation used is with number of blocks in the X axis and the verification times in the Y axis. For the 100 blocks of data that had been considered is in blocks of 10.T he decryption time of proposed method has taken 1102ms compared The Decryption times of hash tree and collaborative method methods are 1375 ms and 1275 ms respectively. We observe that in Encryption time performance of the proposed method gives 24.71% efficiency for the hash tree and 15.6% efficiency for Collaborative tree method. The key handling is carried out based on the tree structure and performs the dynamic update to encrypt and decrypt the data.

Table 3: The quantitative analysis of proposed RSA CP-ABE with Access tree structure method in terms of encryption, decryption and execution time

Key Length	Encryption Time	Decryption Time	Execution Time (ms)
8	21070	20299	41977
16	14994	14382	29990
32	7795	7394	15822
64	4436	3813	8856
128	2544	2019	5198
256	1638	1102	3437

Table 3 shows the Execution time in milliseconds for the proposed RSA CP-ABE with Access tree structure for Secure Revocable scheme, The simulation used is with number of blocks in the X axis

and the verification times in the Y axis. For the 100 blocks of data that had been considered is in blocks of 10.The execution time of proposed method has taken 3437ms compared to other existing method. Bilinear mapping in the proposed method helps to protect the data in Third Party Audit and encrypt the data based on attributes. Attributes helps to provide effective update of the tree related to user data.

CONCLUSION

The proposed RSA CP-ABE with Access tree structure for Secure Revocable scheme approach is shown to be more efficient than all other methods in this study. An upgraded CP-ABE using the RSA approach was developed in this research study to guarantee security for outsourced huge data on the cloud. Using the RSA technique, the proposed upgraded CP-ABE effectively identifies the person who decrypts the cipher texts during decryption. Using the setup process, the TA generates PK, MSK, and UID. The secret key is forwarded to the user by the trusted authority and saved in the server proxy. Using the CP-ABE technique, the data owner encrypts the data and sends the cipher text to the cloud environment. The RSA technique is used to decrypt the user's sensitive encrypted data. The encryption and decryption processes took a total of 3437 milliseconds to complete. To test the performance of the proposed and existing methods in the cloud, simulation is used.

REFERENCES

1. Saroiu, S., & Wolman, A. (2009, February). Enabling new mobile applications with location proofs. In *Proceedings of the 10th workshop on Mobile Computing Systems and Applications* (pp. 1-6).
2. Luo, W., & Hengartner, U. (2010, November). Veriplace: a privacy-aware location proof architecture. In *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems* (pp. 23-32).
3. Zhu, Z., & Cao, G. (2019). Towards privacy-preserving and colludingresistance in location proof updating system, *IEEE Trans. Mobile Comput*, 12(1), 51-64.
4. Sastry, N., Shankar, U., & Wagner, D. (2003, September). Secure verification of location claims. In *Proceedings of the 2nd ACM workshop on Wireless security* (pp. 1-10).
5. Hasan, R., & Burns, R. (2011). Where have you been? secure location provenance for mobile devices. *arXiv preprint arXiv:1107.1821*.
6. Davis, B., Chen, H., & Franklin, M. (2012, May). Privacy-preserving alibi systems. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (pp. 34-35).
7. Krontiris, I., Freiling, F. C., & Dimitriou, T. (2010). Location privacy in urban sensing networks: research challenges and directions [security and privacy in emerging wireless networks]. *IEEE Wireless Communications*, *17*(5), 30-35.
8. Desmedt, Y. (1988, March). Major security problems with the 'unforgeable'(Feige)-Fiat-Shamir proofs of identity and how to overcome them. In *Proceedings of SECURICOM* (Vol. 88, pp. 15-17).
9. Bussard, L., & Bagga, W. (2005, May). Distance-bounding proof of knowledge to avoid real-time attacks. In *IFIP international information security conference* (pp. 223-238). Springer, Boston, MA.
10. Sneha, Y. S., Mahadevan, G., & Prakash, M. (2012). A personalized product based recommendation system using web usage mining and semantic web. *International Journal of Computer Theory and Engineering*, *4*(2), 202.