Scientific Journal of Research Studies

in Future Engineering Sciences

www.journalhi.com/eng/

New Attribute-Based Encryption Schemes with Anonymous Authentication and Time Limitation on Fog computing

Hafiz Soltani[1]

1- Master's student in Computer Science, Payam Noor University, Urmia, Iran.

Article Information

Original Research Paper
Received 18 March 2023
Accepted 02 October 2023
Available Online 04 October 2023

Keywords:
CP-ABE
KP-ABE
Key Generation
Encryption
Decryption

Abstract

Fog computing faces threats that pose security and privacy challenges to users. Despite the many advantages that cloud computing has, it has many disadvantages and problems that can be partially covered by applying fog computing and its advantages such as increasing security and reducing bandwidth, and reducing network latency. Using the various advantages and features of fog computing, fog computing can be considered a suitable platform for IoT applications and services. Despite all of the above, fog calculations face security issues, threats, and privacy challenges. In this paper, we proposed two new schemes on ABE schemes. New schemes called CP-ABE-AA and KP-ABE-AA are based on CP-ABE and KP-ABE. New schemes have more secure steps and anonymous timed communications. In the communication stage, the server and the user each apply for registration to the RC separately. This request can be at any time and in general. On these schemes, we have more secured communication with timed and anonymous knowing between servers and users. the two schemes are faster than all schemes in key generation, encryption, and decryption in ABE types. CP-ABE-AA in comparison to 5 schemes average for key generation shows less time (5.48%) but in encryption shows more time, 11.28%, at last in decryption again shows less time, 11.33%. Also, KP-ABE-AA in comparison to 2 other schemes average for key generation shows more time (17.31%) but encryption and decryption show fewer times, 17.31% and 9.57%. so, we can say these new schemes are almost fast in some areas and they are more secure too.

Introduction

In 2014, Cisco introduced a concept called Fog Computing. This concept, which includes fog nodes, can be defined as a layer between the cloud and end users. Fog nodes are actually network components that have computational capabilities. In addition to network activities such as sending packets, routing, switching, etc., fog nodes have the ability to perform computational tasks. In cases where transaction time is of particular importance, these nodes, as one of the computationally capable components, play a greater role than other members of the network. On the other hand, the networking capabilities of fog nodes are more important in computational activities. Therefore, a cooperation structure between fog nodes is needed to allow users to privatize. This privatization should be tailored to the needs of the users. Previous research has addressed many features of fog nodes, but the cooperation structure of these nodes needs to be re-examined. Fog nodes can include hundreds of routers, switches, and the like.

Attribute-Based Encryption (ABE) known technology that guarantees privacy to users. In ABE systems, the problem of time required for encryption and decryption must be considered. Many articles have discussed how to encrypt based on data properties, and in this study, we are looking for a mechanism for encryption and decryption more confidential [2]. The main difference between cloud computing and fog computing is the layer between cloud servers and the Internet of Things. Because of this, fog technology may be available for complex attacks, which in turn requires a stronger cryptographic system[۳] .

ABE is promising basic cryptography to control fine-grained access to distributed data. There is a deposit is an inherent key in the ABE system. The curious key generation center in that construction has the power to decrypt any password. We find that many existing ABE designs suffer from key deposit problems depending on their single-key power. Key Generation Center and Feature Authority. This proposal divides the user's key issuance power into two parties .

In this article, we present schemes in data encryption based on data outsourcing in systems and Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) based on fog computing. In these proposed schemes we will focus on time and security. We are looking for better timing in key generation, encryption, and decryption. We'll use Registration Center (RC) for anonymous authentication. We propose schemes for key issuance architecture that solves the key deposit problem mentioned earlier. In these schemes' construction, the key generation center and authority feature this issue of different parts of the secret key components for users through a two-party secure computing scheme so that none of them can determine the full set of keys of users individually he does. We demonstrate how the proposed key issuance scheme can be applied in the existing ABE scheme and solve the key deposit problem.

In this article, next we discust consepts that we use several times and must be known. In section 4 we intridoce related works as base of proposed schemes. In section 5 proposed schemes are introduce, they are two schemes which we named them as KP-ABE-AA and CP-ABE-AA. We discuse security analysis of proposed schemes for the safty behavior they have. It is important to ensure them security in known attacks. We simulate proposed porotocols and compare them with some famous protecols in timing in the 7th section. At last we canclue all subject and informations about what it done.

Cosepts

This research needs to explain the following six concepts:

RC

The registration center is a reference that provides user and cloud service provider information to the system.

Cloud Service Providers (CSPs)

They are responsible for running and maintaining software programs, operating systems, and computing resources.

Bilinear Maps (BM)

Here are some rules for mapping Bilinear Maps to groups:

If G1 and G2 are two polycyclic groups of groups of order p. g is the construct of G1 and e is a two-way function mapping as follows:

e:G1×G2 - G2

Then the following rules apply in e:

Bilinearity: For all u,v∈G_1and a,b∈Z_p we have e(u^a,v^b)=e〚(u,v)〛^ab

Non-degeneration: e (g, g) ≠ 1

We say that G1 is a two-way group if the group operators in G1 and the BM (e:G1×G2 - G2) are both perfectly computable. Note that the mapping e is symmetric, because:

e(g^a,g^b)=e〚(g,g)〛^ab=e(g^b,g^a)

Access tree

An access control tree is used to define access control in attribute-based cryptographic systems. The access tree is defined as follows:

Suppose T is a tree that represents an access structure. Each non-leaf node of this state is a threshold gate. This node is described by its children and a value of Kx. If numx is the number of children in node x and Kx is the threshold value of this node, then:

0≥K_x≤num_x

It is clear that if Kx = 1 then the threshold gate is an OR and when Kx = numx, the threshold gate will be an AND[۵] .

KP-ABE

Encryption is the basic public key for one-to-many communications. In KP-ABE, data is defined with attributes, each of which is a public key component. The encoder encrypts a set of message-related features by matching the public key components. In this system, each user's key depends on an access tree structure in which the leaves have the same properties. A user can decrypt text if the attributes of the encrypted text in the access tree in his key apply[۵] .

CP-ABE

In the CP-ABE schema, the user's private key is associated with an arbitrary number of descriptive features. On the other hand, when a user encrypts text, it specifies an access structure based on its attributes. The decoder can only open encrypted text if its properties apply to the encrypted text access tree. The password with the encrypted text policy is quite similar to the password with the key policy, except that the access tree is encrypted in the text and the attributes are in the key of each user. [5].

Related works

Fog nodes are much closer to the end-users than the cloud structure, and some of the behaviors and tasks of cloud systems are similar in these nodes. [6] ABE (Attribute-Based Encryption) is a scalable and flexible encryption scheme that allows good access control. ABE was first introduced by Sahay and Waters as a new scheme for fuzzy identity-based encryption. [7, 8] ABE has two schemes for encryption: KP-ABE (Key-Policy ABE) [9] and CP-ABE (Ciphertext Policy) [10]. It works so well that it controls access to many IoT applications[۱۱-۱۴] .

For the first time, Yu et al. [12] introduced a good access control scheme for wireless network sensors, and they chose KP-ABE to protect data. CP-ABE is also one of the best ways to manage cryptographic access, first proposed by Betancourt et al.[۱۶] .

In contrast to KP-ABE, CP-ABE is much more suitable for controlling access in the IoT, due to how the cryptographic policy is expressed. Hu et al. [13] designed a communication schema for secure data that works between wearable sensors under CP-ABE management on the body's wireless networks. The clients of this project are doctors and nurses. Jiang et al. [14] used a CP-ABE schema against key misuse in fog calculations. Yeh et al. [15] developed a well-designed health information access control framework, which is used in cloud networks and for lightweight IoT devices. However, the biggest significant obstacle for ABE to use in fog calculations is the computational cost in the encryption and decryption phases, the time complexity of which is linear depending on the scheme used.

Fog nodes are at the edge of the cloud and closer to the end-users. These are the best agents for

outsourcing [17, 18] that can be allocated in heavy computing to reduce computational overhead. Overhead is a computational overhead that is negligible on IoT devices. The main solution of this scheme is to generalize the CP-ABE encryption and decryption phase calculations to network nodes, by which IoT devices are forced to manage the consumption factors to the network nodes[۱۹-۲۴] .

Lunis et al. [21] designed a cloud-based architecture that is medical for WSNs (Wireless Sensor Networks). Sensor nodes outsource encryption operations to secure interfaces, encrypting data based on CP-ABE before sending it to the cloud. This solution requires full trust to be able to encrypt the data, so this solution is not practical in terms of computational outsourcing.

Zoe et al. [22] designed an ABE schema that can outsource decryption operations in fog calculations. Yang et al. [23] introduced you in a way that works with low computational overhead for the IoT health system. They introduced a quasi-secure system for the computing center that performed most of the heavy computing in the encryption phase. Based on the ABE schema for IoT, Yang et al. [24] identified two dual clouds that could outsource computational cloud encryption. This operation was a bit costly. However, the listed schemes can only support encryption or decryption outsourcing. Almost all ABE generation of schemes, research focus just on time; times of key generation, encryption, and decryption. We have done the same and produce good results, in the implementation section we'll check that. Also, in this article, we would focus on security and key generation practically.

Scheme in [31], the private key is associated with the set of attributes for encryption and decryption purposes for using. The proposed scheme [32] also allows a user to access the secure data stored in the blocks into the blockchain using the CP-ABE scheme. in [33], authores propose an original hybrid cloud multi-authority ciphertext-policy attribute-based encryption (HCMACP-ABE) scheme. They utilize the LSSS (Linear Secret-Sharing Schemes) access structure to realize secure access control.

Proposed schemes

ABE allows the encoder to more generally specify the persons allowed to decrypt. In an Attribute-based encryption system, user keys and encrypted texts are labeled with a set of descriptive features. In these schemes, a special key can open a special encrypted text, if there is a match between the properties of the unencrypted text and the user key, in the access-based access control, access control decision based on the features taken from the requester, services, Its resources, and environment. Next, we'll introduce two new models on ABE and KP/CP-ABE. Each one has three phases.

KP-ABE-AA[1] scheme

In attribute-based cryptography with a key policy with anonymous authentication, we upgrade the KP-ABE scheme and introduce the KP-ABE-AA model, which consists of three phases:

Setup

[1] Key-Policy Attribute-Based Encryption Anonymous Authentication

In this algorithm, the cloud service provider CSPs and the user first register in the registration center and receive aliases, encryption functions, and other security information. The important point in this process, first the user must select an image from several images. This photo plays a key role in the registration process and the selection of private, public, and session keys. Another point is to use the time parameter t. Time t is a number between m and n. This parameter determines the validity period of the key.

Encryption

The first difference with the KP-ABE algorithm is that in building the T-tree section, user/node aliases are used. To do this, users, who can be any smart and intelligent device, first open an account through a registration center, and then as much as time t is specified in RC, two-way communication between the user and the server can be established after the time is up. The server and user are required to obtain a new alias. The time interval t can be m to n seconds. This number is selected randomly at the beginning of the nickname.

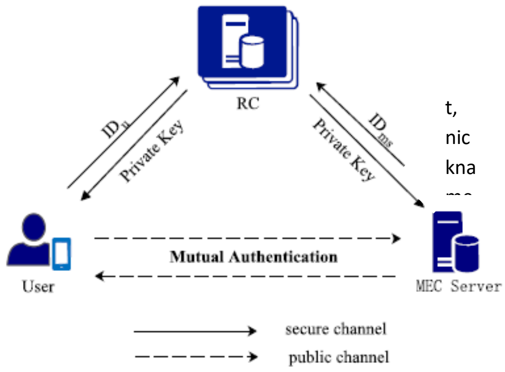

Figure 1: Scheme of how users receive the name

The user registers at the center and can then interact with cloud/fog systems. Cloud/fog systems will identify users by their virtual names based on information received from the RC, and from then they will be in direct contact with users, the nickname identifies the user. Also, the servers are registered in the registration center, and this is another step towards more security. The proposed scheme is also designed to make the user anonymous and uncontrollable, allowing a registered mobile user to access multiple MEC servers with a single registration. Besides, cross-authentication between the user and the MEC server requires only one unit of message exchange per time, as long as t time, and is as valid as that time. The proposed architecture also provides other security services, such as privacy, confidentiality, mutual authentication, and no tracking. The system is secure and resistant to known attacks of repetition, middle man, eavesdropping, forgery, etc., like conventional schemes. Securing the data in the cloud/fog using appropriate technology and the KP-ABE algorithm are other issues considered in this research.

In short, if time t is still valid, encryption is performed in full based on the security data sent by the RC. If time t has lost its validity, the start-up algorithm is repeated except for image selection. The user selects an image only once.

Decryption

The information is decrypted according to the access tree and public and private keys and other security information.

CP-ABE-AA scheme

In the attribute-based encryption diagram with an anonymous authentication encrypted text policy, we upgrade the CP-ABE scheme and introduce the CP-ABE-AA model, which consists of three algorithms:

Setup

Like the KP-ABE-AA algorithm, this algorithm first registers the CSPs cloud service provider and the user at the RC Registration Center and receives the aliases, encryption function, and other security information. Other explanations are the image selection and time t sections, such as the KP-ABE-AA algorithm startup section.

Encryption

Like the CP-ABE algorithm, with the difference that in the T tree construction section, like the KP-ABE-AA algorithm, user/node aliases are used. Other explanations of the KP-ABE-AA encryption section in this algorithm are also used to build the tree. And the connection between network components applies.

Also, as we declare in Encryption phase if time t is still valid, such as encryption of the KP-ABE-AA algorithm, encryption is performed in full based on the security data sent by the RC.

Decryption

Like the CP-ABE algorithm, so in general, it can be said that having a licensed production center can implement this system for IoT.

In the proposed schemas, for license of connection shcemas work with the registration center before contacting the license generation center. This registration center will introduce them to the license generation center. In fact, according to the access tree and public and private keys, and other security information, the information is decrypted.

A formal model of the registration scheme

In this model and to describe it, we will use the following table.

Table 1:Symbols used in this paper

Addition and multiplication functions	H_1, H_2	User i, Server j	U_i, SP_j
User ID and private key	ID_i, S_i	H_1 Generator	P
Sequence continued	$\|\|$	Messages used during authentication	Z, K_2, C_1, D_i
Server ID	ID_j	Private key s and public key P_{pub}	s, P_{pub}
Registration Center	RC	Cloud Provider Service	CSP_s

User password	PW_i	Cloud Provider Service ID	SID_j
The main RC key	s^*, s_1^*	User-selected image i	X_i
function hash	h(.)	function X-Hashing	H(.)
Decryption function	Dec(.)	Encryption function	Enc(.)
Session key	SK	Bilinear pairing function	E(.,.)
Time threshold range	TΔ	Time steps	t_1, t_2, t_3, t_4, t
Time	t	XOR function	$\oplus$

The following happens during the registration phase:

1- Registering of CSPs through a secure channel

a. The cloud service provider (CSP) selects ID_j

b. CSP sends ID_j to RC

c. RC gets values from CSP. It is consists of two parts:

i. RC receives ID_j from CSP and calculates $SID_j = h(ID_j||s^*)$

ii. SID_j and the random value of t (an integer between m and n seconds) stores in RC

d. RC sends SID_j and t to CSP

e. CSP gets values from RC. It is consists of two parts:

i. CSP receives SID_j and t from RC

ii. CSP stores SID_j and t

2- User registration through a secure channel

a. User ID_i selects PW_i , X_i and CSPs name

b. User ID_i sends PW_i , X_i and CSPs name to RC

c. RC receives and calculate the values of user. It is consists of four parts:

i. RC receives the identifier from the user (ID_i and PW_i and CSPs names) and calculates this value $R = h(ID_i||PW_i) \oplus s^*$

ii. The value of R is stored in RC concerning ID_i

iii. RC calculates the value $U_i = h(ID_i||s^*)$

iv. RC stores the values R, s *, H (.), h (.), Enc (.), Dec (.), E (.,.) And t (from the server registration step) as secret information

d. RC sends series information and SID_j to the user

e. User side gets information and does a calculate and saves. It is consists of two parts:

i. The user receives the series information and SID_j from the RC and calculates the following value and stores it in the fog device in secret $G_i = h(R||H(X)_i)$

ii. The device now contains the values R, G_i, s *, H (.), h (.), Enc (.), Dec (.), E (.,.) And t and SID_j

f. RC sends U_i to CSPs

g. CSPs receive the U_i from the RC and store it in CSPs

3- Authentication and entry phase:

a. Calculating and checking parameters. This step consists of 10 sections:

i. The user ID_i enters the value PW_i in the fog machine and re-selects the image he/she selected during the registration step from among the n images displayed

ii. $h(ID_i||PW_i) \oplus s^* = R^*$

iii. is $R^* =? R$

iv. $h(R||H(X)_i) = G_i^*$

v. is $G_i =? G_i^*$

vi. $X_1 = h(ID_i||s^*) \oplus SID_j$

vii. $X_2 = h(ID_i|\|H(X_i))$

viii. $B = Enc_{h(X_1)}(X_2)$

ix. Is $t >?$ t*

b. The mobile user sends B and X_2 to CSP

c. CSP receives values (B and X_2) from the user and calculates the following values:

i. $t_2 - t_1 \leq \triangle T$

ii. $X_1^* = U_i \oplus SID_j$

iii. $X_2^* = Enc_{h(X_1^*)}(\mathrm{B})$

iv. $X_2^* =? X_2$

v. $Z_1 = h(X_1^*||B)$

vi. $Z_2 = Enc_{h(X_{1||}^*B)}(Z_1)$

vii. $Z_3 = h(Z_1||Z_2||t_3)$

viii. The key to the session is $SK = Z_3||t$

d. CSP sends the values Z_1, Z_2, Z_3 to the user

e. The user receives the values from the CSP (Z_1, Z_2, Z_3) and calculates the following values:

i. $t_2 - t_1 \leq \triangle T$

ii. $Z_1^* = Dec_{h(X_{1||}^*B)}(Z_2)$

iii. $Z_1^* =? Z_1$

iv. $Z_3^* = h(Z_1||Z_2||t_3)$

v. $Z_3^* =? Z_3$

vi. The key to the session is $SK = Z_3||t$

Carefully in the eighth part c and the sixth part e, we see that the two sides of the connection have reached a common key. This confirms the correctness of the performance of formal relationships. This connection will be as long as t seconds.

Security analysis of proposed schemes

Mutual authentication: Only registered users and MEC servers are allowed in the MEC environment and can verify each other's legality by implementing the scheme .

Session Key Agreement: Successful implementation of the scheme creates a shared session key shared by the mobile user and the MEC server for further communication, while other users, including RC, are unable to receive key session information.

Discussed layer: The session key is exchanged and verified in the session layer. On the other hand, information exchange, encryption, and decryption take place in the transmission layer.

The anonymity of the user: The mobile user must be anonymous to others except for direct access via RC and indirectly with the MEC server. Neither party can identify the user from the intercepted messages.

No tracking: Except for access to a specific MEC server, not every user in this system can obtain the activities and behavioral patterns of a user from the intercepted messages.

Complete confidentiality forward: it is impossible for the other party to find anything about the key of the meeting in the previous meeting except the part related to him, even if he has short-term secret keys (time-dependent t) of both participants in a secure connection To know.

SSO[1] function: To benefit from the services of multiple MEC servers, the mobile user only needs to register in the RC once.

Online RC: RC must be online all the time, ie after obtaining private keys, the user and the MEC server can achieve mutual authentication without the help of RC. In practice, the two sides of the connection must be independent, but due to the time t of the connection, the RC must be online.

Resistance to various attacks: The proposed scheme should resist attacks such as forgery, authentication, middle man, and so on.

Simulation

We implement our CP-ABE-AA and KP-ABE-AA schemes in Rust which are installed on Ubuntu 20 as OS. Rust is a multi-paradigm programming language designed for performance and security concurrency. Rust is syntactically similar to C++. In this phase, we calculate the time of run of the proposed scheme with some other basic schemes that had so many cite on them. There are lots of schemes in CP-ABE and KP-ABE. With these selected schemes we can compare our scheme with so many schemes that compared with them. In CP-ABE we implemented these schemes:

- BDABE[۲۵]
- AC17[۲۶]
- AW11[۲۷]
- BSW[۲۸]
- MKE08[۲۹]

And for KP-ABE we implemented these 2 schemes:

- AC17[۲۶]
- LSW[۳۰]

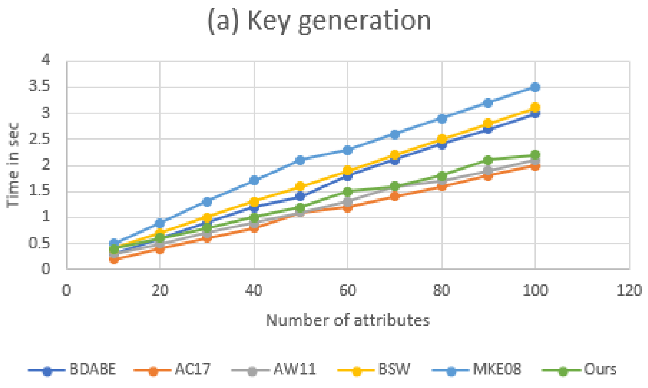

Figure 3: Ciphertext-policy attribute-based encryption time for key generation.

[1] Single sign-on (SSO)

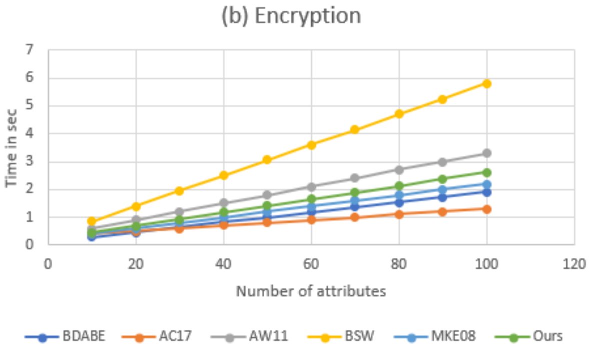

Figure 4: Ciphertext-policy attribute-based encryption time for encryption.

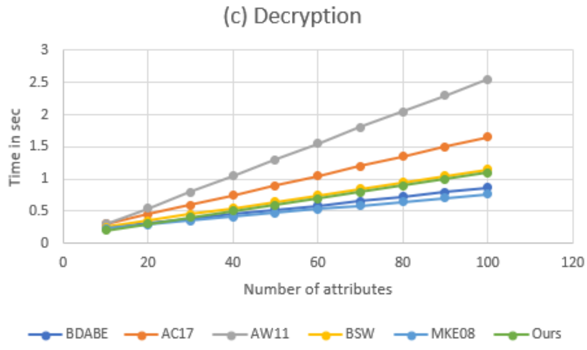

Figure 5: Ciphertext-policy attribute-based encryption time for decryption.

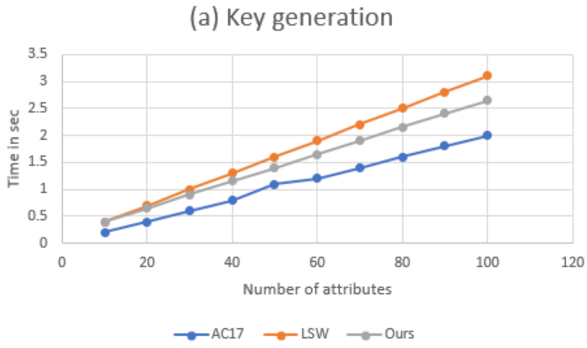

Figure 6: Key-policy attribute-based encryption time for key generation.

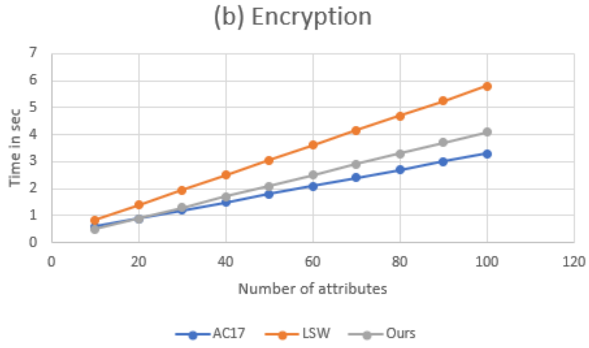

Figure 7: Key-policy attribute-based encryption time for encryption.

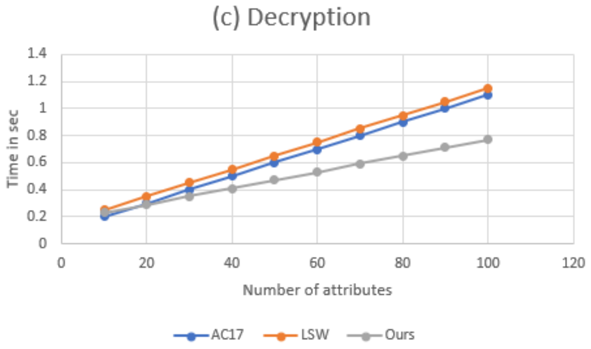

Figure 8: Key-policy attribute-based encryption time for decryption.

In these charts, we can see the different percentages of time in a competition of CP-ABE-AA and KP-ABE-AA. CP-ABE-AA shows for BDABE and MKE08, key generation time was shorter but encryption and decryption were longer. For AC17 decryption was shorter but 2 other measures were longer. For AW11 we see longer time on key generation and better time in the other two measures. For BSW, in all measures, we see better timing. KP-ABE-AA was faster in decryption than BSW and longer timing in key generation and encryption but it was better in all measures than LSW.

Table 2: CP-ABE-AA

class	BDABE	AC17	AW11	BSW	MKE08
Key generation	-12.3095	29.58766	12.43763	-21.272	-35.8522
Encryption	43.19816	71.31318	-22.0199	-53.0214	16.97018
Decryption	12.64471	-34.8203	-51.4891	-8.9102	24.41337

Table 3: KP-ABE-AA

class	BSW	LSW
Key generation	45.69453	-11.0777
Encryption	13.13456	-32.2669
Decryption	-17.7813	-25.7437

We have so many connections and calculated as proposed schemes compare to other schemes but still, our scheme is in average timing comparing to other schemes and it is better in some (Fig. 3-5, Fig. 6-8).

Conclusion

In this paper, we have a review of KP-ABE and CP-ABE schemes. We have already defined the ABE algorithm and the access tree. Next, we defined the two new algorithms KP-ABE-AA and CP-ABE-AA in such a way that in the new definitions, servers and users register using an RC and then their nicknames to build the access tree. The whole work consists of two phases, which in general, this registration must have taken place before the exchange of communication. Access to The key to the session reminds until a specific time after that user must register himself/herself again. To do this, first, open an account, and then as long as time t, two-way communication between the user and the server can be established, after the end of the server and user time are required to receive a new nickname. Also like CP-ABE and KP-ABE algorithms, KP-ABE-AA and CP-ABE-AA algorithms we have to build the tree. The proposed schemes are designed to make the user anonymous and uncontrollable, allowing a registered mobile user to access multiple MEC servers with a single registration. In short, our schemes are more safe then all examined schemes, also, in some aim they were better in timing and in some worst but in average they are better overall. Communication in a discrete channel with unknown noise is our next goal to reach for better safty.

References

[1] R. Lu, K. Heung, A. Lashkari, and A. Ghorbani, “A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT,” IEEE Access, vol. 5, pp. 3302-3312, 2017.

[2] P. Zhang, Z. Chen, J.K. Liu, K. Liang, and H. Liu. (2016, Dec.). An efficient access control scheme with outsourcing capability and attribute update for fog computing. Future Generation Computer Systems. [Online]. Available: https://doi.org/10.1016/j.future.2016.12.015.

[3] Zuo, Cong, et al. "CCA-secure ABE with outsourced decryption for fog computing." Future Generation Computer Systems 78 (2018): 730-738.

[4] Wang, Shulan, et al. "An efficient file hierarchy attribute-based encryption scheme in cloud computing." IEEE Transactions on Information Forensics and Security 11.6 (2016): 1265-1277.

[5] Lee, J., Oh, S., & Jang, J. W. (2015). A Work in Progress: Context based encryption scheme for Internet of Things. Procedia Computer Science, 56, 271-275.

[6] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, “On security and privacyissues of fog computing supported Internet of Things environment,” in Proc.2015 International Conference on the Network of the Future, Montreal, QC,Canada, 2015.

[7] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. 24thAnnual International Conference on the Theory and Applications ofCryptographic Techniques Aarhus, Denmark, 2005, pp. 457-473.

[8] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” inProc. 30th Annual International Conference on the Theory and Applications ofCryptographic Techniques, Tallinn, Estonia, 2011, pp. 568-588.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-basedencryption for fine-grained access control of encrypted data,” in Proc. 13thACM Conference on Computer and Communications Security, New York,USA, 2006, pp. 89-98.

[10] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policyattribute-based encryption,” in Proc. 2007 IEEE Symposium on Security andPrivacy, Berkeley, California, USA, 2007, pp. 321-334.

[11] S. Ruj, A. Nayak, and I. Stojmenovic, “Distributed fine-grained accesscontrol in wireless sensor networks,” in Proc. 2011 IEEE InternationalParallel & Distributed Processing Symposium, Anchorage, Alaska, USA, 2011,pp. 352-362.

[12] S. Yu, K. Ren, and W. Lou, “FDAC: toward fine-grained distributed dataaccess control in wireless sensor networks,” IEEE Transactions on Paralleland Distributed Systems, vol. 22, no. 4, pp. 673-686, 2011.

[13] C. Hu, H. Li, Y. Huo, and T. Xiang, “Secure and efficient datacommunication scheme for wireless body area networks,” IEEE Transactionson Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94-107, 2016.

[14] Y. Jiang, W. Susilo, Y. Mu, and F. Guo. (2017, Jan.). Ciphertext-policyattribute-based encryption against key-delegation abuse in fog computing.Future Generation Computer Systems. [Online]. Available:https://doi.org/10.1016/j.future.2017.01.026

[15] L. Yeh, P. Chiang, Y. Tsai, and J. Huang. (2015, Oct.). Cloud-basedfine-grained health information access control framework for lightweight IoTdevices with dynamic auditing and attribute revocation. IEEE Transactions onCloud Computing. [Online]. Available: https://doi.org/10.1109/TCC.2015.2485199

[16] J. Bethencourt, A. Sahai, B. Waters, Ciphertext policy attribute-based encryption,in: Proceedings of the 2007 IEEE Symposium on Security and Privacy, IEEEComputer Society, 2007, pp. 321–334. http://dx.doi.org/10.1109/SP.2007.11.

[17] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiabledatabases with efficient updates,” IEEE Transactions on Dependable & SecureComputing, vol. 12, no. 5, pp. 546-556, 2015.

[18] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New algorithms for secureoutsourcing of modular exponentiations,” IEEE Transactions on Parallel &Distributed Systems, vol. 25, no. 9, pp. 2386-2396, 2014.

[19] S. Hohenberger and B. Waters, “Online/offline attribute-based encryption,”in Proc. 17th International Conference on Practice and Theory in Public-KeyCryptography, Buenos Aires, Argentina, 2014, pp. 293-310.

[20] N. Oualha and K. T. Nguyen, “Lightweight attribute-based encryption forthe internet of things,” in Proc. 25th International Conference on ComputerCommunications and Networks, Waikoloa, Hawaii, USA, 2016, pp. 1-6.

[21] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, “Healing on thecloud: Secure cloud architecture for medical wireless sensor networks,” FutureGeneration Computer Systems, vol. 55, pp. 266-277, 2016.

[22] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji. (2016, Nov.). CCA-secureABE with outsourced decryption for fog computing. Future GenerationComputer Systems. [Online]. Available: https://doi.org/10.1016/j.future.2016.10.028.

[23] Y. Yang, X. Zheng, and C. Tang. (2016, Nov.). Lightweight distributedsecure data management system for health internet of things. Journal ofNetwork and Computer Applications. [Online]. Available: https://doi.org/10.1016/j.jnca.2016.11.017.

[24] Yang, L., Humayed, A. and Li, F., 2016, December. A multi-cloud based privacy-preserving data publishing scheme for the internet of things. In Proceedings of the 32nd Annual Conference on Computer Security Applications (pp. 30-39).

[25] Bramm, G., Gall, M. and Schütte, J., 2018. Blockchain-based Distributed Attribute based Encryption.

[26] Agrawal, S. and Chase, M., 2017, October. FAME: fast attribute-based message encryption. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 665-682).

[27] Lewko, A. and Waters, B., 2011, May. Decentralizing attribute-based encryption. In Annual international conference on the theory and applications of cryptographic techniques (pp. 568-588). Springer, Berlin, Heidelberg.

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

[29] Müller, S., Katzenbeisser, S. and Eckert, C., 2008, December. Distributed attribute-based encryption. In International Conference on Information Security and Cryptology (pp. 20-36). Springer, Berlin, Heidelberg.

[30] Lewko, A., Sahai, A. and Waters, B., 2010, May. Revocation systems with very small private keys. In 2010 IEEE Symposium on Security and Privacy (pp. 273-285). IEEE.

[31] Jalwa S, Sharma V, Siddiqi AR, Gupta I, Singh AK. Comprehensive and comparative analysis of different files using CP-ABE. InAdvances in Communication and

Computational Technology 2021 (pp. 189-198). Springer, Singapore.

[32] Banerjee S, Bera B, Das AK, Chattopadhyay S, Khan MK, Rodrigues JJ. Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT. Computer Communications. 2021 Mar 1;169:99-113.

[33] Xie M, Ruan Y, Hong H, Shao J. A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices. Future Generation Computer Systems. 2021 Aug 1;121:114-22.