IJE TRANSACTIONS C: Aspects Vol. 32, No. 9, (September 2019) 1290-1298

International Journal of Engineering

Journal Homepage: www.ije.ir

DoS-Resistant Attribute-Based Encryption in Mobile Cloud Computing with Revocation

H. Nasiraee, M. Ashouri-Talouki*

Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran

PAPER INFO

Paper history:
Received 25 October 2018
Received in revised form 15 May 2019
Accepted 31 July 2019

Keywords:
Attribute-Based Encryption
Dos Resistance
Iot Devices
Mobile Cloud Computing
Secure Access Control

ABSTRACT

Security and privacy are very important challenges for outsourced private data over cloud storages. By taking Attribute-Based Encryption (ABE) for Access Control (AC) purpose we use fine-grained AC over cloud storage. In this paper, we extend previous Ciphertext Policy ABE (CP-ABE) schemes especially for mobile and resource-constrained devices in a cloud computing environment in two aspects, a novel authentication mechanism and a new revocation approach. To wide-spread adoptions of ABE for a resource-constrained device, a very light-weight authentication mechanism is required to authentication ciphertext before starting cost expensive ABE techniques to thwart Denial-of-Service (DoS) attacks which are used to power depletion and network downing purposes by attackers. We introduce and address the problem to more robustness of whole networks when DoS attacks are present. Moreover, we propose an efficient revocation mechanism which is a very important challenge in the context. Finally with a discussion on different aspects of the proposal and extensive experimental results we show its profitability.

doi: *10.5829/ije.2019.32.09c.09*

1. INTRODUCTION

Computing over the cloud is a very important technology paradigm, which resources (data storages and computing) are provided dynamically via the Internet. It got much attention due to high profitability. In outsourcing, it is important to have secure and efficient access control to prevent unauthorized access. The reason is that when computation or private data is outsourced to the clouds, privacy and security risks will emerge because the Cloud Service Providers (CSPs) are untrusted. Then owner of private data must encrypt them before outsourcing by including an access policy in the ciphertext. Consequently, the data owner should be able to select a secure and dependable fine-grained access control over data before outsourcing.

Various techniques have been proposed for the content of private data via access control upon after proposing the Identity-Based Encryption (IBE) by Shamir. In 2005, Fuzzy Identity-Based Encryption or Attribute-Based Encryption is proposed [1]. In ABE, identity is considered as a set. The set is composed of some attributes [2, 3].

Upon proposing ABE, so many ABE schemes have proposed for access control especially to be used in cloud computing. In spite of many research in this hot research filed, still, there is many existing open issues and unresolved challenges which we address two important in this paper. In an ABE scheme, due to the high cost of asymmetric cryptography and attribute-based encryption, it is required a light-weight authentication mechanism before full decryption, especially for low capacity Internet-of-Things (IoT) devices and resource constrained mobile devices, to resist them against DoS attacks and power depletion. Moreover, attribute and user revocation is a very important challenge and open problem which attracted very attentions. We address the challenge and efficiently resolve it as our second extension. Finally, using a limited and only AND-gates access structure to provide efficiency in many existing works, violates the main strength of attributed based encryption idea (as expressiveness and flexibility). Then

*Corresponding Author Email: *m.ashouri@eng.ui.ac.ir* (M. Ashouri-Talouki

Please cite this article as: H. Nasiraee, M. Ashouri-Talouki, DoS-Resistant Attribute-based Encryption in Mobile Cloud Computing with Revocation, International Journal of Engineering (IJE), IJE TRANSACTIONS C: Aspects Vol. 32, No. 9, (September 2019) 1290-1298

another motivation is proposing a new scheme to address the before mentioned problems along with considering a strong monotonic access tree structure (including both of AND, OR gates).

We provide an efficient approach to authenticate and verify the source of downloaded ciphertext before full decryption which has negligible computation cost versus previous approaches. As an extention of our previous work in [4], it can revoke both attribute and user in an efficient manner (inspired from [5]). Secondly, we provide an extensive and comparative implementation, and then we summarize the results in some diagrams. The proposal also can efficiently detect and discard replayed packets. Our proposal is expressive and the access structure includes both AND-gates and OR-gates in a monotonic access tree structure and has only one output ciphertext per any access tree. Moreover, our proposal provides other necessary and fundamental requirements of an ABE scheme, such as confidentiality and collusion-resistance.

We organized the rest of the content as follow. In section 2, we review related works in the field. Section 3 gives preliminary required to understand the proposal. System architecture and security model are presented in section 4. We detailed the proposal in section 5. Discussion on different aspects of the proposal is presented in the next section. Our implementation and its experimental results elaborated in section 7. Conclusion of the paper presented in section 8.

2. RELATED WORKS

Upon proposing the ABE in the implementation of fine-grain access control, an abundance of research has been carried out on ABE systems. ABE has two kinds, called KP-ABE (Key Policy ABE) and CP-ABE (Ciphertext Policy ABE) [2, 3].

In a CP-ABE access control system, the Data Owner (DO) encrypts the data with a public key and access policy (for example an access tree built by AND, OR gates). Then secret keys, which are associated with the attributes, are used to decrypt the ciphertext by Data Customer (DC). KP-ABE is dual of CP-ABE, which means DO encrypt the data with a set of attributes and the authorized DC decrypts it with an access policy.

Goyal et al. in [2] realized the policy of access structure for key policies as first KP-ABE scheme. For more flexibility in an access policy, the first KP-ABE system that supports the expression of non-monotone formulas in key policies is proposed in [6]. Zhang et al. [7] presented another construction that proved to be safe. Unfortunately in their proposal access structure is limited to only AND gates to provide efficiency. To protect the confidentiality of user attributes, anonymous ABE has been studied in [8–10]. They introduced new schemes, which can perform hidden policies of encrypted text from the limited access structure.

Recently, the confidentiality of identities and attributes was taken into account in the CP-ABE decentralized schemes [11–14]. However, they are very expensive for resource-constrained devices and needs more efficiency and improvements. Another proposed construction to address the confidentially as [15], suffer from serious disadvantages of efficiency due to decryption cost. Another recent work which is proposed in [16] suffers from a security drawback in terms of the backward and forward secrecy. The proposed idea is based on validation time and timely fashion.

Very recent two works which are proposed to resolve the source authentication problem with fast decryption and verifiable outsourced decryption are [7, 17]. But unfortunately, both of them use asymmetric cryptography and pairing operations in verification mechanism that itself is a potential for denial-of-service vulnerability in mobile devices by launching so many request-based attacks. Other very recent eligible works are [16–22]. In [16], a new access structure as Blocked Linear Secret Sharing Scheme (BLSSS) is proposed for more scalability, but providing efficiency by managing partial blocks left for future works. In LYYJ [20], a verifiable mechanism is provided to verify outsourced computations but require two pairing operations in the verification process which is expensive for resource-constrained mobile devices. An online/offline cryptographic technique is used in [19] to reduce online computation cost for users but there is not access policy extension and privilege grant for authorized users. In [5], an innovative CP-ABE scheme is proposed to efficiently support attribute and user revocation. We inspired from the scheme and proposed a more efficient revocation mechanism. As multi-authority and accountability support scheme two interesting schemes are proposed in DAC-MACS [22] and Li [21], respectively. In the practical comparison and analysis, we implemented the two schemes to compare with our proposal. Finally, in [18] the online/offline techniques and Chameleon hash function (to generate immediate ciphertext) is used to increase efficiency in the decryption phase for resource-constrained users.

Now, along with keeping in mind the pros and cons of the reviewed state-of-the-arts, we propose a dependable and robust ABE scheme to cover ours before-mentioned contributions.

3. RPRELIMINARIES AND DEFINITIONS

3. 1. Bilinear Pairings Let assume G_1 and G_2 are the cyclic multiplicative and the order of them is a large prime order p. The identities of G_1 and G_2 are denoted as 1_G and 2_G, respectively. We call e a bilinear

pairing if $e: G_1 \times G_1 \rightarrow G_2$ is a map which has the following properties:

- Bilinear: $e(g^a, g^b) = e(g,g)^{ab}$ for all $a, b \in Z_p$.
- Non-degenerate: There exists $g \in G_1$ so $e(g,g) \neq 1_{G_2}$.
- Computable: There is an efficient algorithm to compute $e(g^a, g^b)$ for all g, $g \in G_1$.

3. 2. One-Way Hash Chain A public one-way function h and a random value a_M are selected by the DO. The one-way chain is iteratively calculated by $a_{i-1} = h(a_i)$. The elementa_{i-1}, as the commitment, would be included in the outsourced ciphertext. Concerning the one-way function, calculating in a reverse way is expected to be infeasible. So it is easy to check the validity of any newly received element using the commitment.

3. 3. Complexity Assumptions Definition 1: The DBDH (stand for Decisional Bilinear Diffie-Hellman) problem with generator g in the group and prime order p is as the following: on input g, g^a, g^b, $g^c \in G_1$, and $e(g,g)^z \in G_2$, where $a, b, c, z \in_R Z_p$, decide whether $e(g,g)^z = e(g,g)^{abc}$.

The security of many ABE systems and ours are based on the assumption that there are not any probabilistic polynomial- time algorithms that be able to solve the Decisional Diffie-Hellman (DDH) or DBDH problem with a significant advantage. It is reasonable due to the intractability of DL (Discrete Logarithm) problem in the cryptography.

3. 4. Definitions Let $U = \{DC_1, DC_2, DC_3, \dots, DC_n\}$ and $\pi = \{\gamma_1, \gamma_2, \gamma_3, \dots, \gamma_q\}$ are the universe of data customers and attributes, respectively. Attribute group $G_k \subset U$ is a set of users that holds the attribute γ_k and is a revocation (user access) list to γ_k. Finally $G = \{G_1, G_2, \dots, G_q\}$ is the universe of such attribute groups and K_{γ_k} that is shared among non-revoked users is named as attribute group key.

3. 5. Lagrange Coefficients We use $LC_{i,S}$ for $i \in Z_p$ and a set S of elements in Z_p as the Lagrange Coefficient:$LC_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x - x_j}{x_i - x_j}$. As we see later, in decryption process we need the coefficients for polynomial interpolation. Moreover, we need a non-reversable hash function $H: \{0,1\}^* \rightarrow G_1$ in random oracle model.

3. 6. Access Structure We describe encryption policy with an access structure which is a tree data-structure. In the tree, a leaf-node is an attribute and a non-leaf node assumed as a threshold-gate. For a given tree T_o, if we set c_x as the number of the node's x children then its threshold value t_x satisfy $0 < t_x \leq c_x$, and if at least t_x children nodes have been assigned true value then the node x is assigned a true value. In fact, for OR-gate we have $t_x = 1$ and for AND-gate we have $t_x = c_x$. As satisfying rules, if $T_o(S) = 1$ or $x(S) = 1$ then it means the tree T_o or the node x is satisfying by the user's attributes. T_o is usually calculated recursively as follows. If at least t_x child return 1 and x is a non-leaf, then we have $x(S) = 1$. If $att(x) \in S$ and $S(x) = 1$ then x is a leaf node. For root the node R_o of T_o, $T_o(S) = 1$ only if $R_o(S) = 1$.

4. SYSTEM ARCHITECTURE AND SECURITY MODEL

We first describe the system architecture of the proposal and then detail our security model.

4. 1. The Architecture The architecture consists of four entities: Service Provider, Attribute Authority (AA), Data Owner (DO) and user or Data Customer (DC) as detailed below and shown in Figure 1 and for more convenience the main notations used in this paper are described in Table 1.

- AA generates system common parameters and master secret key.
- The service provider provides data outsourcing services and includes data servers and a data service manager (DSM). The first consists of many of Public Cloud Servers (PCS) and is responsible for saving ciphertext and encrypted outsourced files. The second is in charge of controlling access from outside.
- DO is a data owner who wants to outsource encrypted files.
- DC is a user with limited resources who intends to encrypt data in cloud storage servers hosted by PCS access.

4. 2. Security Model First, we define the proposal which is followed by the formalized security model. Our scheme has six algorithms, Setup, KeyGenAA, BEKGen, Encrypt, ReEncrypt, and Decrypt, which are specified as the following:

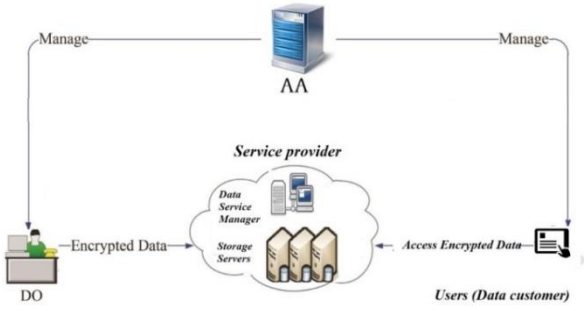


Figure 1. System Architecture

TABLE 1. Main Notations

PK, MK, SK_S	The public, master and secret keys.
λ	The security parameter
q_x	The polynomial of node x
W, T	The access structure and Tree Policy
d_x, t_x	Degree of polynomial & threshold value of node x
LC	The Lagrange Coefficients
g	The generator of the bilinear group
$AP_{PT_{k,i}}$	The Authentication Part
C_W	The ciphertext under W
$PT_{k,i}$	The policy Tree
$CT, C, C_x, C', \tilde{C}$	The outsourced ciphertext
D, D_x, D'_x	Attribute secret keys
n	Number of attributes

$Setup(1^\lambda) \rightarrow (PK, MK)$. It is run by AA and takes a security parameter as input. Then generates the system public key PK and the master key MK. The former is distributed to users and the later is kept private.

$KeyGenAA(PK, MK, S) \rightarrow SK_S$. The algorithm is executed by AA. It takes the system public key PK, the master key MK and an attribute set S as input parameters. Then it generates SK_S as the attribute secret key associated with the attribute set S as output.

$BEKGen(U)$. This is Blinding value Encrypting Key (BEK) algorithm. Input is a set of user indices $\overline{U} \subseteq U$, and outputs are BEKs for each DC in $\overline{U}$. The output is used to encrypt attribute group keys BV_{γ_z} for each $G_k \subset G$.

$Encrypt(P, M, PT_K, PT_{k,i}, i, W) \rightarrow C_W$. It takes the system public key PK, a message M, a symmetric encryption key (PT_K), a seed value ($PT_{k,i}$), an integer and a ciphertext policy as input parameters. The output is ciphertext of message M. This encryption algorithm is run by DO.

$ReEncrypt(C_W; G)$. As input takes the ciphertext C_W which includes a set of attribute groups G and an access structure W. The output is ciphertext $\overline{C_W}$ and only privileged DCs in the group can decrypt the message.

$Decrypt(PK, C_W, PT_K, SK_S) \rightarrow M$: It takes PK, C_W as a ciphertext over policy W, PT_K as the secret key for authentication and SK_S related to attribute set S. The ciphertext C_W will be decrypted by DC. It is run by DC (user).

Based on the system architecture and the definitions, we formalize the security model by specifying adversary ability. Our security game is as follow:

Setup. The public parameters and PK are given to the adversary, Adv when challenger runs the setup algorithm.

Phase 1. In this phase, Adv does repetitive process to generate attribute secret associated with sets of $S1, S2, \dots, S_\varphi$.

Challenge. Now, Adv sent two messages which have equal length, as M_1 and M_2. We select an access structure Γ^+ which is the challenge. None of the sets satisfy Γ^+. Then by flipping a random coin z, the challenger encrypts $M_z$under access structure Γ^+. Then the generated ciphertext, C^+, will be sent to Adv.

Phase 2. With the restriction that none of the sets of attributes $S1, S2, \dots, S_\varphi$ satisfy Γ^+ corresponding to the challenge, phase 1 will be repeated.

Guess. Adv output a guess z' of z.

Now we are ready to define the advantage of Adv as $\Pr[z' = z] - \frac{1}{2}$.

Definition 2. If most advantages of all PPTA (stand for Probabilistic Polynomial-Time Adversaries) in the game is negligible then the proposal is secure.

5. THE PROPOSAL

Assume g is a generator of group $G_1$and G_1 is a bilinear group of prime order p. Also, e: $G_1 \times G_1 \rightarrow G_2$ denotes the bilinear map and ζ is the size of the groups. Our construction is as the following.

5. 1. Initialization and Setup $Setup(1^\lambda) \rightarrow (PK, MK)$: As the first phase in our scheme, the setup function selects a bilinear group G_1 and two random $a, b \in_R Z_p$. The function generates the master key as (b, g^a) and public parameters as:

$$PK =< G_1, g, h = g^b, e(g,g)^a > \quad (1)$$

5. 2. Key Generation Function $KeyGenAA(PK, MK, S) \rightarrow SK_S$: It is run by AA. The algorithm takes the master key, public keys and a set of attributes S as inputs. It outputs attribute secret keys that correspond with the attribute set.

For each attribute $k \in S$, the function selects a random $t \in Z_p$ and random $t_k \in Z_p$ and then generates the attribute secret keys as

$$\forall k \in S\ , SK = (D, D_k, D'_k)$$
$$D = g^{(a+t)b}, D_k = g^{t_k} H(att(k))^{t_k}, D'_k = g^{t_k} \quad (2)$$

Inspired from [4], AA gives the attribute groups G_v for each $\gamma_v \in W$ to DSM.

BEK Generation. Now, DSM executes $KEKGen(U)$ and builds BEKs for DCs in U. She generates a binary BEK tree for users U as in Figure 2. It is used to distribute the attribute group keys to DCs in $\overline{U} \subseteq U$. In the tree, each node n_j of the tree holds a BEK, denoted by BEK_j. Similar to [5], a set of BEKs on the path nodes from a leaf to the root are called *path keys*.

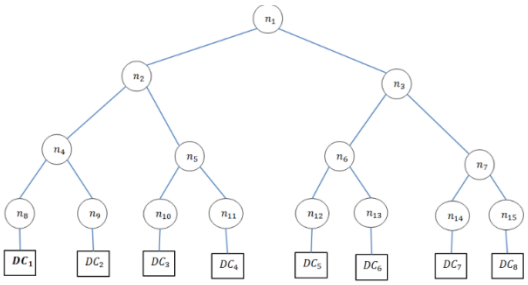


Figure 2. BEK Tree for attribute group key distribution

5. 3. Encryption $Encrypt(P, M, PT_K, PT_{k,i}, i, W) \rightarrow C$. The algorithm includes an authenticator built with symmetric encryption and a hash function. Next phase after key generation is encryption which is encryption of data before outsourcing with a public key which matches with corresponding secret key owned by DC.

The function $Encrypt$ performs the encryption with considering the policy W and access structure T. For each node x (including leaves) of tree T, the function selects a polynomial q_x. The Polynomials are calculated and selected as follows:

Node x has the polynomial degree d_x of q_x and the threshold value t_x, we set $d_x = t_x - 1$. The algorithm starts from root node R and chooses a random $s \in_R Z_p$ and $q_{R(0)} = s$. It chooses d_R other points of R to define it completely. For any other node x, $q_x(0) = q_{parent(x)}(index(x))$ and selects other points randomly for q_x as well. Assume Y is a cluster of nodes (leaf) in Γ associated with W. PT stand for the Policy Tree and is for Authentication Part (AP) of our scheme, and $PT_{k,0}$ is a seed value of our hash chain [17]. The seed value is randomly and securely generated and is kept secret for DO. Another value of the chain will be generated by consecutive hashing on the seed value so we have $PT_{k,i} = h(PT_{k,0})^i$. The authentication part (AP) which is the mechanism to verify outsourced decryption is as below. It only uses symmetric cryptography primitives which is negligible against pairing operations in previous works.

$$AP_{PT_{k,i}} = E_{PT_K}(PT_{k,i}|i) \text{ where } PT_{k,i} = h(PT_{k,0})^i \quad (3)$$

The included ciphertext with the AP is as below.

$$C_W = (\Gamma, \tilde{C} = M'e(g,g)^{as}|AP_{PT_{k,i}}, C = h^s, \forall z \in Y: C_z = g^{q_z(0)}, C'_z = H(att(z))^{q_z(0)}) \text{ where } M' = M|PT_{k,i}|i. \quad (4)$$

The concatenated values to M, $(PT_{k,i}|i)$, and generating M' is to ensure synchronization of index i after disrupting or losing previous packets when network designer want to continuous update of the commitment value. Moreover, the index, i, can easily and efficiently help to detect replayed packets by an attacker. The symmetric key PT_K corresponding to the tree policy is securely transmitted to users along with attribute secret keys.

Data Re-encryption. DSM executes $Encrypt(C_W; G)$ with $G \subseteq \bar{G}$ that is in C_W. The execution progresses as follows:

For all $G_y \in G$, chooses a random $BV_{\gamma_z} \in Z_p^*$. Then, re-encrypts C_W and generates:

$$\overline{CT}_W = (\Gamma, \tilde{C} = M'e(g,g)^{as}|AP_{PT_{k,i}}, C = h^s, \forall z \in Y: C_z = g^{q_z(0)}, C'_z = BV.H(att(z))^{q_z(0)}) \text{ where } BV = \frac{BV_{\gamma_z,j}}{BV_{\gamma_z,j-1}} \text{ and } M' = M|PT_{k,i}|i. \quad (5)$$

Then choose root nodes of the minimum cover sets in the BEK tree from DCs in G_v, for all $G_v \in G$. A set of BEKs that such root nodes of sub-trees for G_i hold are denoted by $BEK(G_v)$.

Finally builds the following header:

$Hdr = (\forall \gamma \in Y: \{E_K(BV)\}_{K \in BEK(G_v)}), (Hdr, \bar{C}_W)$

5. 4. Verification and Decryption $Decrypt(PK, C_W, PT_K, SK_S) \rightarrow M$. Final phase is verification and decryption. After receiving the ciphertext C_W, the user or DC decrypts $AP_{PT_{k,i}}$ with a symmetric algorithm, calculate i times (i at least is one) hash value of $PT_{k,i}$, compares the result with the commitment value. If they are equal then the message is authenticated elsewhere discarded. If the authentication is true, then verification of the outsourced encryption is done and the full decryption of the encrypted outsourced data will be started. It is to extract secret s stored at the root of the access policy tree and then extracting M' and M. Moreover, the secret key of DC_t will be updated as follows:

$$\forall k \in S, SK = (D, D_k, D'_k) \quad D = g^{(a+t)b}, D_k = g^{t_k}H(att(k))^{t_k}, D'_k = g^{t_k}/BV \quad (6)$$

Full decryption algorithm is as $DecryptNode(C_W, SK_S, x)$ and is recursive. The inputs of the algorithm are as: a node x from Γ, a private key, and a ciphertext. The ciphertext is $C_W = (\Gamma, \tilde{C}, C = h^s, \forall x \in Y: C_x, C'_x)$downloaded form PCSs. The private key is SK_S, which is securely transferred to the DC and associated with a set S of attributes. As details, we have two kinds of calculations in full decryption. First is at leaf-node which is proceed by $DecNode(C_W, SK_S, x)$ and the second is calculated recursively by the Lagrange interpolation. For leaf node we set $k = att(x)$. Then it is defined as the following: For each $k \in S$, then

$$DecNode(C_W, SK_S, x) = \frac{e(D_k, C_x)}{e(D'_k, C'_x)} = \frac{e\left(g^t H(att(k))^{t_k}, g^{q_x(0)}\right)}{e\left(\frac{1}{BV}.g^{t_k}, BV.H(att(k))^{q_x(0)}\right)} = e(g,g)^{t.q_x(0)} \quad (7)$$

But if $k \notin S$, it returns null. As the second kind of

calculation of $DecryptNode(C_W, SK_S, x)$, recursive manner, we have: For all children of x, as z, the algorithm $DecNode(C_W, SK_S, z)$ is called and the output is stored as L_z.

Assume S_x is a set of child nodes and its size is k_x. If there is not any such set, the node x will not be satisfied and return false. But if exist, by using polynomial interpolation we calculate,

$$\begin{aligned} L_x &= \\ &\prod_{z\in S_x} L_z^{LC_{k,S'_x(0)}}, where \begin{matrix} k = index(z) \\ S'_x = \{index(z): z \in S_x\} \end{matrix} \\ &= \prod_{z\in S_x} (e(g,g)^{t.q_x(0)})^{LC_{k,S'_x(0)}} \\ &= \prod_{z\in S_x} (e(g,g)^{t.q_{parent(z)}(index(z))})^{LC_{k,S'_x(0)}} \\ &= \prod_{z\in S_x} (e(g,g)^{t.q_x(k)})^{LC_{k,S'_x(0)}} \\ &= e(g,g)^{t.q_x(0)} \end{aligned} \quad (8)$$

and return the result. The decryption algorithms is started by invoking the function on the root R node. As correctness of proposal:
$A = DecNode(C_W, SK_S, t) = e(g,g)^{t.q_R(0)} = e(g,g)^{t.s}$.
The decryption of messages is continuing by calculating:

$$\frac{\hat{C}}{e(C,D)/A} = \frac{M' e(g,g)^{as}.e(g,g)^{(a+t)s}}{e(g,g)^{sb.\frac{(a+t)}{b}}} = M' \quad (9)$$

Finally, M will be easily extracted from M'.

6. DISCUSSION

6. 1. Security In our proposal, as well as previous works, main security and privacy challenge is the collusion of users and PCSs to learn secret keys. Similar to [1, 2, 5], our scheme to prevent the combination of compromised partial attribute keys, randomizes the shared secret and user private keys and includes into ciphertext. For the formal proof purpose, let assume two random encoding γ_1, γ_2 of F_p which is an additive group. It is injective maps $\gamma_1, \gamma_2 : F_p \to \{0,1\}^{\sigma}$, where $\sigma > 3\ log(p)$. We have $G_i = \{\lambda_i(\lambda): z \in F_p\}$ for $i = 0,1$. We have oracles for group action on G_1, G_2, an oracle for hash function H and a one another to calculate the map $e: G_1 \times G_1 \to G_2$. Now to determine the advantage of an adversary to be successful, we give a lower bound by the following theorem.

Theorem. Let ς is the maximum number of received elements by an adversary Adv in interaction with the detailed game. The elements are the response of queries made by the adversary for hash functions, bilinear map, groups G_1 andG_2. With these assumptions, $O(\varsigma^2/p)$ is the advantage of Adv in our security game.

In the following, we give a sketch of proof and remove details due to space limitation. The adversary to successfully break our scheme requires to calculate $e(g,g)^{as}$. To this purpose, s/he has to pair D and C from some user's private key and ciphertext, respectively. In fact, s/he learn $e(g,g)^{as}$, but blinded by some value $e(g,g)^{ts}$. To blind out this value enough users must have the valid secret components. The embedded secret sharing in the ciphertext must be satisfied by the components. Clearly, for unblinding purpose, enough DCs must have valid attribute key components to satisfy access structure and secret sharing included in the ciphertext. Moreover, since in our proposal we randomized the blinding value to the randomness an individual private key, the collusion attacks don't work. The summarized security comparisons of different schemes are shown in Table 2.

6. 2. Computations and Communications In the following, we shortly count the significant computation operations and leave extensive comparison in the extended version. In the key generation algorithm, for every attribute of DC we have two exponentiations and for every attribute in private key two group element. In DO and in encryption process, per each leaf in the access structure, we have two exponentiations. As size of the ciphertext, per each the tree leaf-node we have two group elements. For verification and decryption phase in DC, firstly we have a negligible symmetric hash function calculation in verification mechanism. Secondly, per each leaf-node in the tree access structure, we have two pairings and we require one exponentiation. In our scheme size of ciphertext is $O(n)$ is as equal as some optimal previous scheme and we don't have any extra transmission messages. As short, it means our contribution don't increase bandwidth or communication.

It was a straightforward efficiency analysis of our scheme. Detailed performance and efficiency analysis along with experimental results are left for an extended version of this paper due to space limitation. The summarized efficiency comparisons of different schemes are shown in Table 3.

6. 3. Replay Attack Resistance As before mentioned, the proposal can discard the replayed packets with the included index in the AP. Even in lossy channels where packets will be lost or disrupted by attackers, the concatenated parameters to the M can be used to recover the included index.

6. 4. DoS Attack Resistance Expensive computation or communication tasks on resource-constrained nodes inherently provide DoS vulnerability which usually prevented by using an authentication scheme to discard invalid request or messages, such as matching-and-decryption idea in [6, 9, 23] or verify-then-decrypt instead of the decrypt-and-verify idea in [21].

TABLE 2. Security Comparison

Scheme	Expressiveness	Assumption	Security Model	DoS Attack Resistant	Replay Attack Resistant	Revocation	Expressive
LDGM[12]	Type 1[a]	DBDH	CPA/s-STdM	No	No	No	No
QDLM[13]	Type 1	DBDH	CCA2/s-STdM	efficient	No	No	Yes
NYO [9]	Type 2[b]	DBDH, D-Linear	CPA/s-STdM	inefficient (3n+1)	No	No	No
LRZW[8]	Type 2	DBDH, D-Linear	CPA/s-ROM	inefficient (4n)	No	No	No
ZCLW[10]	Type 2	DBDH, D-Linear	CPA/s-ROM	inefficient	No	No	No
HN[5]	Type 1	DBDH	CPA/s-ROM	No	No	Yes	Yes
Proposed	Type 1	DBDH	CPA/s-ROM	very efficient	Yes	Yes	Yes

[a] Tree-based Structure, [b] AND-gate Structure

TABLE 3. Efficiency Comparison

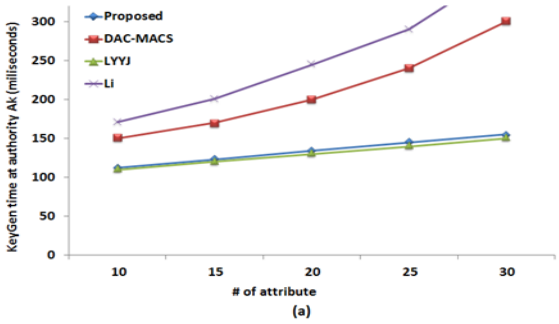
Scheme	Secret key size	Master key size	System public key size	Ciphertext overhead	Auth (Pairing)	Decryption (Pairing)
LDGM[12]	$(2n+1)\|G\|$	$(3n+1)\|Z_p\|$	$(3n+1)\|G\|+\|G_T\|$	$(n+1)\|G\|+\|G_T\|+L_W$	$2n$	$n+1$
QDLM[13]	$(2n+2v+1)\|G\|$	$(3n+2v+1)\|Z_p\|$	$(3n+2v+1)\|G\|+\|G_T\|$	$(n+2v+1)\|G\|+\|G_T\|+L_\alpha+L_W$	n	$n+v+1$
NYO [9]	$(3n+1)\|G\|$	$(2N+1)\|Z_p\|$	$(2N+1)\|G\|+\|G_T\|$	$(2N+1)\|G\|+\|G_T\|$	$3n+1$	$3n+1$
LRZW[8]	$4n\|G\|$	$\|Z_p\|$	$2\|G\|+\|G_T\|$	$4N\|G\|+\|G_T\|$	$4n$	$4n$
ZCLW[10]	$(5n+2)\|G\|$	$\|Z_p\|$	$3\|G\|+\|G_T\|$	$(3N+4)\|G\|+2\|G_T\|$	$n+1$	$n+1$
Proposed	$(2n+1)\|G\|$	$\|Z_p\|+\|G\|$	$3\|G\|+\|G_T\|$	$(2t+1)+\|G_T\|+\|L_W\|$	0	$2n$

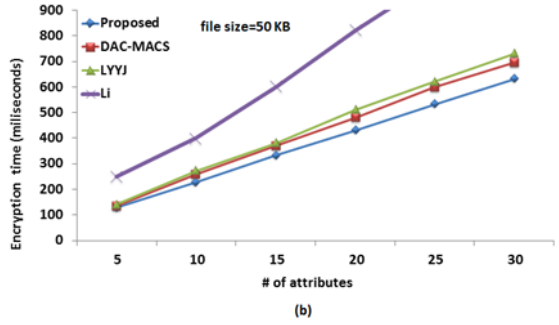
But due to the so lightweight verification and authentication proposed mechanism, our proposal fundamentally doesn't burden any significant computation or communication in the verification of invalid packets. Then the attackers cannot launch the attacks for example to deplete the node's power [24].

7. EXPERIMENTAL RESULTS

We used cpabe-toolkit source code [25] to implement our proposal and conduct a comparison. The evaluation is done on Linux Kali 32-bit with Intel Pentium T4400 @ 2.2 GHz, 4GB RAM and pbc-0.5.14 library. We used a 160-bit elliptic curve g group and non-singular elliptic curve type A, $y^2 = x^3 + x$, over a 512-bit finite filed, as well as the cpabe-toolkit. We evaluated our proposal, DAC-MACS, LYYJ and Li [20].

Figure 3 (a) show significant efficiency of the proposal at DC during the key generation process. The encryption time comparison results are shown in Figure 3 (b). The encryption time is directly related to the number of attributes in the access tree. Figure 3 (c) show the efficiency at DC which are assumed power-limited. The figures confirm that we achieved very small and negligible overhead in the proposal for decryption and verification. We used the optimization methods detailed in Bethencourt et al. paper [25] to minimize the number of pairings and exponentiations in the access tree traverse. For encryption and decryption algorithm evaluation, to avoid domination of symmetric encryption (AES) over ABE algorithm, we retained the small File Size as 50-KB.





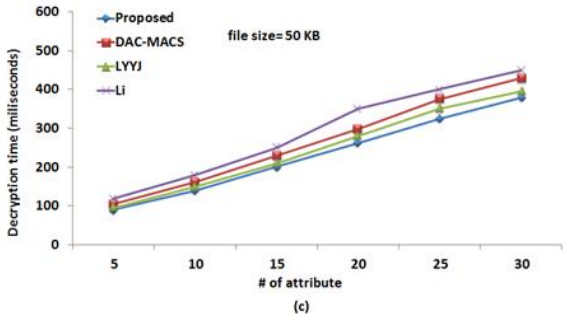


Figure 3. BEK Tree for attribute group key distribution

8. CONCLUSION

We have proposed an access control based on Attribute-Based Encryption which provides so efficient source authentication for fast verification of outsourced encryption especially for resource-constrained devices to thwart DoS attacks along with very efficient attribute and user revocation mechanism. Also with a simple mechanism, it discards the replayed packets. Finally, we conducted an optimized implementation to demonstrate the efficiency of the proposal in comparison to some well-known schemes. As future works, we consider the proposal in a multi-authority architecture with enhanced privacy.

9. REFERENCES

1. Sahai, A. and Waters, B., "Fuzzy Identity-Based Encryption", Springer, Berlin, Heidelberg, (2005).
2. Goyal, V., Pandey, O., Sahai, A. and 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 - CCS '06, ACM Press, (2006), 89–98.
3. Mohammadia, A. and Hamidi, H., "Analyzing Tools and Algorithms for Privacy Protection and Data Security in Social Networks," ***International Journal of Engineering - Transaction B: Applications***, Vol. 31, No. 8, (2018), 1267–1273.
4. Nasiraee, H. and Ashouri-Talouki, M., "Dependable and Robust Attribute-Based Encryption in Mobile Cloud Computing," Iranian Conference on Electrical Engineering (ICEE), IEEE, (2018), 1536–1541.
5. Hur, J. and Noh, D.K., "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," ***IEEE Transactions on Parallel and Distributed Systems***, Vol. 22, No. 7, (2011), 1214–1221.
6. Ostrovsky, R., Sahai, A. and Waters, B., "Attribute-based encryption with non-monotonic access structures," In Proceedings of the 14th ACM conference on Computer and communications security, ACM, (2007), 195–203.
7. Zhang, Y., Chen, X., Li, J., Wong, D.S., Li, H. and You, I., "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," ***Information Sciences***, Vol. 379, (2017), 42–61.
8. Li, J., Chen, X., Chow, S.S., Huang, Q., Wong, D.S. and Liu, Z., "Multi-authority fine-grained access control with accountability and its application in cloud," ***Journal of Network and Computer Applications***, Vol. 112, (2018), 89–96.
9. Nishide, T., Yoneyama, K., and Ohta, K., "ABE with Partially Hidden Encryptor-Specified Access Structure", In Proceedings of Applied Cryptography and Network Security (ACNS), ACNS'08, LNCS 5037, (2008), 111–129.
10. Zhang, Y., Chen, X., Li, J., Wong, D.S. and Li, H., "Anonymous attribute-based encryption supporting efficient decryption test," In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13, ACM Press, (2013), 511–516.
11. Qin, B., Deng, R.H., Liu, S. and Ma, S., "Attribute-Based Encryption With Efficient Verifiable Outsourced Decryption," ***IEEE Transactions on Information Forensics and Security***, Vol. 10, No. 7, (2015), 1384–1393.
12. Lai, J., Deng, R.H., and Li, Y., "Fully Secure Cipertext-Policy Hiding CP-ABE", Springer, Berlin, Heidelberg, (2011).
13. Jung, T., Li, X.Y., Wan, Z. and Wan, M., "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption," ***IEEE Transactions on Information Forensics and Security***, Vol. 10, No. 1, (2015), 190–199.
14. Ahuja, R., Mohanty, S. K., and Sakurai, K., "A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing," ***Computers & Electrical Engineering***, Vol. 57, (2017), 241–256.
15. Han, J., Susilo, W., Mu, Y., Zhou, J. and Au, M.H., "PPDCP-ABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption", Springer, Cham, (2014).
16. Wang, J., Huang, C., Xiong, N.N. and Wang, J., "Blocked linear secret sharing scheme for scalable attribute based encryption in manageable cloud storage system," ***Information Sciences***, Vol. 424, (2018), 1–26.
17. Wang, H., He, D., and Han, J., "VOD-ADAC: Anonymous Distributed Fine-Grained Access Control Protocol with Verifiable Outsourced Decryption in Public Cloud," ***IEEE Transactions on Services Computing***, (2017), 1–1.
18. Li, J., Zhang, Y., Chen, X. and Xiang, Y., "Secure attribute-based data sharing for resource-limited users in cloud computing," ***Computers & Security***, Vol. 72, (2018), 1–12.
19. Liu, Y., Zhang, Y., Ling, J. and Liu, Z., "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," ***Future Generation Computer Systems***, Vol. 78, (2018), 1020–1026.
20. Li, J., Wang, Y., Zhang, Y. and Han, J., "Full Verifiability for Outsourced Decryption in Attribute Based Encryption," ***IEEE Transactions on Services Computing***, (2017), 1–1.
21. Li, J., Huang, Q., Chen, X., Chow, S.S., Wong, D.S. and Xie, D., "Multi-authority ciphertext-policy attribute-based encryption with accountability," In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS '11, ACM Press, (2011), 386–390.
22. Yang, K., Jia, X., Ren, K., Zhang, B. and Xie, R., "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems," ***IEEE Transactions on Information Forensics and Security***, Vol. 8, No. 11, (2013), 1790–1801.
23. Asadi, F. and Hamidi, H., "An Architecture for Security and Protection of Big Data," ***International Journal of Engineering - Transaction A: Basics***, Vol. 30, No. 10, (2017), 1479–1486.
24. Rezai, H. and Speily, O.R.B., "Energy aware resource management of cloud data centers," ***International Journal of Engineering - Transactions B: Applications***, Vol. 30, No. 11, (2017), 1730–1739.
25. Bethencourt, J., Sahai, A., and Waters, B., "Ciphertext-Policy Attribute-Based Encryption," In 2007 IEEE Symposium on Security and Privacy (SP '07), (2007), 321–334.

DoS-Resistant Attribute-Based Encryption in Mobile Cloud Computing with Revocation

H. Nasiraee, M. Ashouri-Talouki

Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran

P A P E R I N F O

Paper history:
Received 25 October 2018
Received in revised form 15 May 2019
Accepted 31 July 2019

Keywords:
Attribute-Based Encryption
Dos Resistance
Iot Devices
Mobile Cloud Computing
Secure Access Control

چکیده

امنیت و حریم خصوصی چالش‌های مهمی برای برون‌سپاری داده‌ها روی سرورهای ابری هستند. با اعمال کنترل دسترسی ویژگی‌مبنا، کنترل دسترسی ریزدانه روی داده‌های برون سپارس شده بدست می‌آید. در این مقاله، کارهای پیشین در حوزه کنترل دسترسی با استفاده از رمزنگاری شناسه‌مبنا برای کاربران با منابع محدود محاسباتی در محیط‌های ابری در دو جنبه توسعه داده می‌شود، یک روش احراز اصالت جدید و یک رهیافت لغو عضویت. برای فراگیر شدن این سیستم کنترل دسترسی، یک روش احراز اصالت سبک وزن برای احراز اصالت متن‌های رمزگزاری شده قبل از شروع الگوریتم‌های پزهزینه رمزگشایی ضروری است تا از حملات منع‌سرویس با هدف از کار انداختن شبکه و تخلیه منابع گره‌های محدود جلوگیری شود. به این منظور یک طرح احراز اصالت بسیار کارا و سبک وزن برای تصدیق متن‌های رمز شده قبل رمزگشایی و در نتیجه افزایش پایداری شبکه در برابر حمله یاد شده ارائه می‌شود. توسعه دوم، مربوط به ارائه یک رهیافت سبک وزن حذف ویژگی و لغو عضویت کاربر است که چالش بسیار مهم دیگر در اعمال کنترل دسترسی ویژگی‌مبنا است. در پایان، با ارائه بحث در خصوص جنبه‌های مختلف و تشریح نتایج پیاده سازی، مزایای طرح را نشان می‌دهیم.

***doi**: 10.5829/ije.2019.32.09c.09*