SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I3P103

Volume 11 Issue 3, 24-30, March 2024

Original Article

Security Analysis for a Revocable Multi-Authority ABE-Attribute-Based Mechanism

Addapalli V.N. Krishna[1], P.R. Ancy[2]

[1,2]*Department of CSE, School of Engineering and Technology, CHRIST (Deemed to be University), Karnataka, India.*

[1]*Corresponding Author : adapalli.krishna@christuniversity.in*

Received: 04 January 2024 Revised: 03 February 2024 Accepted: 03 March 2024 Published: 31 March 2024

Abstract *- Due to the tremendous increase in data, groups or even organizations are storing data with third-party providers to solve storage problems. Ciphertext policy attribute based encryption helps to outsource data, which means encrypt the data at the data owner's end and uploading it to third-party storage with some access policy. In normal Identity-based encryption, if a data owner wants to send information to a data user, it will be sent with some identity of the data user, such as mail id, so that only that particular user can read the message. The main problem is that the data owner should know each user's identity. For instance, in some organizations where a data owner wants to send a message to a group of people with an identical designation, it can be sent with the help of the user's attribute using attribute-based encryption. Here, the data owner does not need to know the specific details of each user; instead, with the help of attributes and the provided access policy, they can access this message. This research mainly focuses on three aspects of CP-ABE: access policy, number of attribute authorities, and revocation. When it comes to access policy, the currently existing access policies are not secure due to their linearity in nature because shares are always calculated using the same linear equation. So, for this problem, this work has developed a non-linear SS- secret-sharing model that increases the confidentiality of the model.*

Keywords *- MA-ABE, Elliptic Curve Cryptography (ECC), Access policy, Revocation, Lagrange interpolation.*

1. Introduction

Attribute-based encryption is a type of encryption that supports public vital concepts where encryption and decryption of a message are performed. Here, the main point is that the data owner must know the authentication of each user for communication. ABE was introduced to overcome this issue by sending messages to different groups of entities whose identities are not known. In attribute-based encryption, attributes identify the association between the keys concerned. The decryption of the ciphertext becomes feasible for a user only if a suitable access policy is used [1].

The user encrypts the data using an access policy or access structure. Ciphertext-Policy ABE has some issues. For example, if there is a single authority in a framework, then there is a chance that all attributes are stored by one authority, and if a failure occurs, it affects the entire scheme. In addition to that, another drawback is the key escrow problem [2], which will be described later in this paper. So, it is good to consider a multi-authority system.

Another problem is the revocation problem. Two kinds of revocation are user revocation and attribute revocation. It is again categorized into two kinds of user revocation: backward and forward security. In the context of forward security, individuals whose access has been revoked should be unable to utilize their old secret keys to gain access to new ciphertext. Conversely, regarding backward security, recently joined individuals should be unable to access previously encrypted information using their newly acquired privileges.

Even though ciphertext-policy ABE is a prominent solution for outsourcing data to a third party, it is facing some issues. This research work has done an extensive study on these issues and has come up with a solution that can solve these problems.

The main issues identified are efficient and secure access structure, security issues due to a single authority, and revocation problems. There are several studies on access policy, the number of attribute authorities, and revocation methods [3]. Most of these Cipher text-policy ABE schemes addressed an attribute or user revocation. There were only a few algorithms that discussed both user and attribute revocation.

The work introduces an MA-ABE with a non-linear access policy. This scheme is characterized by its efficiency, scalability, and revocability, supporting forward and backward security measures.

- This paper constructed an RMA-NL Revocable Multi-Authority Attribute-Based Encryption scheme that relies on a non-linear access policy.
- This proposed scheme effectively addresses two primary challenges encountered in an attribute-based encryption system: the key-escrow issue and the most common problem, revocation, by providing an efficient solution.
- Also, a comprehensive analysis of the given scheme was conducted by evaluating its security and performance. The results of our study prove that the presented model resists Chosen Ciphertext Attacks (CCA).

2. Literature Review

Sahai and Waters have proposed a novel approach to secure data encryption known as attribute-based encryption by introducing the concept through a fuzzy-based process [1]. Bethencourt [4] used the idea of attributes, but this method is much like an outdated access policy called Role-Based Access Control. The proposed scheme follows an access structure for accessing the information. The access structure proposed by the author in this paper is a monotonic "access tree". Ali [5] proposed a fully distributed hierarchical ABE that uses an access tree to represent access policies. Here, leaf nodes represent attributes, and the inner node represents threshold value. It provides lightweight computation in the decryption phase.

[6] introduced a system associated with the cost of encryption, cipher text testing and safety. The critical size of the scheme is slightly more significant than the schemes with smaller offline ciphertexts. [7] proposes a fast encryption scheme based on high-dimensional attribute domains for securing messages. The paper addresses concerns related to the reduced security of data, more computational complexity and the high cost of revoking attributes in high-dimensional attribute domains. [8] discussed the importance of secure data sharing in industrial environments. The paper addressed the access revocation in the access policies for securing data sharing in different contexts such as industry.

The paper proposes integrating Attribute-Based Access Control (ABAC) and ABE to address the specific needs of secure data sharing in industrial contexts. As a future scope, the research can focus on developing enhanced implementation strategies for attribute-based encryption that address the difficulty of implementation. Also, it can develop more advanced access control models.

The paper [9] introduces a framework for cloud applications with multi-keyword search capability. As a future work, this work can explore applicability in different domains such as healthcare, finance, and IoT, where secure and privacy-preserving data sharing and high access control are critical requirements. In the paper [10], the authors address challenges related to revocation in attribute-based encryption using a proxy re-encryption mechanism. The main drawback is the scheme uses an additional entity called a proxy server. As future work, it may focus on encryption switching such that both the users cryptosystems become versatile.

[11] introduced the scheme revocable ABE with data integrity protection. The proposed scheme avoids unnecessary operations with ciphertext updates; the data owner need not be online during revocation. [12] proposed revocation method for resource-constrained devices like IoT devices in a cloud-based environment. So even though the removed user gets the ciphertext, it can't be decrypted using the secret key. Updating of the corresponding ciphertext will be done by a third-party server when it receives a revocation signal.

The proposed ABE scheme [15] is modelled to work on high decryption costs and the absence of attribute revocation for altered attributes. The main limitations of this scheme include high decryption costs with complex access policies and the inability to meet policy updating requirements when access control policies change. [17] Presented a novel Data Access (DAC-MACS) scheme incorporating effective and secure data access control measures. The paper showed high-efficiency levels and provided provable security based on the security model. The suggested model [18] for multi-authority attribute-based encryption aims to enhance privacy and security. It does away with the need for a trusted central authority and safeguards users' privacy.

2.1. Preliminaries

- Access Structure
- Linear Secret Sharing Scheme
- Elliptic Curve Cryptography
- Security Assumption

Given the elliptic curve, access policy, Lagrange interpolation and the public parameters PP= (P, a, b, G, n, h), the proposed model is CCA-secure, developed under the DDH model. Security analysis of the system is done by constructing a security model and then proving it based on a CCA security game. It is created under the challenger and advisory model.

3. System Model and Security Model

3.1. System Model

Multi-Authority Attribute-Based Encryption (MA-ABE) system model with Elliptic Curve Cryptography (ECC) involves four distinct entities. The data owner utilizes ECC and an access policy, which can be used to encrypt a given file. The message, user attributes, and user's secret key are points on the given elliptic curve. Ciphertext is then stored on a third-party provider. If the DU wishes to access any file, they must use the secret key obtained from the Attribute Authority (AA). The generation of these shared keys employs Lagrange interpolation. The DU combines each share to create the secret key.

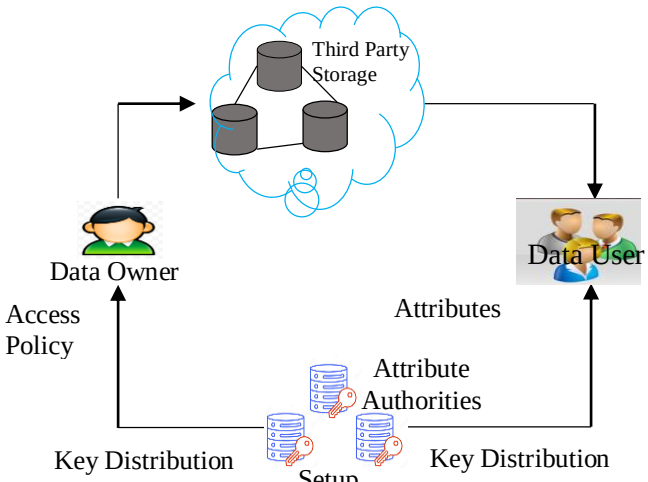

Fig. 1 System architecture

Attribute Authorities (AAs) play a crucial role in the system, responsible for tasks such as storing attributes, generating shares of secret keys, and verifying. Figure 1 shows MA-ABE model constitutes the following five steps.

3.1.1. Setup

$(\lambda, \mathrm{U}) \rightarrow (PK, MSK)$ During the setup phase, the system undergoes initialization by generating public parameters PK *and* MSK. This setup phase is executed independently in each attribute authority.

3.1.2. Encrypt

$(PK, \mathbb{A}, M) \rightarrow CT$ The encryption phase involves taking inputs such PK, M, and $\mathbb{A}$, and generating the corresponding ciphertext CT. Where the access policy is implemented using quadratic residue techniques, the encryption process employs Elliptic Curve Cryptography (ECC).

3.1.3. KeyGen

$(MSK, S) \rightarrow SK$ The process involves taking the MSK, and S as input. Notably, this key generation phase is executed independently at each attribute authority. In this distributed scheme, each attribute authority generates a share of the secret key, which is then transmitted to the user. Upon receiving these shares from various attribute authorities, the user consolidates them to create their complete secret key. This collaborative approach ensures that the user can construct their private key from the distributed shares provided by each attribute authority, contributing to the secure generation of the secret key.

3.1.4. Decrypt

$(PK, CT, SK) \rightarrow M$ The decryption involves the use of PK, CT, that encapsulates an access policy and SK.

3.1.5. Revoke

To enhance scalability, the user receives different secret key shares each time. This variability is achieved by introducing lagrange interpolation, a technique that facilitates the reconstruction of the secret key by combining the various shares received by the user. Ultimately, the decryption operation retrieves the original message from the ciphertext.

3.2. Security Model

Security analysis of the system is done by constructing a security model and then proving it based on a CCA security game.

Security Model

Security of the given scheme is proven based on selective CCA. It is considered the security game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Initialization : Using some corrupted authorities $\cup_{AA'} \subseteq \cup_{AA}$. $\mathcal{A}$ constructs an access structure $\mathbb{AP}^{*}$, which will be challenged and sent to the challenger $\mathcal{C}$.

Setup : By executing the setup algorithm as mentioned $\mathcal{C}$ generates the public parameter PP and sends it to the adversary $\mathcal{A}$.

Query Phase 1 : In this stage, adversary $\mathcal{A}$ make a key query request to the challenger $\mathcal{C}$.

- Decryption Key Query : A secret key query request is made by $\mathcal{A}$ based on uid, which is the identity of DU and $\{S_{uid,\,AA_{id}}\}_{AA_{id} \in U_{AA'}}$, which is the set of an attribute of particular data user stored in that corrupted authority, U_{AA}'. $\mathcal{C}$ executes keygen algorithm and share $\{SK_{uid,\,AA_{id}}\}_{AA_{id} \in U_{AA'}}$ to $\mathcal{A}$. Here, the main point is access structure $\mathbb{AP}^{*}$ cannot be satisfied by only the share. $\{SK_{uid,\,AA_{id}}\}_{AA_{id} \in U_{AA'}}$.
- Decryption Query : $\mathcal{A}$ makes update keys queries based on revoked attributes. $\mathcal{C}$ executes the revoke algorithm and sends a share of the update key $\{UK_{uid,\,AA_{id}}\}_{AA_{id} \in U_{AA'}}$ where $UK = \{S_{uid} - A_{R,uid}\}$ where, $A_{R,uid}$ is the revoked attribute of user id, uid. The UK alone cannot create the given access structure.

Challenge : Adversary $\mathcal{A}$ chooses plaintext messages, m_0' as well as m_1' and send it to the challenger $\mathcal{C}$ along with the access policy $\mathbb{AP}^{*}$. $\mathcal{C}$ flips randomly a bit $\in \{0,1\}$ and generate, m_b' according to $\mathbb{AP}^{*}$ and using the encrypting algorithm, it generates ciphertext ct and returns it to $\mathcal{A}$.

Query Phase 2 : $\mathcal{A}$ repeats Query Phase 1 to get a certain number of secret keys.

Guess : Now Adversary $\mathcal{A}$ will try to make guesses about b. Suppose $\mathcal{A}$ guesses like b'. If b=b', then we can say $\mathcal{A}$ wins the game, and the advantage of $\mathcal{A}$ is:

$$\mathrm{Adv}_{\mathcal{A}} = \Pr[b' = b] = 1/2.$$

Definition 1: It can be said that this scheme is CCA secure if no polynomial time adversary wins the above game with a non-negligible advantage $\mathrm{Adv}_{\mathcal{A}}$.

4. The Proposed RMA-NL Scheme

This paper uses a model named RMA-NL to address two critical challenges in attribute-based encryption: the fundamental escrow problem and the revocation problem. The proposed scheme presents an efficient solution to mitigate key escrow issues [14]. To discuss the critical escrow problem, consider a scenario with a single Attribute Authority (AA) responsible for storing attributes, generating secret keys, and verification.

While this AA is deemed trustworthy, there is a potential concern regarding its curiosity about third-party data. In such a case, AA could independently create the key and try to decrypt it without the knowledge of both the Data Owner (DO) and Data User (DU). This challenge is commonly referred to as the critical escrow problem. To overcome the key escrow issue, the proposed solution involves using multiple Attribute Authority (AA) instead of a single one. In a multi-authority setting [13], each AA stores a subset of attributes related to the user.

Additionally, each AA generates only a part of the secret key and sends this part to the DU. The data user combines all received parts to construct his complete secret key. This approach effectively mitigates the key escrow problem by distributing the key generation process among multiple AAs, ensuring that no single AA possesses the full capability to decrypt files independently.

The architecture of a multi-authority system is outlined below. The ECC algorithm [13] is employed for both encryption and decryption of messages. The chosen elliptic curve must be non-singular, implying the absence of self-intersections.

Another crucial aspect to consider in Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is the efficiency of revocation. Most of the existing approaches typically require updating ciphertexts to accommodate [3, 15-17]. However, the proposed scheme introduces a notable improvement by eliminating the need for ciphertext updating. This enhancement contributes to the efficiency and simplicity of the scheme. Instead, the proposed approach focuses on updating the secret key, leveraging a straightforward process.

The scheme utilizes Lagrange interpolation along with random numbers to generate secret keys, ensuring the generation of unique random keys each time. This research addresses forward revocation and backwards security, designed to prevent new users from accessing previous or old messages upon joining the system. This comprehensive approach enhances the scalability of the proposed scheme. The implementation of revocation in this scheme relies on the concept of Lagrange interpolation, a technique used in secret key generation.

5. Security Analysis

5.1. Security Proof

Theorem 1: The proposed model is CCA-secure, developed under the DDH model.

Proof: We proved the security of our construction via the following parts.

Initialization: Adversary $\mathcal{A}$ defines a set of corrupted authority$\mathrm{U_{AA}}' \subseteq \mathrm{U_{AA}}$ wants to attack and sends the $\mathbb{AP}^*$ to the challenger $\mathcal{C}$.

Setup: $\mathcal{C}$ runs a setup algorithm and returns the PP=(P, a, b, G, n, h) public parameters to $\mathcal{A}$. In addition, $\mathrm{U_{AA}} - \mathrm{U_{AA}}'$ which is uncorrupted authorities, $\mathcal{C}$ randomly chooses $\mathrm{X_{AA_{id}}}, \mathrm{Y_{AA_{id}}} \in \mathrm{Z_q^*}$, as the secret key of $\mathrm{AA_{id}}$ and computes the public keys $\mathrm{X_{AA_{id}}}.\mathrm{P}, \mathrm{Y_{AA_{id}}}.\mathrm{P}$. For each attribute $\mathrm{a_{AA_{id}}} \in \mathrm{U_{AA_{id}}}$, $\mathcal{C}$ chooses a secret key share $\{\mathrm{SK_{uid,\,AA_{id}}}\} \in \mathrm{Z_q^*}$, and returns this to $\mathcal{A}$.

Query Phase 1: Advisary $\mathcal{A}$ sends a query request to the challenger $\mathcal{C}$, $\mathcal{C}$ respond as follows.

- Decryption key query $(\mathrm{U_{id}}, \mathrm{S_{id}})$: Once $\mathcal{C}$ obtains a request on the decryption essential query, $\mathcal{C}$ sends the corresponding decrypt key dk to $\mathcal{A}$. The polynomial $\mathrm{p(x, r)}$ is generated based on the parameters r, pk, s, G, and P. Then the model chooses a random number $\mathrm{r_1}$ calculates the polynomial according to the set of values and sends the polynomial to $\mathcal{A}$.
- Decryption query $(\mathrm{p(x, r,)}, \mathrm{U_{id}}, \mathrm{r}, \mathrm{S_{id}})$: When $\mathcal{C}$ receives the decryption request from $\mathcal{A}$, $\mathcal{C}$ checks the authentication of the user by finding out whether there is a corresponding $\mathrm{U_{id}}$ in the system. Then, solve the polynomial using SK and r, and if it matches, then send the decrypted plaintext m to $\mathcal{A}$. Otherwise, it returns $\emptyset$.

Key-escrow Problem: A secret key is requested by the adversary $\mathrm{U_{AA}}'$ from the framework by sending a query. $\mathcal{C}$ generates part of the secret key with the help of an algorithm $\{\mathrm{SK_{uid,\,AA_{id}}}\}$ with this share of the secret key he cannot decrypt the message.

Backwards and Forward Security: Update key also requested by $\mathcal{A}$ when attribute or user is changed. If $\mathrm{U_{id}}'$ is a user who is revoked or his attributes are changed request for a decryption key, the random number of the polynomial r will change, and when solving the polynomial, S/he cannot able to match it to the secret key and decryption attempt will be failed.

Challenge: The ciphertext selected by the adversary, $\mathcal{A}$ say c_0', c_1' is decrypted based on the flipped coin value. The message selected by the adversary, $\mathcal{A}$ say m_0' and m_1' is sent to $\mathcal{C}$. Challenger $\mathcal{C}$ will flip a coin and encrypt m'. $\mathcal{A}$ now gets the ciphertext $ct' = \{\mathbb{AP}^{*'}, c_0', c_1'\}$. $\mathcal{A}$ randomly selects a secret value s and a random number r.

$$c_0' = \{kG, m_0' + ks_{uid}\}$$

Afterwards, $\mathcal{C}$ gives the ciphertext ct' to $\mathcal{A}$.

$$ct' = \{\mathbb{AP}^{*'}, c_0', c_1', p(x, r)\}$$

$$S=\{0,1\},\ \omega \cong b^2 \text{mod} P,\ r \in z_P$$

$$SUM_\omega = \omega^s r^2$$

Query Phase 2: $\mathcal{A}$ can repeatedly request several decrypt key queries and decryption queries as in query phase 1, but the decrypt key or update essential relevant to an attribute set satisfying the access structure $\mathbb{AP}^*$ cannot be issued by $\mathcal{A}$. Guess Adversary $\mathcal{A}$ sends their guess s' of s to $\mathcal{C}$.

If s' = s, $\mathcal{C}$ outputs 1; otherwise, $\mathcal{C}$ outputs 0. $\mathcal{C}$ outputs 1 means it is the correct ciphertext, and the advantage of $\mathcal{A}$ is ε. Thus,

$$pr[\mathcal{C}(=1)] = \frac{1}{2} + \varepsilon$$

$\mathcal{C}$ outputs 0, which means it is random from $\mathcal{A}$, Therefore,

$$r[\mathcal{C}(=0)] = \frac{1}{2}$$

Hence, $\mathcal{C}$ capable of tackling the DDH problem is:

$$pr[\mathcal{C}(=1)] + pr[\mathcal{C}(=0)] - \frac{1}{2}$$

$$=1/2(1/2+ \varepsilon+1/2)-1/2$$

$$= \varepsilon/2$$

6. Performance Evaluation

The performance analysis of the scheme was done based on a few parameters like key generation time, size of secret key, encryption time, decryption time, and secret key update time. The proposed scheme is implemented in an eclipse framework, using Java as a programming language and the Bouncycastle library for cryptographic algorithms. All results are averaged over ten tests, and the number of attributes is fixed to a maximum of 10. When compared with the existing work, it is found that some of the works are discussed with a single authority that restricts data sharing to one authority and is also resource-intensive. This can lead to a central authority to decrypt every ciphertext. Also, a few schemes have high decryption costs due to complex access structures and the inability to meet policy updating requirements when access policy changes. The proposed model can address all these existing limitations by implementing multiple attribute authority and using Lagrange interpolation for attribute and user revocation.

Figure 2 shows the proposed scheme, which is RMA-NL, compared with some existing work [15, 17, 18]. The graph is plotted based on the time taken to generate a share of the key to the attributes. Figure 3 shows our proposed scheme compared with some existing work [15, 17, 18] based on the size of the secret key. The graph is plotted based on the size of the secret key concerning the number of attributes.

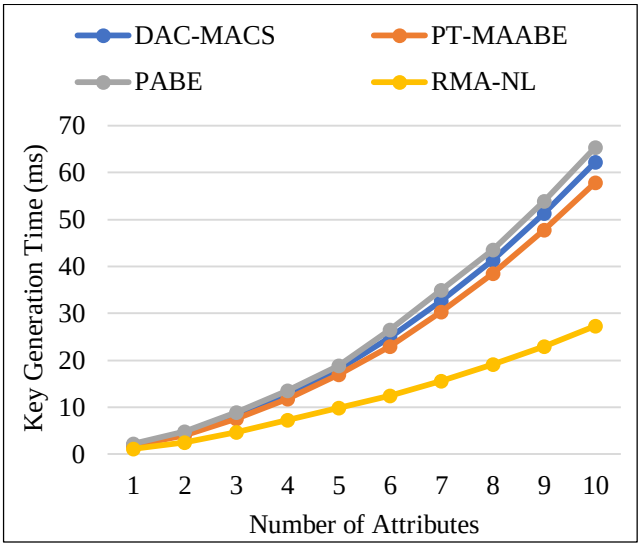

Fig. 2 Key generation time concerning the number of attributes

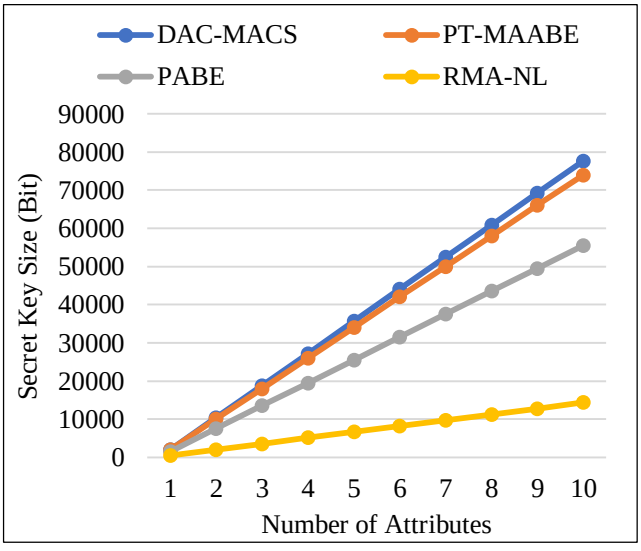

Fig. 3 The size of the secret key to a number of attributes

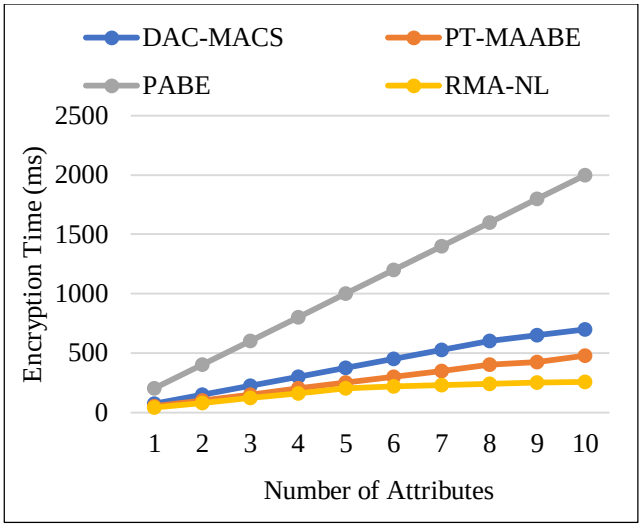

Fig. 4 Encryption time to the number of attributes

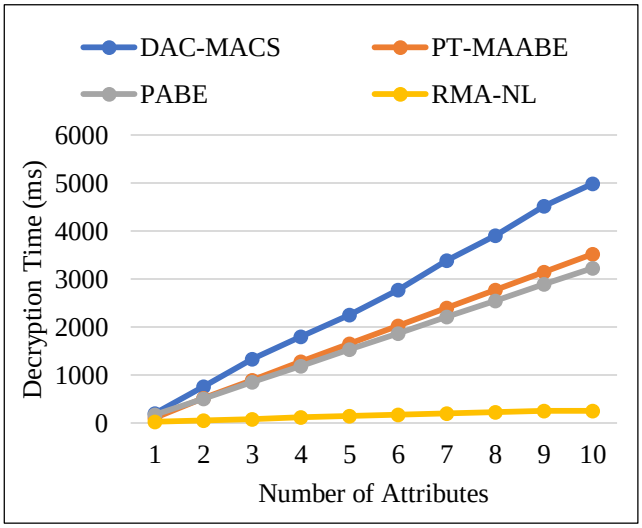

Fig. 5 Decryption time concerning number of attributes

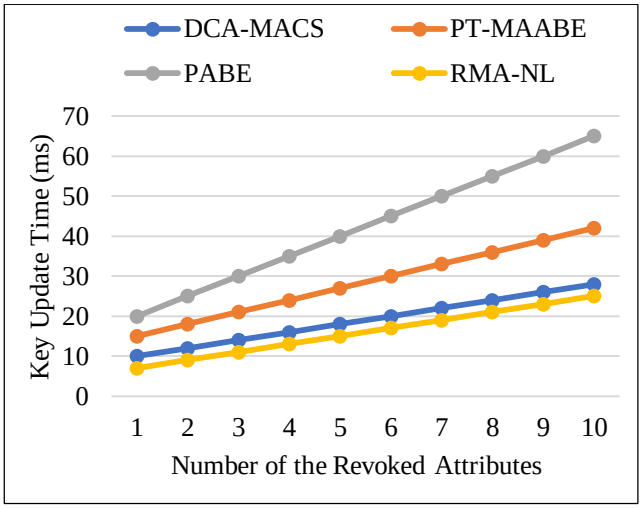

Fig. 6 Time taken to update key concerning the number of revoked attributes

Figure 4 shows the comparison of the proposed scheme with some existing work [15, 17, 18] based on encryption time. The graph shows that the PAABE scheme takes more time than another model as it performs re-encryption.

Figure 5 shows the comparison of the proposed scheme, which is RMA-NL, with some existing work [15, 17, 18] based on decryption time. The graph shows that the DAC-MACS scheme takes more time for decryption as it uses some third-party servers to perform decryption.

Figure 6 Shows the comparison of the proposed scheme, which is RMA-NL, with some existing work [15, 17, 18] based on the time taken for the key update. The graph is plotted based on the key update time concerning the number of revoked attributes.

7. Conclusion

A model has been devised to address various challenges inherent in Attribute-Based Encryption (ABE) systems, including key escrow issues, revocation concerns, and overall security improvements. Besides conventional linear secret sharing, the proposed model incorporates quadratic residue, enhancing the system's overall security. This innovative approach is specifically implemented within a multi-authority system to mitigate key escrow problems effectively.

Furthermore, the model leverages Lagrange interpolation to address the revocation problem and enhance scalability. By employing this technique, the research work successfully resolves revocation issues and ensures the proposed system's scalability. This comprehensive approach aims to provide a robust solution to the identified problems in attribute-based encryption schemes.

It is proven that the proposed scheme is selective CCA secure and has done performance analysis of the model based on parameters like key generation time, size of the secret key, encryption time, decryption time, and secret key update time. It has also compared the proposed scheme with some existing work.

As future work, this work can be extended to IoT environments where resource-constrained devices are used. The non-linear access policy can outsource data in a resource-constrained device. It can apply the Lagrange interpolation polynomial in other encryption techniques like identity-based encryption. It can be used for other applications like keyword search and hierarchy access roles with concepts like lattices, computing, etc.

Acknowledgments

The authors acknowledge the support given by CHRIST University, Bangalore, in taking this work forward.

References

[1] Amit Sahai, and Brent Waters, "Fuzzy Identity-Based Encryption," *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457-473, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[2] Melissa Chase, "Multi-Authority Attribute-Based Encryption," *Theory of Cryptography: 4th Theory of Cryptography Conference*, pp. 515-534, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jianghong Wei, Wenfen Liu, and Xuexian Hu, "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1731-1742, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[4] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-Policy Attribute-Based Encryption," *2007 IEEE Symposium on Security and Privacy (SP'07)*, Berkeley, USA, pp. 321-334, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohammad Ali et al., "A Fully Distributed Hierarchical Attribute-Based Encryption Scheme," *Theoretical Computer Science*, vol. 815, pp. 25-46, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jin Li et al., "Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing," *Computers & Security*, vol. 72, pp. 1-12, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Caimei Wang et al., "A Personal Privacy Data Protection Scheme for Encryption and Revocation of High-Dimensional Attribute Domains," *IEEE Access*, vol. 11, pp. 82989-83003, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Alex Chiquito, Ulf Bodin, and Olov Schelén, "Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts," *IEEE Access*, vol. 11, pp. 10180-10195, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Hua Shen et al., "Multi-Keywords Searchable Attribute-Based Encryption with Verification and Attribute Revocation over Cloud Data," *IEEE Access*, vol. 11, pp. 139715-139727, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Suryakanta Panda et al., "Secure Access Privilege Delegation Using Attribute-Based Encryption," *International Journal of Information Security*, vol. 22, no. 5, pp. 1261-1276, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Chunpeng Ge et al., "Revocable Attribute-Based Encryption with Data Integrity in Clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 2864-2872, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yi Wu et al., "Efficient Access Control with Traceability and User Revocation in IoT," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 31487-31508, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] A. Beimel, and Y. Ishai, "On the Power of Nonlinear Secret-Sharing," *Proceedings 16th Annual IEEE Conference on Computational Complexity*, Chicago, USA, pp. 188-202, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[14] Nishant Doshi, and Reema Patel, "An Improved Approach in CP-ABE with Proxy Re-Encryption," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 2, pp. 1-5, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Zechao Liu et al., "Practical Attribute-Based Encryption: Outsourcing Decryption, Attribute Revocation and Policy Updating," *Journal of Network and Computer Applications*, vol. 108, pp. 112-123, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kamalakanta Sethi, Ankit Pradhan, and Padmalochan Bera, "Practical Traceable Multi-Authority CP-ABE with Outsourcing Decryption and Access Policy Updation," *Journal of Information Security and Applications*, vol. 51, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Kan Yang et al., "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," *2013 Proceedings IEEE INFOCOM*, Turin, Italy, pp. 2895-2903, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[18] Melissa Chase, and Sherman S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp. 121-130, 2009. [CrossRef] [Google Scholar] [Publisher Link]