International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Revocable and Secure Multi-Authority Attribute- Encryption Scheme

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

Submitted: 23/02/2023 **Revised:** 15/04/2023 **Accepted:** 09/05/2023

Abstract: Security is an important factor as nowadays many systems generates and process huge amount of data. This also leads many of us to rely on a third-party service provider for storing sensitive and confidential data. Providing outsourcing means the data owner will encrypt and store the data in a third-party storage system. In this paper, we are proving solutions for two main problems. The first issue is what if the attribute authority itself can access the data because the attributes and secret keys are known by attribute. This issue is called the key escrow problem. For solving it we are proposing a multi-authority system with Elliptic Curve Cryptography. The second issue that we addressed in this paper is the revocation problem, which means when someone leaves the system should be prohibited from accessing subsequent data this is called forward security and as a second case when someone joins the system should be prevented from accessing previous shared date this is called backward security. In this paper, we address both forward and backward security. For solving this problem we are using the concept of the Lagrange interpolation technique for generating and verifying secret keys. Based on this technique secret key will be dynamically altered and used for encryption and due to this can achieve greater security.

Keywords*: Multi-Authority CP-ABE; Access policy; Elliptic curve cryptography; Revocation; Lagrange interpolation.*

1. Introduction

The ABE technique provides security and access control for the data used which are stored third party cloud based systems. In this case, the data owner is mainly concerned about the security of the shared. CP-ABE and KP-ABE are the two types of ABE schems[1]. Most of the research works are based on CP-ABE. For access policy, the existing papers are based on a linear secret sharing scheme or access tree or Boolean algebra but we are using a non-linear secret sharing scheme as access policy. In this paper, we are focussing on the CP-ABE scheme. Attribute authority is the one who issues the secret key and the secret key is generated based on the attributes of the participants. The attributes can be any entity like his department, designation, etc. All the attributes and secret keys are stored in attribute authority. One issue that can arise here is what if the attribute authority is curious about the information stored in it. In that case, he can use the secret key, pretend like the user and retrieve the data. This issue is called the key escrow problem. This problem mainly arises in a single authority system. So for solving this problem we are using a multi-authority system. For solving this problem we are using multiple attribute authority and each attribute authority will contain a subset of attributes and develop a shared key and send it to the participants[3]. The user receives all the shares from different attribute authorities and combines them to form his secret key. Another issue is revocation problem in ABE [4]. Revocation is used when a person is leaving the system or when a person is newly joined. In this paper, we are addressing both backward and forward security. Forward security is used when a person leaves the system he can't access the new messages and backward security is used when a new person joined the system he can't access the previous message. We are using a new design for the multiauthority system which uses Lagrange interpolation for generating secret keys and uses elliptic curve cryptography for a cryptographic function. This makes our system secure and scalable and also improves security and address revocation problem efficiently.

A. Proposed Model

In this work a multi-authority CP-ABE based model is proposed, which uses nonlinear access policy. This is an efficient scalable and revocable scheme that supports both forward and backward security.

1. In our paper, we introduce a multi-authority CP-ABE with scalable and revocable mechanism. This scheme can solve key-escrow problem.

2. In this model the cryptographic operations are done using elliptic curve cryptography and generating a secret key using Lagrange interpolation.

3. We explained how we can solve the revocation problem in a simple method by using Lagrange interpolation. The paper also discussed both forward and backward security.

1Professor,
CSE Dept, School of Engineering and Technology,
CHRIST (Deemed to be University), Bangalore
adapalli.krishna@christuniversity.in
2Research Scholar,
CSE Dept, School of Engineering and Technology,
CHRIST (Deemed to be University)
ancy.prasadam@res.christuniversity.in

B. Contents

In section II delts with some definitions and related work. Section III delt with a system model which support multi-authority CP-ABE and how we can solve key escrow problems using it. We also describe the working of elliptic curve cryptography and Lagrange interpolation in a multi-authority ABE scheme. In section IV we have described how the revocation problem is solved with the help of Lagrange interpolation.

2. Related Works

Sahai and Waters have introduced a new scheme for encrypting data called attribute-based encryption[5]. They introduced this concept by considering fuzzy based process. A scheme based on CP-ABE and proxy re-encryption[6] is proposed. It can trace policy changes by policy versioning technique. This scheme is based on lightweight policy updates in the multi-authority environment. For addressing the challenges of resource-constraint devices and attribute revocation[7], this paper proposes efficient RMA-ABE based on elliptic curve cryptography. To enable attribute revocation, a key is added to the values of the user. To reduce the burden of authority center introduced hierarchical ABE schemes[8]. This scheme can be used to access multiple files at the same level of security. A dishonest authority center may obtain all of the decryption keys and unlock the data. Incorporate the polynomial interpolation in an elliptic curve cryptosystem[9].It describes how to use the elliptic curve cryptosystem for encoding the message in point form. A secure e-healthcare system using IBE and signature is proposed [10]. Only people with permission to view the shared data can do so using a unique public identity (ID) [11]. The size of the share represents the complexity of the scheme.

Both revocations that is user revocation and attribute revocation[12] are addressed. The proposed scheme is based on ciphertext updating. Binary tree and Revocation list. To support revocation [13], introduced the concept of group keys. The main focus is on devices having limited resources. The security concepts that can be implemented for revocation are explained in [14]. The data owner is not required to perform unnecessary decryption and re-encryption processes. The main focus is on resource-constrained devices [15]. The technique eliminates the need for the user to routinely update the key and instead relies on the cloud based server.

3. System Model

The system model of MA-ABE with ECC comprises of four unique values: Data Owner (DO), Data User (DU), Third-Party Service Provider(SP), and Attribute Authority (AAs). The DO uses ECC and access policy to encrypt the file. The message, attributes, and secret key will be considered as a point in an elliptic curve. The resulting ciphertext can be stored in any third-party service provider. When DU wants to access a file he will send the request to AAs and get one shared key from every AA. For generating a shared key we are using Lagrange Interpolation. He combine each share and generated the secret key. He can read the file only if the attributes in the secret key and access policy are matched. AAs are responsible for storing attributes, generating share of secret key verification, etc. Fig. 1 represents the system architecture of our scheme.

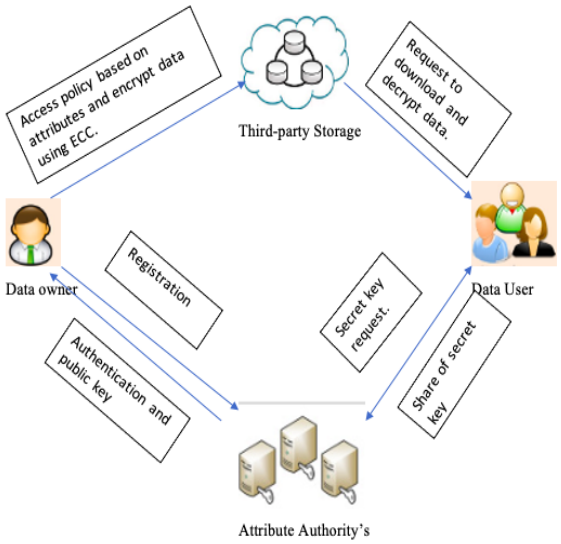

Fig. 1. System Architecture.

In general MA-ABE consist of four phases:

Setup $(\lambda,U)\rightarrow(PK,MSK)$ In this phase with the help of security value λ and set of attributes as U we are generating public values PK and a master secret key MSK. This will initialize the system and as we have multiple attribute authority this phase will execute in all attribute authority.

Encrypt $(PK,A,M)\rightarrow CT$ It considers input as public values PK, a plain text M, also an access mechanism A it encrypt the message. As the access policy we are using non-linear secret sharing scheme with quadratic residue[16]. Output is the respective ciphertext CT and for encryption we are using ECC.

KeyGen $(MSK,S)\rightarrow SK$ In this model private key is generated by considering master secret key and a group of user values S. This phase is executed at each attribute authority. Thus, at each level a share of the secret key will be generated and send to the users. At the user end he collect all the share combine it and generate his secret key.

Decrypt $(PK,CT,SK)\rightarrow M$ With public value PK, a ciphertext CT, which associates and access mechanism and private secret key it decrypt the ciphertext and generate original message. The user will get different secret key share each time for the purpose of scalability and this is done by introducing Lagrange interpolation.

4. Multi-Authority CP_ABE Scheme Using ECC and Lagrange Interpolation

A. Design of a Multi-authority system

Our MA-ABE is an efficient technique for solving key escrow problems[17]. First, we will discuss the key escrow problem. Suppose we are using only one attribute for storing attributes, generating the secret key, and verification even though we say AA is a trusted system but sometimes it can be curious about the data stored in third-party storage. In this case, the AA itself can generate a key based on the attribute and can decrypt the file without knowing DO and DU. This issue is called the key escrow problem. To solve this issue, instead of one AA we are using multiple AAs. In the case of multi-authority[18], [19] AA each AA will store a subset of attributes about the user. And for generating a secret key each AA will generate only a share of the secret key based on the attribute it stores and send it to DU. The DU will combine all the shares of a secret key and generate his secret key. In this way, we can solve the key escrow problem.

The design of a multi-authority system is going to be discussed. For encryption and decryption of messages we are using the ECC algorithm[20]. The curve should be non-singular, which means no self-intersections. And the condition for selecting a & b is such that:

$(4a^3+27b^2)\bmod p \neq 0 \bmod p$

Select a suitable curve & point G, where G is the base point. Every participants identifies a private value as key $k_A<p$ and evaluates the public available key $P_A=k_AG$. Then the plaintext can be encoded as corresponding points on the elliptic curve P_m. For encryption and decryption, we have the equation:

Encryption: $C_m= \{kG, P_m + kP_B\}$

Decryption: $P_m+kP_B-k_B(kG) = P_m+k(k_BG)-k_B(kG)=P_m$

Table 1 gives the attributes and global parameters of each user. Each attribute is a set of some common information like department, designation, etc. The graph of Fig. 2 and 3 give the relation of attributes and global parameters for attribute authority and user. With this diagram, it will be easy for us to relate the relation between them.

Table 1. Attributes and global parameters of each user.

User	*1*	*2*	*3*	---------	*n*	*GP 1*	*GP 2*
Attributes	*A 1*	*A 1*	*A 1*	---------	*A 1*	*g*	*p*

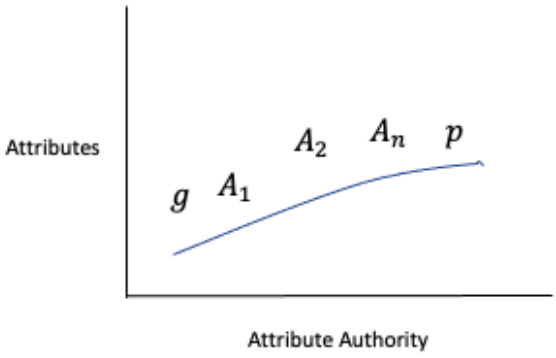

Fig 2: Relationship between attributes and global parameters

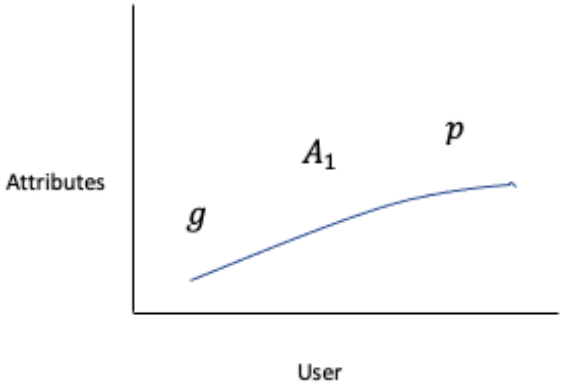

Fig 3: Relationship between attributes and global parameters of each user.

As we are using ECC for encryption and decryption we can write the equation for encryption as two terms $(M + rP_B)$, Gr.

Below we are given the design of the multiauthority system for elliptic curve cryptography.

In this let $C_1= M +rP_B$ and $C_2= Gr$. For decryption, we can say$C_1- C_2 k_B= M$.

Where,$P_B=k_B.G$

M=message + Access policy

Here, our access policy is based on a non-linear secret sharing scheme [21] based on quadratic residue [16].

$C_2=G.r$

C_2*k_B *polynomial of user = MK* P_B of user

G.r* k_B *polynomial of user

For generating the secret key, we are using the concept of Lagrange interpolation with the help of a random number. Below we have given a brief idea about Lagrange interpolation.

For each user, there is a polynomial that is generated by Lagrange interpolation.

The polynomial is given by

$P_k(x)=\sum^{k}_{i=0} L_i(x) f(x_i)$

B. Example

An elliptic curve E: $y^2=x^3+9x+17$ defined over a prime field, F_{23}.

Points in this elliptic curve are: (1,2) (1,21) (3,5) (3,18) (4,5) (4,18) (5,7) (5,16) (7,3) (7,20) (8,7) (8,16) (10,7) (10,16) (12,6) (12,17) (13,10) (13,13) (14,9) (14,14) (15,10) (15,13) (16,5) (16,18) (17,0) (18,10) (18,13) (19,3) (19,20) (20,3) (20,20) ∞

The base point is G = (1,2) and r=5.

Alice chooses, k_A =5 and compute her public key, k_A G = (16,18).

Encryption steps:

Alice wishes to send the message "M" to Bob.

So, he embeds the message in point: (16,18).

Bob chooses k_B =7 and computes k_B G = (13,10)

Encryption

$(M + rP_B)$, Gr

Let $(M + rP_B) = C_1$

$Gr=C_2$

$C_1= (M + rP_B)$

= (16,18) +5. (13,10)

= (16,18) + (8,16)

= (12,6)

C_2= Gr

=5. (1,2)

= (16,18)

Encryption= (12,6), (16,18)

Decryption

$C_1- C_2 k_B$

= (12,6)-7. (16,18)

= (12,6) - (8,16)

= (12,6) + (8, -16)

= (12,6) + (8,7)

= (16,18), which is the message.

REVOCATION USING LAGRANGE INTERPOLATION

Another important issue that has to address in CP-ABE is revocation efficiency. According to the existing works, ciphertext has to update to accommodate revocation[22]–[24]. But according to our scheme ciphertext updating is not required. This makes our scheme efficient and simple. Instead, we will update the secret key this is a simple process as we are using Lagrange interpolation with the random number for generating the secret key and every time it will generate some random key. In our scheme, we are addressing both forward and backward revocation. Forward security means that any user who leaves the system cannot be able to access the plain text of subsequent data exchange whereas backward security ensures those who join the system should not be able to access previous or old messages. This will improve the scalability of our scheme. For implementing revocation in our scheme we are using just using the concept of Lagrange interpolation that is used for generating the secret keys.

First, we will generate a polynomial based on the receiver's attribute, global parameters, and some random number. So, we are generating polynomials using the components such as public key, attribute, G, P, and some random number. As an example, we are assuming some values for each parameter.

Let us assume the public key of Bob is (13,10) and the value of the attribute is (4,5). The base point or generator is (1,2). P is 23 let it be (7,3) and let the random number be (5,7). Consider the boundary values are (1,2) and (13,10) which means we are keeping (1,2) as the lower boundary and (13,10) as the upper boundary, so the random number that we are selecting should be in between this range.

Example:

We are using the same elliptic curve which we have discussed in the previous example. Elliptic curve points in between upper and lower boundaries are

(1,2) (1,21) (3,5) (3,18) (4,5) (4,18) (5,7) (5,16) (7,3) (7,20) (8,7) (8,16) (10,7) (10,16) (12,6) (12,17) (13,10)

So, we can take these points as random values.

For generating polynomials, we are using

Basepoint G, attribute, P, random number, public key

First, we are taking (5,7) as the random number

(1,2) (4,5) (7,3) (5,7) (13,10)

$=0.038x^4-0.91x^3+6.651x^2-16.377x + 12.598$

For getting 7, x values are:

x=0.40, x=5.01, x=5.62

Now changing the random values

(1,2) (4,5) (7,3) (3,18) (13,10)

$=-0.164x^4+4.141x^3-32.747x^2+91.717x -60.95$

For getting 7, x values are:

x=1.143, x=3.85, x=7.2

(1,2) (4,5) (7,3) (5,16) (13,10)

$=0.178x^4-4.425x^3+34.07x^2-91.6114x + 63.785$

For getting 7, x values are:

x=0.871, x=4.157, x=6.7

(1,2) (4,5) (7,3) (8,7) (13,10)

$= -0.033x^4+0.871x^3-7.242x^2+21.74x -13.336$

For getting 7, x values are:

x=1.78, x=3.269, x=7.83

(1,2) (4,5) (7,3) (8,16) (13,10)

$= -0.097x^4+2.478x^3-19.777x^2+56.132x -36.735$

For getting 7, x values are:

x=1.242, x=3.767, x=7.24

From this, we identified that we can map polynomials to private keys.

The main advantage of using this system is its strength that is possible attack can be done between AA and the user, according to our scheme AAs are sending different values (random values) at each time this is simple logic with sufficient security.

5. Results and Discussion

In this paper, we have discussed how to solve two issues in attribute-based encryption the key escrow problem and the revocation problem. The key escrow problem is usually seen in a single authority system so for solving this issue we are developing a system with multiple attribute authority. And for this system, each attribute authority will store some subset of values of the participants. By this mechanism a new value will be generated which can be considered as a secret key to be shared to the user. On the user side, he will combine all these shares and generate his secret key. For solving revocation, we are using the technique of Lagrange interpolation. With this technique, each time user will get a different secret key and so the revocation problem will be solved. An example of this and how it will work is already explained in the above section.

Table 2 shows functionality comparison with some existing work.

Schemes	**Authority**	**Revocation level**	**Forward Security**	**Backward Security**
[12]	Multiple	User	Yes	yes
[15]	Multiple	Attribute	No	No
[19]	Multiple	Attribute	No	No
[20]	Single	User	No	Yes
Ours	Multiple	User, Attribute	Yes	Yes

We have done security and performance analysis of the model. A random oracle is used to model the system, and the security of the model is evaluated by considering Key escrow problem, Backward security and Forward security.

Theorem 1: With the assumption that our non-linear multi-authority CP-ABE scheme is considerably secure against any attacks by challenge it in the random oracle model.

Proof: Here we are given security analysis of the model by considering key escrow problem, backward and forward security issues.

Key escrow problem: In our model, every user has a unique id. This id will help Attribute Authority to independently develop a secret key by considering the attributes of the user. That is there is no need that AAs have to cooperate with each other to generate the secret key share.

Forward Security: By providing the revocation functionality, our construction guarantees the backward security. Only a correct decryption key, which is obtained by considering the share of secret key and by proper updating it by Lagrange interpolation can be used for decryption purpose. In a circumstance where a participant is moved out of the system by revocation algorithm the updated key is useless for him/her, since it will generate a different polynomial. Therefore, the user will not get permission to decrypt message.

Backward Security: This mechanism can be addressed by our model using updated key. When a user is added into U

the random key will generate with different parameters. Using this key, he can decrypt only the message after this time period and those previously generated ciphertext cannot be decrypted.

In the performance analysis number of values of the attributes are used to evaluate encryption and decryption time. Fig 4 shows the average time of encryption and decryption algorithm by considering the number of attributes as input to the given model. Fig 5 shows average time of encryption by considering the size of the file. And Fig 6 shows average time of decryption algorithm based on the file size.

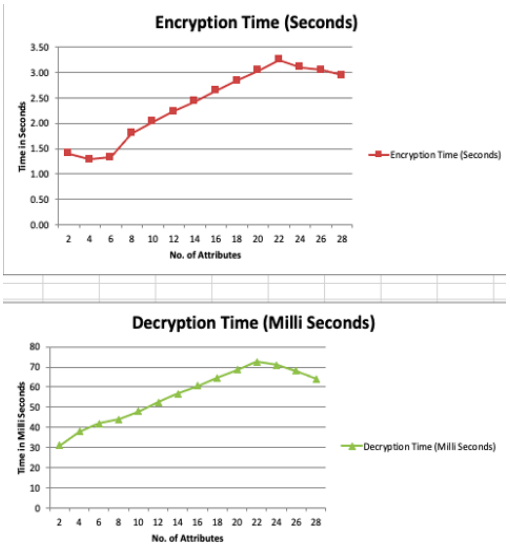

Fig 4: Average time for encryption and decryption - number of attributes.

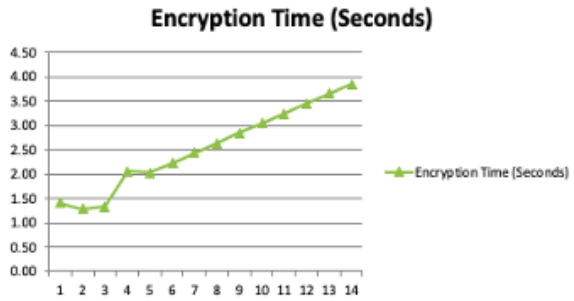

Fig 5: Average time of encryption algorithm based on the file size.

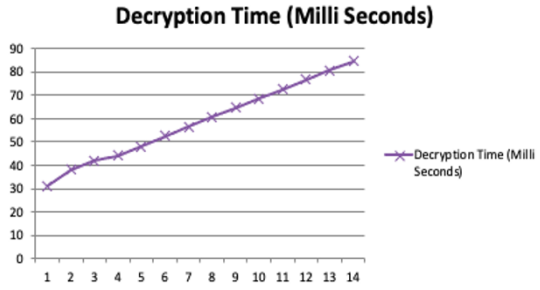

Fig 6: Average time of decryption algorithm based on the file size.

6. Conclusions

In this work, we suggest a model in identifying some of the problems that exist in attribute-based encryption systems such as key escrow problems, revocation, and security. Instead of linear secret sharing, we are using a non-linear secret sharing mechanism with quadratic residue this will help to improve security. Instead of a single authority system, we developed a multi-authority system for solving key escrow problems. And by using Lagrange interpolation we solved the revocation problem and addressed scalability. As future work, we can extend this work in IoT environment for improving the efficiency of the system.

References

[1] J. Bethencourt, A. S. Ucla, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption."

[2] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization."

[3] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption."

[4] Z. Liu, J. Xu, Y. Liu, and B. Wang, "Updatable Ciphertext-Policy Attribute-Based Encryption Scheme with Traceability and Revocability," IEEE Access, vol. 7, pp. 66832–66844, 2019, doi: 10.1109/ACCESS.2019.2918434.

[5] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," pp. 457–473, 2005.

[6] S. Fugkeaw, "A Lightweight Policy Update Scheme for Outsourced Personal Health Records Sharing," IEEE Access, vol. 9, pp. 54862–54871, 2021, doi: 10.1109/ACCESS.2021.3071150.

[7] Y. Ming, B. He, and C. Wang, "Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage," IEEE Access, vol. 9, pp. 42593–42603, 2021, doi: 10.1109/ACCESS.2021.3066212.

[8] J. Li, N. Chen, and Y. Zhang, "Extended file hierarchy access control scheme with attribute-based encryption in cloud computing," IEEE Trans Emerg Top Comput, vol. 9, no. 2, pp. 983–993, Apr. 2021, doi: 10.1109/TETC.2019.2904637.

[9] L. K. Jie and H. Kamarulhaili, "Polynomial interpolation in the elliptic curve cryptosystem," J Math Stat, vol. 7, no. 4, pp. 326–331, Jan. 2011, doi: 10.3844/jmssp.2011.326.331.

[10] K. Sudhamani, P. Rama Rao, & R. Vara Prasad. (2016). Secure Auditing and Deduplicating Data in Cloud. International Journal of Computer Engineering In Research Trends, 3(1), 1-5.

[11] B. Applebaum and O. Nir, "Upslices, Downslices, and Secret-Sharing with Complexity of 1.5 n," 2021.

[12] J. Wei, W. Liu and X. Hu, "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage," in IEEE Systems Journal, vol. 12, no. 2, pp. 1731-1742, June 2018.

[13] D. Han, N. Pan, and K. C. Li, "A Traceable and Revocable Ciphertext-Policy Attribute-based Encryption Scheme Based on Privacy Protection," IEEE Trans Dependable Secure Comput, vol. 19, no. 1, pp. 316–327, 2022, doi: 10.1109/TDSC.2020.2977646.

[14] S. Tu, M. Waqas, F. Huang, G. Abbas, and Z. H. Abbas, "A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing," Computer Networks, vol. 195, Aug. 2021, doi: 10.1016/j.comnet.2021.108196.

[15] Budhhe, A., & Hajare, H. R. (2016). Secure Data Communication Using IDEA for Decentralized Disruption-Tolerant Military Networks. International Journal of Computer Engineering in Research Trends, 3(12), 625-628.

[16] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "Revocable Attribute-Based Encryption with Data Integrity in Clouds," IEEE Trans Dependable Secure Comput, 2021, doi: 10.1109/TDSC.2021.3065999.

[17] Maloth, Bhavsingh, K. Pavan Kumar, G. Nirusha, and C. Vijaya Mohan. "Discrete Keyword Search in Cloud Computing over Attribute Based Encryption." International Journal of Computer Science Engineering & Technology 2, no. 3 (2012).

[18] A. P. R and A. v N Krishna, "An Efficient Nonlinear Access Policy Based On Quadratic Residue For Ciphertext Policy Attribute Based Encryption," J Theor Appl Inf Technol, vol. 15, no. 21, 2021, [Online]. Available: www.jatit.org

[19] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, Jul. 2014.

[20] D, B. S. and P, V. K. (2023) "Digital Railway Ticketing Using Ethereum and Smart contracts", International Journal of Computer Engineering in Research Trends, 10(4), pp. 167–171. doi: 10.22362/ijcertpublications.v10i4.10.

[21] J. Gu, J. Shen, and B. Wang, "A robust and secure multi-authority access control system for cloud storage," Peer Peer Netw Appl, vol. 14, no. 3, pp. 1488–1499, May 2021, doi: 10.1007/s12083-020-01055-5.

[22] P. S. Challagidad and M. N. Birje, "Efficient Multi-authority Access Control using Attribute-based Encryption in Cloud Storage," in Procedia Computer Science, 2020, vol. 167, pp. 840–849. doi: 10.1016/j.procs.2020.03.423.

[23] L. Zhang, Y. Ye, and Y. Mu, "Multiauthority Access Control with Anonymous Authentication for Personal Health Record," IEEE Internet Things J, vol. 8, no. 1, pp. 156–167, Jan. 2021, doi: 10.1109/JIOT.2020.3000775.

[24] G. K. Sandhia and S. V. K. Raja, "Secure sharing of data in cloud using MA-CPABE with elliptic curve cryptography," J Ambient Intell Humaniz Comput, vol. 13, no. 8, pp. 3893–3902, Aug. 2022, doi: 10.1007/s12652-021-03287-6.

[25] A. Beimel and Y. Ishai, "On the power of nonlinear secret-sharing," SIAM J Discret Math, vol. 19, no. 1, pp. 258–280, 2005, doi: 10.1137/S0895480102412868.

[26] K. Lee, "Revocable hierarchical identity-based encryption with adaptive security," Theor Comput Sci, vol. 880, pp. 37–68, Aug. 2021, doi: 10.1016/j.tcs.2021.05.034.

[27] K. Dhal, S. C. Rai, P. K. Pattnaik, and S. Tripathy, "CEMAR: a fine grained access control with revocation mechanism for centralized multi-authority cloud storage," Journal of Supercomputing, vol. 78, no. 1, pp. 987–1009, Jan. 2022, doi: 10.1007/s11227-021-03908-z.

[28] C. Wang, H. Jin, R. Wei, and K. Zhou, "Revocable, dynamic and decentralized data access control in cloud storage," Journal of Supercomputing, vol. 78, no. 7, pp. 10063–10087, May 2022, doi: 10.1007/s11227-021-04277-3.