International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5471
***Article Received**: 10 March 2021 **Revised**: 18 March 2021 **Accepted**: 02 April 2021 **Publication**: 31 May 2021*

An Innovative Approach for Enhancing Cloud Data Security using Attribute based Encryption and ECC

Souad Hafidi
RO.AL&I Team,
PHD student, Faculty of Sciences and Technics, Errachidia, Moulay Ismaïl University, Morocco.

Fatima Amounas
RO.AL&I Team, Computer Sciences Department, Faculty of Sciences and Technics, Errachidia, Moulay Ismaïl University, Morocco.

Lahcen El Bermi
GL-ISI Group, Computer Sciences Department, Faculty of Sciences and Technics, Errachidia, Moulay Ismaïl University, Morocco.

Moha Hajar
RO.AL&I Team, Mathematical Department, Faculty of Sciences and Technics, Errachidia, Moulay Ismaïl University, Morocco.

***Abstract*—**Cloud computing is future for upcoming generations. Nowadays various companies are looking to use Cloud computing services, as it may benefit them in terms of price, reliability and unlimited storage capacity. Providing security and privacy protection for the cloud data is one of the most difficult task in recent days. One of the measures which customers can take care of is to encrypt their data before it is stored on the cloud. Recently, the attribute-based encryption (ABE) is a popular solution to achieve secure data transmission and storage in the cloud computing. In this paper, an efficient hybrid approach using attribute-based encryption scheme and ECC is proposed to enhance the security and privacy issues in cloud. Here, the proposed scheme is based on Cipher text-Policy Attribute Based Encryption (CP-ABE) without bilinear pairing operations. In this approach, the computation-intensive bilinear pairing operation is replaced by the scalar multiplication on elliptic curves. Experimental results show that the proposed scheme has good cryptographic properties, and high security level which depends in the difficulty to solve the discrete logarithm problem on elliptic curves (ECDLP).

***Keywords**: Hybrid approach, Attribute-based encryption, ciphertext-policy, Elliptic Curve, Data Security, cloud computing.*

I. INTRODUCTION

With the enormous growth in cloud computing services, data and network security are important issues in cloud computing environment. The information technology model for computing is composed of the components like hardware, software, networking and services (Figure 1). Hence, it is necessary to enable the development and delivery of cloud services via the Internet. There are users in the cloud. Cloud Provider and Cloud User are the prominent actors in Cloud Computing. Cloud Provider provides cloud services. Hence, security, confidentiality and visibility with respect to the cloud providers is much essential. As the cloud computing resources and services are open for public use and communication is performed over the Internet, data security risks and challenges are raised under untrusted cloud environments. The main aspect is to protect the data from hacking. Security in cloud computing is an evolving area in today's world. Confidentiality, integrity and availability are the greatest concerns with regards to security in cloud computing [1]. Recently, the attribute-based encryption is one of the emerging solutions to achieve secure data transmission and storage in the cloud. The attribute-based encryption (ABE) techniques are preferred in cloud-based secure data storage. To provide efficient access control and protection to user information, different kind of ABE encryption techniques are used in cloud environment. But, the security strength of the ABE depends on the number of attributes, key values or roles are involved in an encryption process. There are two categories of ABE techniques called key-policy attribute-based encryption (KP-ABE), and cipher text policy attribute-based encryption (CP-ABE).

- The KP-ABE is an encryption scheme based on the key strategy. Here, the cipher text is associated with an attribute set and the secret key is associated with an access policy. The cipher text can be decrypted with the secret key if and only if the attribute set of cipher text satisfies the access policy of secret key.
- The CP-ABE is an attribute encryption scheme based on the cipher text strategy. Here, the cipher text is associated with an access policy and the secret key is associated with an attribute set. The cipher text can be decrypted with the secret key if and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.
***Article Received**: 10 March 2021 **Revised**: 18 March 2021 **Accepted**: 02 April 2021 **Publication**: 31 May 2021*

only if the attributes of the secret key satisfies the cipher text access policy.

In the literature, most of the existing CP-ABE schemes use the bilinear maps and also produce the large size secret keys and cipher texts [2, 3, 4]. The bilinear map loses the high efficiency over ECC because of the requirement of the security parameters of larger size. Therefore, designing an expressive access structure CP-ABE using ECC is an emerging research problem in this area [5, 6]. In the present paper, our research will focus on CP-ABE such as an efficient attribute-based encryption scheme using ECC for enhancing the security in cloud. Here, we attempt to develop a hybrid encryption scheme which combine the most commonly used symmetric-key algorithm AES with the CP-ABE based ECC for cloud security enhancement.

The rest of the paper is organized as follows. We briefly review some basic notions connected with elliptic curve cryptography and the attribute-based encryption in section 2. Section 3 is devoted to the description of the proposed approach. Section 4 presents the experimental result and comparison with other existing schemes. Finally, section 5 ends with conclusion.

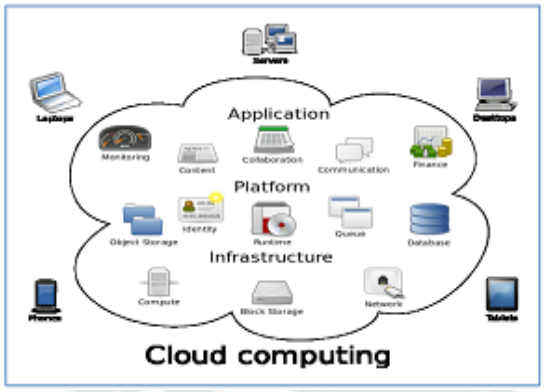

Figure 1. General framework for Cloud Computing.

II. BACKGROUD INFORMATION

In this section, we give a brief review on some cryptographic background and attribute based encryption technology. Next, we give all preliminaries and definitions associated with ciphertext-policy attribute-based encryption.

A. Cryptography

Cryptography is one of the broad areas for researchers today. Encryption is most effective way to achieve data security. Generally, there are two types of algorithms, symmetric-key algorithms and asymmetric-key algorithms. Cryptographic system entails the study of mathematical techniques of encryption and decryption to solve security problems in communication. Public-key cryptography usually uses complex mathematical computations to scramble the message. There are some popular public-key encryption algorithms, for example, RSA, ElGamal. The security of the most public-key encryption algorithms is based on discrete logarithms in finite groups or integer factorization [7]. Recently, the bit length for secure RSA use has increased and this has put a heavier processing load on applications using RSA. Then, a competing system that has emerged is elliptic curve cryptosystem (ECC)[8] and have been attracting increased attention of many authors, because they have opened a wealth possibilities in terms of security.

1) Elliptic Curve Cryptography

Elliptic Curve Cryptography(ECC) was introduced by Victor Miller and Neil Koblitz [9] as an alternative to other established public key cryptosystem such as RSA, Elgamal Cryptosystems, etc. The mathematical background of ECC is more complex and thus it provides greater security and more efficient performance than other first generation public key cryptosystems. With elliptic curves one of the main advantage is that the similar level of security can be achieved with considerably shorter keys than in methods based on the difficulties of solving discrete logarithms over integers or integer factorizations.

a) Mathematical operation

An elliptic curve over a finite field is defined by the following equation:

$$E: x^3+ax+b=0 \bmod p \qquad (1)$$

By substituting different values for x and y in equation (1), the ECC points are generated. The set of all elliptic curve points is denoted by $E_p(a, b)$ and defined as:

$$E_p(a, b)=\{(x,y): y^2=x^3+ax+b \bmod p\}$$

together with the point at infinity. The point at infinity denoted by 'Ω' is the additive identity for the abelian group. All the entities in the elliptic curve cryptosystem agree upon a, b, p, G, n which are called Domain parameters ofECC.

The dominant operation in ECC cryptographic schemes is scalar point multiplication. It can be done by a series of doubling and addition operations of a point on EC. The mathematical operation using in the elliptic curve cryptography are described in [10].

b) Elliptic Curve Discrete Logarithm Problem

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP). Let P and Q be two points on an elliptic curve such that $\alpha P = Q$, where α is a scalar. Given P and Q, it is computationally infeasible to obtain α, if α is sufficiently large. α is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is point multiplication. i.e. multiplication of a scalar α with any point P on the curve to obtain another point Q on the curve.

B. Attribute-based encryption (ABE)

Attribute-Based Encryption (ABE) is a public key encryption scheme that allows users to encrypt and decrypt messages based on user attributes. In ABE system, a user's identity is composed of a set of strings which serve as descriptive attributes of the user. Messages are encrypted under a set of attributes describing the intended receivers, and the secret or private key of these users is also associated with the attributes set for encryption. Attribute-based encryption schemes allow any user to decrypt cipher-text as long as it has the attributes satisfying a threshold policy. This feature makes ABE a very popular solution to provide data security. The performance of the ABE is high compared to other encryption methods. Thus

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.
***Article Received**: 10 March 2021 **Revised**: 18 March 2021 **Accepted**: 02 April 2021 **Publication**: 31 May 2021*

attribute based encryption is the solution to all cloud applications.

In recent years, Attribute-based encryption provides good solutions to the problem of anonymous access control by specifying access policies among private keys or cipher texts over encrypted data. The first ABE scheme introduced by A. Sahai and al.[11] only supports threshold access control strategies. Subsequently, V. Goyal and al. proposed two different and complementary schemes [12,13] called key-policy ABE and cipher text-policy ABE to support more flexible access control strategies. Since then, a number of novel ABE schemes have been proposed with different properties [14,15,16] for supporting flexible and fine-grained access control of sensitive data. Moreover, specialized ABE schemes have been proposed and applied in various domains [17-23].

C. Preliminaries of CP-ABE

a) Definition

The attribute and access policy are defined as follows:

Let the attribute universe U = {A_1, A_2, …, A_n} be the set of n attributes A_1, A_2, … , A_n.

An attribute set of a user is denoted by $A \subseteq U$ and presented with an n-bit string ($a_1a_2 \dots a_n$) defined as follows:

$$\begin{cases} a_i = 1, \text{ if } A_i \in A \\ a_i = 0, \text{ if } A_i \notin A. \end{cases}$$

We define an access policy by P specified with attributes in U and represented with an nbit string ($b_1b_2 \dots b_n$), where:

$$\begin{cases} b_i = 1, \text{ if } A_i \in P \\ b_i = 0, \text{ if } A_i \notin P. \end{cases}$$

b) Ciphertext-policy attribute-based encryption scheme

A cipher text-policy attribute-based encryption scheme is composed of four algorithms, which are summarized as a generic system model in Figure 2.

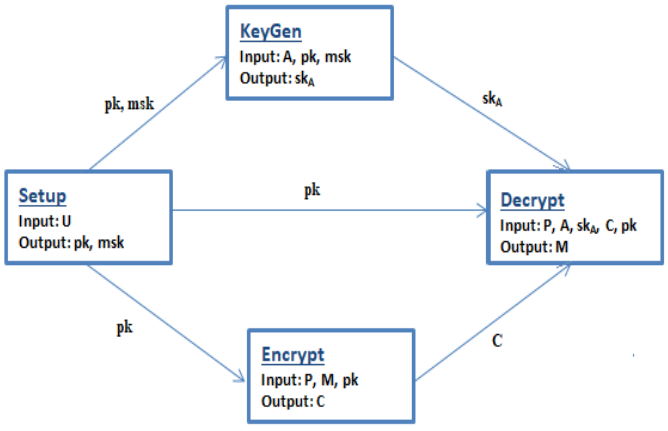

Figure 2. A Generic system model of CP-ABE.

- *Setup:* this algorithm is provided with a security parameter λ and the universe of attributes U = {A1, A2, …, An} as inputs, and it produces a public key pk and its corresponding master secret key msk.

- *Encrypt:* It takes an access policy P, the public key pk and a plaintext M as inputs. The encryption algorithm E(P, M) then outputs a cipher text C.

- *KeyGen:* Taking as input an attribute set A, public parameters pk and the master secret key msk. The key generation algorithm outputs the decryption key of A, which is denoted by sk_A.

- *Decrypt:* Taking as input a cipher text C generated with access policy P, public parameters pk and the decryption key sk_A corresponding to the attribute set A. The decryption algorithm Dec(C, P, sk_A, A) outputs the message M or an error.

III. PROPOSED METHODOLOGY

In this section, our proposed scheme is presented. The proposed hybrid encryption scheme has advantages of both AES and CP-ABE based ECC computing. In encryption, AES is more suitable. CP-ABE based ECC is considered to be more expensive. So, the plaintext is first encrypted symmetrically using AES algorithm. Then, the secure key is again encrypted asymmetrically with CP-ABE algorithm based ECC according to the access policies over a set of attributes that specifies with them the owner is able to share her/his data. Figure 4 and Figure 5 show encryption and decryption of data using both AES and CP-ABE based ECC respectively.

Our proposed hybrid encryption scheme includes of 4 entities as shown in Figure 3: Data Owner, Cloud storage server, Attribute Authority and Data User.

- *Data Owner:* it can define access control policy over attributes in the system and under which encrypt the data before outsourcing it to the cloud. Only the user, with enough attributes satisfying the access policy, can decrypt the ciphertexts.

- *Cloud storage Server*: it is responsible for storing the data and responding to user queries.

- *Attribute Authority:* it is in charge of issuing and revoking users' attributes according to their identities in the system. The secret key of each attribute is generated by it and the corresponding public key is published to all of the users in the system.

- *Data User*: it tries to access data stored in the data storage server. Each user possesses a set of attributes to decrypt the authorized cipher text using his decryption key.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.
***Article Received**: 10 March 2021 **Revised**: 18 March 2021 **Accepted**: 02 April 2021 **Publication**: 31 May 2021*

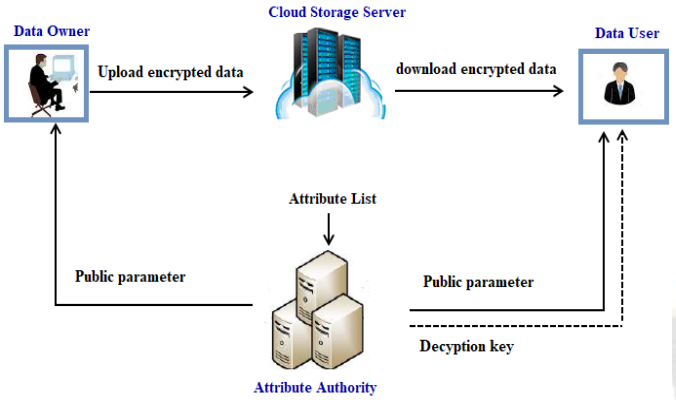

Figure 3. Hybrid cloud security model.

Here, the proposed approach adopts ECC to perform the cryptographic operations. The proposed hybrid encryption scheme consists of three algorithms as follows:

a) Generation key

1. Generates the elliptic curve parameters (p; a; b;G).
2. For each attribute Atti∈U, chooses a number $a_i \in Fp$ and computes Ai $=a_iG$ as its public key, where U denotes the attribute space.
3. publishes the public parameters pp= {p, a, b, G, A_{att1}, A_{att2}, …, A_{attn}} and secretly keeps the privacy parameter sp= {a_{att1} ; … ; a_{attn}}

a) Encryption process

The encryption process works as follows:

1. Input the plaintext as a text file and store it as a secret data into the encryption algorithm.
2. Generate a random session key.
3. Encrypt the message using AES encryption algorithm. The results cipher text is C1.
4. Imbed the symmetric key as a point on the elliptic curve E. Then, encrypt the result key using CP-ABE with an attribute policy based ECC to give cipher text C2.
5. C1 concatenated with C2 represents the ciphertext C. Then the encrypted data is stored on the cloud server.

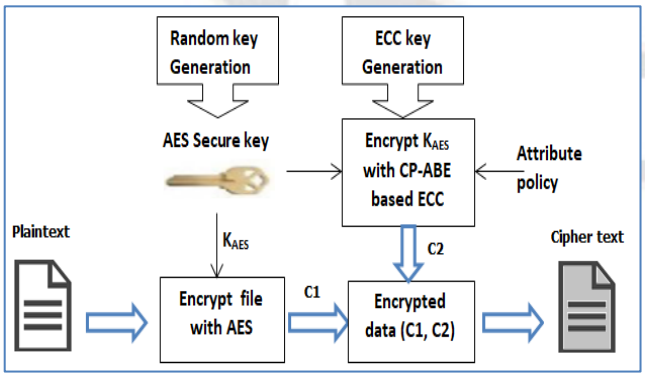

Figure 4. Encryption process.

b) Decryption process

To recover the plain text from the cipher text, the Data user will first determine which of his attributes satisfy the policy. Then after reception of the cipher text C, the user should do following steps:

1. Get the cipher text C= (C1, C2) from the cloud storage server.
2. Decrypt C2 using his private attribute set A and ECC private key. On successful decryption, the code points are recovered.
3. Reverse the embedding to get the secure key.
4. Apply AES decryption process to get back the original data.

Thus, the Data User obtains the original plaintext sent by the Data Owner securely.

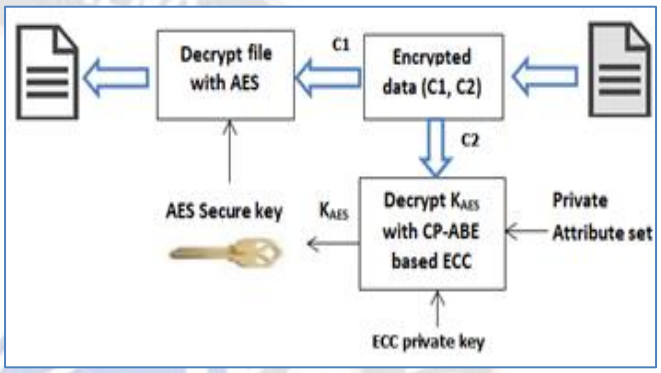

Figure 5. Decryption process.

IV. PERFORMANCE ANALYSIS

In this section, we present the performance analysis of the proposed hybrid encryption scheme. Here, we carried out experiments to measure the time required for encryption and decryption process. We compared our scheme with the existing methods: ABE and the model proposed by Jaichandran et al. [24]. The authors in [24] propose a hybrid architecture invoking attribute based encryption (ABE) for encrypting the key and advanced encryption standard (AES) for file encryption. Table 1 provides the execution time required for encryption and decryption of a message of size 1KB using different number of attributes.

TABLE 1. EXECUTION TIME FOR ENCRYPTION AND DECRYPTION USING DIFFERENT NUMBER OF ATTRIBUTES

	Encryption (sec)			**Decryption (sec)**		
Number of attributes	***5***	***10***	***20***	***5***	***10***	***20***
ABE	0.038	0.052	0.063	0.018	0.034	0.047
Ref. [24]	0.031	0.044	0.052	0,015	0.029	0.042
Proposed scheme	0.026	0.038	0.044	0.011	0.022	0.032

Figure 6 and Figure 7 show the execution time of the encryption and decryption, respectively, over various numbers of attributes.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.
***Article Received**: 10 March 2021 **Revised**: 18 March 2021 **Accepted**: 02 April 2021 **Publication**: 31 May 2021*

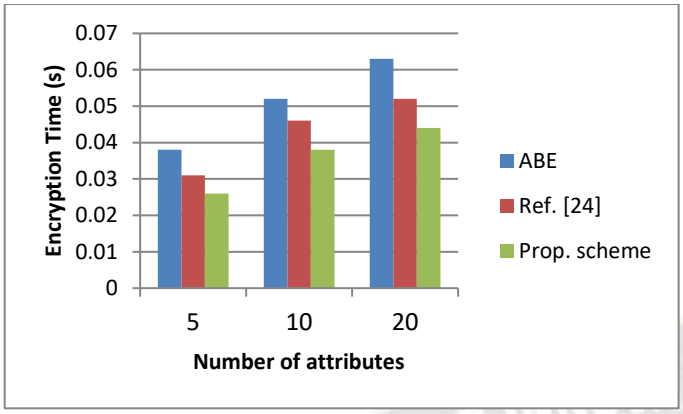

Figure 6. Encryption time for the proposed scheme vs ABE and Ref [24] for different number of attributes.

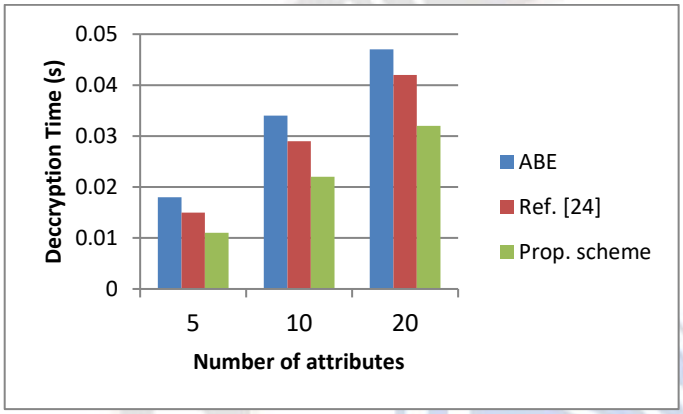

Figure 7. Decryption time for the proposed scheme vs ABE and Ref [24] for different number of attributes.

In summary, our algorithm is giving hopeful results for different number of attributes. From the results, it is found that the encryption time increases linearly with increase in the number of attributes, but the time taken to decrypt is lesser than the encryption time. Similarly, when the number of attributes increases, the time taken for encryption and decryption also increases. It proves that the computational complexity is less.

V. CONCLUSION

In this paper, we have proposed a hybrid approach based on the amalgamation of AES and Cipher text-Policy Attribute Based Encryption (CPABE) without bilinear pairing operations. Here, our goal is to enhance the security and privacy issues in cloud using the CP-ABE based ECC. In this approach, the computation-intensive bilinear pairing operation is replaced by the scalar multiplication on elliptic curves. The use of ECC in the proposed approach makes it more strong and secure than traditional method. The performance analysis shows that the proposed scheme very suitable for high storage requirements in the cloud environment. As future work, the proposed approach will be implemented and evaluated in realistic IoT scenarios.

REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U. S. Department of Commerce, 2011.
[2] Boneh, D.; Franklin, M. "Identity-based encryption from the Weil pairing". Siam J. Comput., 32, pp.586-615, 2003.
[3] Z. Zhou, D. Huang, and Z. Wang, "Efficient Privacy-Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption", IEEE Transactions on Computers, 64 (1), pp.126-138, 2015.
[4] A. Lewko and B. Waters, "Decentralizing attribute-based encryption", Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol.-EUROCRYPT, pp. 568-588, 2011.
[5] V. Odelu and A. K. Das, "Design of a New CP-ABE with Constant-Size Secret Keys for Lightweight Devices Using Elliptic Curve Cryptography", Hoboken, NJ, USA:Wiley, 2016.
[6] V. Odelu, A. K. Das, M. K. Khan, K.-K. R. Choo and M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts", IEEE Access, vol. 5, pp. 3273-3283, 2017.
[7] Nentawe Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment". International Journal of Computer Science and Network Security, Vol.13 No.7, 2013.
[8] Darrel Hankerson, Alfred Menezes, Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, 2004.
[9] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203-209, 1987.
[10] Darrel Hankerson, Alfred Menezes, Scott Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag New York, 2004.
[11] A. Sahai and B. Waters. "Fuzzy identity-based encryption". In 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp.457-473. Springer, 2005.
[12] Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. "Attribute-based encryption for fine-grained access control of encrypted data". In Proceedings of the 13th ACM conference on Computer and communications security, 2006.
[13] Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), Oakland, CA, USA, pp.20-23 2007.
[14] Nguyen, K.T.; Oualha, N.; Laurent, M. "Securely outsourcing the ciphertext-policy attribute-based encryption", World Wide Web, 21, pp.169-183, 2018.
[15] Lai, J.; Tang, A.Q. Making Any Attribute-Based Encryption Accountable, Efficiently; Springer International Publishing: Berlin/Heidelberg, Germany, 2018.
[16] Asst. Lect. Saif Khalid Musluh, Asst. Lect. Riyadh Rahef Nuiaa, "A Novel Multi-Attribute Authority Based Encryption for Controlling Access to Cloud Data". International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 4, no. 6, pp. 558 -562, 2016.
[17] H. Wang, Z. Zheng, L. Wu, and P. Li, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," Cluster Computing, vol. 20, no. 3, pp.2385-2392, 2017.
[18] P. Li, H. Cao and M. Wang, "BSA: "Enhancing Attribute-Based Encryption in Cloud Computing with Decentralized Specification", in IEEE Global Communications Conference, pp. 1-6, 2019.
[19] Miao, Y.; Ma, J.; Liu, X.; Li, X.; Liu, Z.; Li, H. "Practical Attribute-Based Multi-Keyword Search Scheme in Mobile Crowdsourcing", in IEEE Internet Things, vol 5, no 4, pp.3008-3018, 2018.
[20] Yiliang, Han & Di, Jiang & Xiaoyuan, Yang. (). "The Revocable Attribute Based Encryption Scheme for Social Networks", 2015 International Symposium on Security

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.
Article Received: 10 March 2021 Revised: 18 March 2021 Accepted: 02 April 2021 Publication: 31 May 2021

and Privacy in Social Networks and Big Data, pp. 44-51, 2015.

[21] S. Wang, Y. Zhang and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," in IEEE Access, vol. 6, pp. 38437-38450, 2018.

[22] Wu, A.; Zhang, Y.; Zheng, X.; Guo, R.; Zhao, Q.; Zheng, D. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Ann. Telecommun, 74, pp. 1-11, 2019.

[23] Ambrosin, M.; Anzanpour, A.; Conti, M.; Dargahi, T.; Moosavi, S.R.; Rahmani, A.M.; Liljeberg, P. "On the Feasibility of Attribute-Based Encryption on Internet of Things Devices". IEEE Micro, 36, pp.25-35, 2016.

[24] Jaichandran R, Shunmuganathan K.L, Subapriya V, Rahul G, Shahal S H and Rahul Raj, " A Hybrid Encryption Model with Attribute Based Encryption and Advanced Encryption Standard Techniques", Turkish Journal of Computer and Mathematics Education Vol.12 No.2, pp. 334-336, 2021.